*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. 18, Issue No. 5, August-2021, ISSN 2230-7540*

# Cyber Threats and the Laws to Protect against It in India

**Harsh Gopalia[1]* Dr. Arvind Rathore[2]**

[1] Research Scholar, Maharishi Arvind University, Jaipur-302041

[2] Supervisor, Faculty of Law, Maharishi Arvind University, Jaipur-302041

***Abstract – As far as cyber security is concerned, it is the process of guarding against hostile assaults on internet-connected systems including computers, servers and mobile devices, as well as electronic systems and networks and the data they contain. Threats to cyber security or the digital world in general are hostile acts designed to corrupt or destroy information or disrupt digital activities. Computer viruses, data breaches, and Denial-of-Service (DoS) assaults are examples of cyber threats. Most often, cyber-attacks happen because criminals want your business financial details and customers financial details (e.g. Credit Card data) customers or staff email addresses and login credentials. Direct, indirect, veiled, and conditional threats all fall within this category. In this article, the researchers seek to offer some insight on the "Big 3" forms of cyber assaults, such as Malware, Ransomware, and Phishing. Social hacking (employees still fall prey to social assaults), ransomware, using active cyber security monitoring, unpatched vulnerabilities/poor updating, and distributed denial-of-service (DDoS) attacks were recognised as the worst cyber security threats in 2019. Although there will be a plethora of new cyber dangers and assaults by 2020, the primary cause for this is still a lack of awareness and a low level of technical proficiency. The object of this article is to make aware of the types of Cyber threats and attacks from security point of view and in order to prevent the multiplication of Cyber-crimes too in a very simple language.***

***Key Words – Cyber-attacks, Cyber threats, Cyber Security, Malware, Ransom ware, and Phishing, Distributed Denial of Service, Password attacks***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - X - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

## INTRODUCTION

The rapid and continual evolution of security vulnerabilities is one of the most challenging aspects of cyber security. The hacking methods of cyber thieves are advancing at a fast pace. Because they strike so rapidly, being protected is more important than ever. Because of this, recognising the threat is a necessary first step in implementing a successful cyber security plan. To define a cyber-assault, we need to look at what it means to launch one from a computer and what it means to target a website, computer system, or individual machine. Cyber assaults may take a variety of shapes and sizes. ”[1]Their objectives include (verbatim):

1. Unauthorized access to a computer system or its data is gained by gaining, or attempting to obtain, this access.

2. Attacks that cause unintended interruption or denial-of-service, such as the downtime of whole websites.

3. Installing harmful software like viruses or malware on a computer system.

4. Unauthorized processing or storage of data on a computer system.

5. Modifications made to a computer system without the owner's knowledge, approval, or direction, and

6. Inappropriate use of computer systems by employees or former employees.[2]

[1] “Cyber Attacks: Prevention and Proactive Responses,” Practical Law Company, 2011 [Authors: Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP], https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/ PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Reprinted with permission from the author]

[2] “Cyber Attacks: Prevention and Proactive Responses,” Practical Law Company, 2011 [Authors: Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP],

To preserve your IT infrastructure and data, you must create and execute effective protections to assure the supply of key infrastructure services. The accompanying image depicts common cyber assault threat tactics.[3]

## THE MOST COMMON TYPES OF CYBERATTACKS

**A.** **Advanced persistent threats, or APTs**, assaults that target a network over the long term and penetrate it in steps to evade discovery Recon (studying and understanding the target), incursion (delivery of targeted malware), discovery (exploiting captured information).

**B.** **Distributed Denial of Service or DDoS** may take place when a server is deliberately overburdened with requests in order to bring down a targeted website or network infrastructure. As a result, users may be unable to access your site or network, which may cause your company activities to be partially or completely suspended, depending on how heavily you rely on the Internet.

**C.** **Inside attack:** A complex software programme may not even be necessary for this sort of cyber-attack: Administrative rights are intentionally misused by someone from within the business who wants access to sensitive corporate data. In particular, if an employee leaves the firm on poor terms, they create a hazard. As a result, your organisation should have protocols in place to revoke any access to corporate data as soon as an employee is terminated. When a hacker poses as a representative of a firm with whom your business does business in order to obtain access to sensitive data, this is known as an inside assault.

**D.** **Malware or "malicious software,"** It encompasses all software used to harm or gain unauthorised access to the target computer. Ransomware, spyware, and worms are among the numerous forms of malware that may infect a computer.

**E.** **Password attacks:** It's easy for hackers to get into a target's accounts and databases by cracking the password to that target's system. Password assaults fall into three categories: brute force, dictionary, and key logging. Brute force attacks entail guessing passwords until the hacker gains access, whereas dictionary attacks utilise a computer to attempt different word combinations from the dictionary.

**F.** **Phishing:** Phishing is a popular method of cyber theft in which a legitimate-looking (but ultimately fraudulent) Sensitive information such as credit card details and login passwords are collected by a website and sent to unintended recipients through email. It's crucial to stay on top of the newest security measures to defend yourself against phishing scams, as individuals become increasingly aware of classic phishing strategies such as a notification from a financial institution with a URL that's incorrect or insecure." [4] Given the goals of a cyber-assault and some of the techniques employed to carry them out, a small company' cyber security strategy should include physical, network and data protection.

Cyber Security is a process that's designed to protect networks and devices from external threats. Typically, companies hire Cyber Security Professionals in order to safeguard their private information while also preserving staff morale and increasing consumer trust in their products and services.. CIA is the industry standard for confidentiality, integrity, and availability (or CIA) in cyber security. There must be no unauthorised access to the data or systems, and no one except the rightful owners may make changes or remove information. Finally, there must be no limitations on the usage of systems, functions, or data, and all of these things must be available on demand within predetermined limits. When it comes to cybersecurity, using authentication techniques is critical. User names identify accounts that a person wants access to, whereas passwords ensure that person is indeed who they say they are.

Unauthorized use of a computer, device, or network is considered cybercrime. There are three sorts of computer crimes: crimes against computers, crimes against computers as a target, and crimes against computers that are just incidental to the crime. Denial-of-Service attacks, when a hacker uses all of a server's resources to prevent legitimate users from accessing any data, are common methods used by cybercriminals to make money from their crimes. When a worm or virus infects a victim's computer, it renders it inoperable. A hacker who places himself between a victim's computer and a router in order to sniff data packets is known as a "Man in the Middle." The term "phishing" refers to the practise of a hacker sending an email that looks to be from a trustworthy

https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/ PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Reprinted with permission from the author]

[3] "M-Trends® 2015: A View from the Front Lines," [Threat Report], Mandiant®, a FireEye® Company, 2015, https://www2.fireeye.com/rs/fireye/images/ rpt-m-trends-2015.pdf

[4] "Cybersecurity: A Small Business Guide," Business News Daily, 7/28/15, http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html [Reprinted with permission from the author

source while really being from an impostor. In addition to these sorts of cyber assaults, there are a number of others, such as cross-site scripting, password, eavesdropping, and SQL-injection attacks.

The primary goal of cybercrime is to do significant harm to businesses and vital infrastructure. Additionally, cybercriminals frequently exploit stolen data to their advantage monetarily, to cause financial loss, to harm a person's reputation, to accomplish military goals, or to spread religious or political ideologies. Some hackers don't even require a reason; they do it for the sheer enjoyment of it or to demonstrate their prowess. Here’s a breakdown of the most common types:

- **Black-Hat Hackers:** Black-hat hackers create fictitious identities and then use those identities to carry out harmful acts for financial gain.
- **Gray-Hat Hackers**: They're both shady hackers and honest security experts..
- **White-Hat Hackers:** As security experts, white-hat hackers find and patch vulnerabilities and guard against hostile hackers.
- **Suicide Hackers:** Ultimately, they want to publicly bring down key infrastructure for societal good.
- **Script Kiddies:** Scripts and software written by more experienced hackers are run by inexperienced hackers.
- **Cyber Terrorists:** They instill terror by causing havoc on huge computer networks, and they do it because of religious or political convictions.
- **State-Sponsored Hackers:** As a result of their intrusion into the government's networks, they have access to highly sensitive information and have the ability to cause significant harm to information systems.
- **Hacktivists:** Promote political agendas by secretly defacing and disabling websites

## CYBER LAWS OF INDIA

To put it another way, cyber-crime is any illegal activity that utilizes a computer, whether as a tool, a target, or both. India's Penal Code covers a wide range of cybercrime offences such as theft, fraud, forgery and defamation. Information Technology Act of 2000 tackles the problem of new-age crimes generated by computer abuse. We can categorize Cyber-crimes in two ways:

**Computer as a Target:** attacking another computer by the use of software such as a virus or worm or by using a DOS assault.

**Computer as a Weapon:** computer crime such as cyber terrorism, IPR infringement, credit card fraud, electronic funds transfer fraud and pornography.

To explain the legal concerns associated with the use of communications technology, notably "cyberspace," a phrase used to characterised the Internet, is called cyber law It is a junction of several legal areas, including Intellectual property, Privacy, Freedom of speech, and Jurisdiction, rather than a discrete subject of law like property or contract. At its core, Cyber law is an attempt to address the unique problems posed by human behaviour online while yet adhering to traditional legal principles. During the development of the Internet, the pioneers had no idea that it would become an all-encompassing revolution that would be abused for criminal purposes and demand control.

## JURISPRUDENCE OF INDIAN CYBER LAW

The Information Technology Act, 2000 (IT Act), which went into effect on October 17, 2000, is India's major source of Cyber legislation. With this Act, electronic trade will be recognised by the law and electronic records will be easier to file with the government. Other computer crimes are likewise penalized under the IT Act, and those who commit them face stiff penalties. This Order, which was passed on September 19th, 2002, corrected a few inconsistencies in the Information Technology Act. A Digital Signature Certificate application procedure was outlined in a Presidential Executive Order that was issued on September 12th, 2002. By the Negotiable Instruments (Amendments and Other Provisions) Act of 2002 the IT Act was modified. Truncated checks and electronic cheques were also introduced as a result of this. To ensure that papers are filed with the government in a timely manner and to ensure that licences are issued by the government, Information Technology Rules, 2004 was implemented. Additionally, it outlines how fees are paid and received for services provided by government agencies. IT Rules, 2000 were implemented on the same day. There are regulations dictating who is eligible to be a Certifying Authority and who can be appointed (CA). These regulations also specify the technological requirements, processes, and security measures that a CA must follow.. [...] This set of guidelines was revised three times, the last time in 2006. The Negotiable Instruments Act, 2002, made changes to the IT Act. Truncated checks and electronic cheques were also introduced as a result of this. To ensure that papers are filed with the government in a timely manner and to ensure that licences are issued by the government, Information Technology Rules, 2004 was implemented. Additionally, it outlines how fees are paid and received for services provided by government agencies. IT Rules, 2000 were implemented on the same day. There are regulations dictating who is eligible to be a Certifying Authority and who can be appointed (CA). These regulations also establish technological norms and processes, and presently a great deal of unsettling stuff occurs in cyberspace as a result of these things. Various illegal actions may be carried out on the Internet without repercussions due to its anonymous character, and those with intelligence have taken use of this fact to further illicit operations in cyberspace. As a result, India need Cyber laws. For the majority of Indians, the internet is a way of life. We have a lot of fun here and spend a lot of time doing entertaining things, but it's not without its share of difficulties as well.

## CYBER LAW-A SEPARATE DISCIPLINE

Cyber law may be defined as the law governing cyberspace which is a non-physical terrain created when two or more computers are networked together. Online systems create a cyberspace[5] within which computer users can communicate with one another. Considered from this point of view the term cyber law refers to law relating to computer, computer networks and includes all ' activities that take place in relation to information stored, exchanged or retrieved using the computer system.[6] Ever increasing use of computers and internet have provided enormous scope for the computer abusers to carry on their illegal activities for personal gain, avenge rivalry or for political or commercial purposes and innocent persons , become potential victims of their criminal acts. Therefore, a separate law to prevent and control cyber criminality was the need of the time. Reacting sharply against cybercrime and criminals, many countries have enacted cyber laws that specifically deal with cybercrimes, while others have made these crimes as punishable offences under their existing penal statutes. It hardly needs to be reiterated that cyberspace recognizes no territorial boundaries therefore, a person skilled in computer operations in India can easily dupe a person having bank account in U.S.A. by transferring millions of rupees in another bank in England within no time, with the help of his laptop and a cell phone.[7] Again, extremely fast mobility and anonymity in cyberspace further facilitates the cyber criminals to remain unidentified and untraceable for the offence committed through computer networks. 36 The violation of rights to intellectual property and right to privacy are other vulnerable areas where cyber criminals usually operate, which requires special cyber laws to deal with and apprehend these criminals. There was no separate and independent cyber law in India prior to the enactment of the Information Technology Act37 2000 and all the computer related crimes were tried under the traditional law of crimes i.e. the Indian Penal Code, 1860. However, the information technology advanced by computer networks started having its impact on every aspect of society and governance in , the new millennium. With the increased dependence on e-commerce and e-governance, a variety of legal issues related to use of computers and internet or digital processing devices such as violation of IPR's, piracy, freedom of expression, jurisdiction etc. emerged which could not be redressed by the existing laws because the cyberspace has no geographical limitations nor does it have any physical characteristics such as sex, age etc. This posed practical problems, before the law enforcement agencies in regulating cyberspace transactions of citizens within the country as also the countries abroad. Though in practical terms an internet user is subject to the laws of the State within which he/she operates, but this general rule runs into conflict where the disputes are transnational in nature. It is true that at the time when computer technology was in its developing stage, no one ever contemplated that it can be discretely [8] On June 9, 2000, the President of India signed into law the Information Technology Act, 2000, which went into effect on July 1, 2001.October 17, 2000, it consists of 94 Sections in 13 Chapters and four Schedules. Though the computers misused by internet users for criminal purposes but experience has shown that the world of internet too has a dark side as it gives rise to new variety of crimes called the cybercrime. It is in this backdrop that Information Technology Act was enacted by Indian Parliament. The objectives of the Act as contained in the statement of the objects as follows :- "Using non-paper-based means of information transmission and storage for electronic filing of papers with government bodies and amending the Indian Evidence Act, 1872, and the Bankers Book is known as electronic commerce (e-commerce for short)." A plain reading of the statement of objects of the Act would reveal that the Information Technology Act was primarily introduced to facilitate arid promote e-commerce,[9] which had gained momentum due to the switchover from traditional paper-based methods of information[10] A transaction is considered an e-commerce transaction if it is completed using electronic data interchange and other electronic communication techniques rather than paper-based methods of communication and information storage[11] i.e. networked computers' communication system. The Preamble of the Act sought to:

1. Provide legal recognition for e-commerce;

[5] Cyberspace is not restricted to internet alone, but in its wider sense, it includes computers, computer networks, software data etc

[6] Asian School of Cyber Law : Fundamentals of Cyber Law (2005) p. 4.

[7] Abdul Kalam : The Law of Cyberspace (Published by Institute of Training and Research, U.S.A.; (2006)p. 12

[8] Ibid.

[9] The' Information Technology Act, 2000 received the accent of the President of India on June 9, 2000 and came into force w.e.f. October 17, 2000, it consists of 94 Sections in 13 Chapters and four Schedules

[10] E-commerce refers to transactions out by means of electronic data interchange and other means of electronic communication which involve the use of alternative to paper-based methods of communication and storage of information

[11]Infra Chapter VII

2 Streamline the process of filing papers electronically with government organisations.;

3. The Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Bankers Books Evidence Act of 1891, and the Reserve Bank of India Act, 1934, all need to be updated, and:

4. Ensure efficient delivery of government-services by means of reliable electronic records.[12]

As a result, the Act creates a legal framework that protects the integrity of electronic records and other electronic-based activities. It must be stated that the Information Technology Act[13] 2000 enacted by the Parliament is essentially based on the Model Law on e-commerce adopted by the United Nations Commission on International Trade Law to which India is a signatory member. It was only after years of implementation that flaws and weaknesses in the Act became apparent, preventing it from functioning properly. Indian authorities developed regulations to regulate application and provide guidance for certification authorities in light of the Information Technology Act, 2000, which was passed in the country in 2000. The rules made under the Act were called the Information Technology ' Rules, 2000 which came into force on October 17, 2000. Cyber Regulation Appellate Tribunal Rules, 2000 came into effect at the same time as these other rules. The Information Technology Bill, 2006 was passed by Parliament on December 24, 2008, and the President of India gave his assent on February 5, 2009, making it the Information Technology (Amendment) Act, 2008 when it came into effect (Act No. 10 of 2009). The Amendment Act aims to close the gaps in current IT legislation and make it more useful.

Because of the rapid advancement of technology and widespread availability of the Internet, cybercrime has also increased in frequency. There are several ways to become prey to criminal cyber operations, including hacking computers or fabricating fictitious online transactions. The Information Technology Act, 2000 was passed by the Indian government to deal with actions that infringe on the rights of Internet users. It has sections like these that aim to empower Internet users while also protecting cyberspace:

Section 65 – Tampering with computer Source Documents

When computer source code is required by law to be kept, it is a crime to conceal, delete or change it in any way. The offender faces 3 years in jail or a fine of 2 lakh INR, or both.

Section 66 - Using password of another person

Section 66D - Cheating Using computer resource

Section 66E - Publishing private Images of Others

Section 66F - Acts of cyber Terrorism

Section 67 - Publishing Child Porn or predating children online

Section 69 - Govt.'s Power to block websites

Section 43A - Data protection at Corporate level

## CONCLUSION

The Need for a Uniform Cyber Law Across the Globe Despite the UN's sincere efforts to develop comprehensive cyber legislation that could be applied uniformly across all countries for the prevention and control of cybercrimes, member states' responses have been less than encouraging because there is no unanimity of opinion regarding the concern for control and minimization of these crimes. Different legal regimes have different organisational structures, which explains the disparity in their approaches to internet crime. Despite the fact that a number of international conventions and treaties have been established to provide a uniform legal approach for the prevention of borderless cyber-crime, these attempts have failed due to a lack of member country cooperation and initiative. Further, there being no uniformity as to the concern and sensitivity of countries to cybercrimes due to variation in their socio-economic and cultural conditions, the countries which are not much affected by these crimes are bound to react differently than those which are seriously affected by them. Under the circumstances, it is futile to expect a uniform approach of all the countries towards prevention and control of cybercrime. Perhaps, this is the main reason for lack of active cooperation on the part of different countries to support a global cyber legislation which could be uniformly applicable to all the countries' of the world. Though a cyber-law on a global scale is yet to evolve, the urgency of such a law is being increasingly felt by countries all over the world due to the growth of internet which provides innumerable opportunities for criminals to engage in a variety of criminal activities which have transnational or international repercussions.

## REFERENCES

1. "Comp. TIA Career Roadmap". Comp. TIA. Retrieved 20 Aug 2019.

[12] Consequent to the passing of the Information Technology Act, 2000, the Government of India framed rules under the Act for regulating the application and providing guidelines for certifying authorities

[13] The rules made under the Act were called the Information Technology (Certifying Authorities) ' Rules, 2000 which came into force on October 17, 2000. Another set of rules called the Cyber Regulation Appellate Tribunal (Procedure) Rules, 2000 were also enforced on the same date.

2. Ciampia, Mark (2018). Security+ Guide to Network Security Fundamentals. Cengage. ISBN 978-1337288781.

3. Stallings & Brown (2017). Computer Security: Principles and Practice (4 ed.). Pearson. ISBN 978-0134794105.

4. Stallings, William (1995). Network and Internetwork Security: Principles and Practice. IEEE Press. ISBN 0-7803-1107-8.

5. The Open University (2016). Network security. Kindle.

6. Merkow & Breithaupt (2014). Information Security: Principles and Practice (2 ed.). Pearson. ISBN 978-0789753250.

7. Stallings, William (2016). Cryptography and Network Security (7th ed.). Pearson. ISBN 978-0134444284.

8. Kahn, David (1967). The Code Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner. ISBN 0-684-83130-9.

9. Fridrich, Jessica (2009). Steganography in Digital Media. Cambridge. ISBN 978-0521190190.

10. Macrakis, Kristie (2014). Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to Al-Qaeda. Yale University Press. ISBN 978-0300179255.

11. Kao, I Lung (2019). Effective and Efficient Authentication and Authorization in Distributed Systems. University of Florida. ISBN 978-0530003245.

12. ICT School (2019). Hacking Tools for Computers. ICT School. ISBN 9781088521588.

13. Diogenes & Ozkaya (2018). Cybersecurity--Attack and Defense Strategies. Packt Publishing. ISBN 978-1-78847-529-7.

14. Andes, Thomas (8 April 2016). The Encyclopedia of Computer Security Exploits. ISBN 9781530944682.

15. Britz, Marjie (2013). Computer Forensics and Cyber Crime (3 ed.). Pearson. ISBN 978-0132677714.

16. Kaplan, Fred (2016). Dark Territory: The Secret History of Cyber War. Simon & Schuster. ISBN 978-1476763262.

17. Lopez & Setola (2012). Critical Infrastructure Protection. Springer-Verlog. ISBN 978-3642289194.

18. Stewart, Michael (2013). Network Security, Firewalls, and VPNs (2 ed.). James & Bartlett Learning. ISBN 978-1284031676.

19. Grasser, Michael (2008). Secure CPU: A Secure Processor Architecture for Embedded Systems. VDM Verlag. ISBN 978-3639027839.

20. Jacobs & Rudis (2014). Data-Driven Security. Wiley. ISBN 978-1118793725.

21. Campbell, T. (2016). Practical Information Security Management: A Complete Guide to Planning and Implementation. APress. ISBN 9781484216859.

22. Calder, Alan (28 September 2018). NIST Cybersecurity Framework: A Pocket Guide. IT Governance Publishing Ltd. ISBN 978-1787780422.

23. Alsmatti, Izzat (2019). The NICE Cybersecurity Framework. Springer. ISBN 978-3030023591.

24. NIST. "Framework for Improving Critical Infrastructure Cybersecurity v1.1" (PDF). NIST. Retrieved 19 Aug 2019.

25. NIST. "Cybersecurity Framework Page". NIST. Retrieved 19 Aug 2019.

26. NIST. "NIST SP 800-181: NICE Cybersecurrity Workforce Framework" (PDF). NIST. Retrieved 19 Aug 2019.

27. U.S. Congress. "Cybersecurity Enhancement Act of 2014". U.S. Congress. Retrieved 19 Aug 2019.

28. Center for Internet Security. CIS Controls V7.1.

29. NIST. Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations (PDF).

30. Talabis & Martin (2013). Information Security Risk Assessment Toolkit. Syngress. ISBN 978-1597497350.

31. ISACA. The Risk IT Practitioner Guide.

32. Kosseff, Jeff (2017). Cyber Security Law. Wiley. ISBN 978-1119231509.

33. Taylor, Laura (2013). FISMA Compliance Handbook (2 ed.). Elsevier. ISBN 978-0124058712.

**Corresponding Author**

**Harsh Gopalia***

Research Scholar, Maharishi Arvind University, Jaipur-302041