

Cyber Law-A Critical View on Existing Cyber Laws in India: Do they Suffice in Today's World?

Kirtika Gupta*

Abstract

In the 21st century, numerous technologies have become fundamental elements of one's life. Although, these technologies are immensely functional and informative but often leads to certain cybercrimes which would not only affect individual but also society at large. Secure cyberspace is very crucial for a nation to defend itself from any cyber-attack. Nowadays, cyber-crime has become a major concern in India and the existing laws related to cyber-crime are insufficient to deal with the increase in the number of crimes related to cyberspace. These policies were designed to eliminate or rather reduce such crimes but clearly, these policies need to be revised and reworked thoroughly to suffice in today's world. There are several laws and policy relating to cyber security in India such as the Information Technology Act, 2000, the Indian Penal Code 1860, and the National Cyber Security Policy, 2013 (a framework of DeitY) which protect and penalizes numerous cyber-crimes. The paper primarily focuses on the critical review of cyber security in India. As per reports, India, in the year 2022, have more than 658 million internet users which are nearly 47% of the total population of India. It denotes that all these millions of internet users are under threat of cyber-attack in one or the other way. Furthermore, the recent it could be very well documented that many governmental agencies have become a target of cyber-attacks; even neighbouring countries are mounting cyber-attack on the Indian army as well. In these situations, India should make strong and viable cyberspace for the safety of governmental agencies as well as for every individual to protect the cyber sovereignty of India. More than that attack on the government, many individuals and hacking groups are there in India which has become a possible reason for cyber threats and attacks in India. Hacking groups conduct such activities for personal gains likely to be fraud through the internet and individual do so for some personal goal as to harass another individual. But overall cyber-attacks and threats must be dealt with utmost strictness to preserve and protect cyberspace in India. The article also discusses how a mechanism can be built, or the foundation of cyber security be made effective for the public at large as cyber sovereignty is of utmost importance in today's world to defend a country from any possible cyber-attacks. The acknowledgment of a weak and meagre framework should be done and preventive measures should be taken as soon as possible. Since in this time a nation to be a superpower must have a proper defense on cyber security and tools to attack the country when needed. This paper aims to critically and comprehensively review the existing cyber laws in India and propose a standard mechanism and framework for the same. In addition, the various method proposed by the stakeholders of cyber security to prevent cyber threats, attacks, and cyber-crimes are also studied in the paper.

*Author for Correspondence

Kirtika Gupta
E-mail: guptakirtika29@gmail.com

Student, Ramaiah Institute of Legal Studies, Bangalore,
Karnataka, India

Received Date: July 13, 2022
Accepted Date: July 15, 2022
Published Date: July 30, 2022

Citation: Kirtika Gupta. Cyber Law-A Critical View on Existing Cyber Laws in India: Do they Suffice in Today's World? National Journal of Cyber Security Law. 2022; 5(1): 7-11p.

Keyword: Cyber law, framework, information technology act, cybercrime, policy

INTRODUCTION

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."

—Britney Hommertzhaim

As we all know Computer scientists *Vinton Cerf* and *Bob Kahn* are credited for the invention of the Internet communication protocol as we today know as 'the Internet' [1]. The fundamental idea behind such invention was to build a community of intercommunication, commercial activity, military use, and entertainment. The Internet has seen a plethora of evolution since its inception. The development of Internet technology *per se* is imperative for the evolving world but it does come with a certain disadvantage. The misuse of technology for gain over others is dangerous for society at large.

When a piece of information available on the internet is misused for a wrongful purpose, it poses a threat to an individual over the safe use of the internet. Today, the security of Cyber Space is quintessential, and without which every information uploaded in cyberspace is jeopardized. The general internet user is quite skeptical while uploading any such information on the internet due to unforeseen misuse of the internet and an increase in the number of cybercrimes.

We all are well aware of the dark web and how it captures most of the insensitive and crucial information of the open space internet [2]. The information available on the dark web is accessible to a few anonymous and private people with a specialized web browser. People behind such creations are elements who make cyberspace unsafe. To curb these activities, a strong policy should be introduced in the International Law, but to a shock, many world governments are also involved in these activities to have an edge over the others by accessing sensitive data of other countries.

In India cyber security is a censorious problem. Today, cyber security in India is at a critical point, and without the integration of cybersecurity into our national agenda nothing can be yielded [3]. Although digitalization, internet-related service, internet economy, and online transactions were at their peak during the COVID-19 pandemic, in a recent report by Indian Computer Emergency Response Team (CERT-In) there were a total of 2.12 lakh cyber security incidents reported in India in just two months of 2022 and a total of 14.02 lakh incident in the year 2021 [4]. This depicts how vulnerable the Indian cyber security system is to cyber attack, threats and crime.

Furthermore, the recent cyber-sabotage of Israeli-based NSO company licensed, Pegasus spyware, military-grade spyware, made news which targeted hundreds of government officials, including opposition party members, journalists, business executives, and human right activist, by hacking their phones through a single tap [5], had led the interference of Supreme Court, where it appointed a technical committee to probe the allegation of unauthorized surveillance [6]. The cyber-attack on such high-level personalities', had outlandish the condition of the general Indian public and raised questions on the spectre of national security.

A US-based private cybersecurity firm has claimed that the Chinese Hacker Group tried to attack India's power grid several times the latest being in the month of March. According to the claim, Chinese hackers reportedly attack seven State Load Dispatch Centres (SLDC) which is near the disputed India-China border [7]. The said hacker group, named Threat Activity Group (TAG) used a family malware called ShadowPad and this group is backed by the Chinese state government and the Chinese Military of State Security. So far, all these cyber-attacks make India look weaker in the International Community and raise the question of National Security.

The IBM Security X-Force Threat Intelligence Report 2022, suggests that the Asian region including Australia; Japan, Australia, and India were the most cyber-attacked countries [8]. All these reports and cyber-attack conclude about the meagre cyber security system in India. India needs a robust cyber security system to safeguard itself against the state-sponsored group and criminal hacking groups from attacking India's cyberspace.

FUNDAMENTAL CONCEPT OF CYBER CRIME IN INDIA

The growth of cyberspace is enormous and it is to be acknowledged that today the Internet is almost in every nook and corner of the world. The new-age technologies and digital media have

brought new values, significance, and even threats into our lives. Additionally, it can now be stated that Cyberspace is a New Living World.

The war-like cry for making India a 'Digital-India' [9], an India where everything becomes digital and accessible to citizens quite easily, is not an easy job. We may focus only on the creamy layer where everything is smooth but the groundwork is missing, and that groundwork is a great cyber security system. New technologies and development will continue to come with every passing day but somewhere or the other protecting this development as well as citizens from any possible threat from these technologies is imperative.

In India, grass-root level people are not well aware of the cyber-attacks and various felonies related to cyberspace, neither our governmental authorities work in a way to provide them with such information which will be useful for them in a long run. In India, some laws state various crimes related to cyberspace for example Indian Penal Code and Information of Technology Act, 2000, but, still general public is unaware of such activities. For that reason, Government is wholly responsible for the protection of every individual from cyber-attacks, threats, and crimes.

Cyber-attacks and threats are not only for active internet users but also for passive internet users, who use the internet for minimalistic things like communication and government digital seva. The information provided for such a cause can even be used for cyber-crimes.

WHAT ARE THE DIFFERENT TYPES OF CYBER-ATTACKS OR THREATS?

As cyberspace has advanced so have the threats to cyberspace. These are some common kinds of cyber-attacks or threats which is posed toward individual and institutions:

- DoS- Denial-of-services
- DDoS- Distributed Denial of Services
- Phishing Attacks
- Malware
- Ransomware
- Viruses
- Password Attack
- SQL Injection Attacks
- MITM Attacks
- Trojan Horse Attack
- XSS Attacks
- Cyber-espionage
- Web Attacks
- URL Interpretation
- DNS Spoofing

These are some known cyber-attacks but it can be said that with the emerging technologies, in the future we might even see some different and more powerful cyber-attacks which may make it even more difficult to share a bit of information in cyberspace.

CYBER CRIMES AND CYBER LAW IN INDIA

Typically, in India, cybercrimes are more prevalent in form of mischief to harass a person or in case of revenge, for example, publishing of obscene acts or information, defamatory messages through electronic mode, etc. India still on average has not seen the high-intensity level of cybercrimes as may be reported in developed countries.

Although, Indian laws have provided specific provisions for punishment against any cybercrime under the Information Technology Act, 2000 and Indian Penal Code, 1860 and also in some particular

acts like Online sale of Arms under Arms Act, 1959 and Online sale of drugs under Narcotic Drug and Psychotropic Substance Act, 1985, yet India don't that stringent punishment which would lead fear in offenders before they commit such an act. This is because India follows the Reformatory Theory which aims at reformation rather than a deterrent. The IT Act, of 2000 is not exhaustive in nature, which makes criminals use loopholes for getting away easily even after committing the offense.

If we draw a comparison between Section 66-B, Section 66-E, and Section 72 of the Information Technology Act, 2000 [10], then it depicts how less we care about violation of the privacy of an individual. In the same manner under Section 66-B dishonestly receiving stolen computer resources has the same quantum of punishment as in case of violation of privacy and both are bailable offenses.

Today, violation of privacy is a substantial issue prevailing in the whole world. It can be seen that bi-annually or annually [11], world governments are coming on a common platform and are holding conferences and seminars to impose strict punishment against any violation of privacy but in India, it is the least important issue.

In the coming decade, when the whole world or at least developed countries and some developing countries would have built a strong ecosystem against violation of cyber laws, India would be way behind, if it doesn't co-operate in a better understanding of the seriousness of these cyber-crimes pose.

Numerous countries especially European countries have different Cyberlaw or cybercrime-related laws which help them identify, lessen the violation, and protect the interest of their country as well as the government from cyber terrorism and cyber espionage which may result in the release of sensitive data in public.

Additionally, if India doesn't have to incorporate a separate cyber law in the coming years, then it should mainly focus on having more strict provisions laid down under Information Technology Act, 2000 and the Indian Penal Code 1860. It will help India in protecting cyberspace overall.

I believe, the quantum of punishment for violation of cyber laws should increase which will pave a way for safe internet use and a cyber environment. Currently, we have to rely mostly on the Supreme Court and High Court's judgment for further development of Cyber Law in India. With a fast-moving economy and development, the cyber law regime is weak to deal with all sorts of cyber security issues. This is a field in which constant change and development should be made keeping in mind how fast the world is evolving. Indian government should at least primarily focus on making the existing cyber law competent enough to fight against all kinds of odds that cyberspace throws on us.

HOW CAN INDIA IMPROVE CYBERSECURITY AND MAKE CYBERSPACE SAFE

- Implement a whole new cyber law.
- Introduce Data Protection Law in Parliament as soon as possible.
- Make stringent punishment for violation of cyber laws.
- Constitute a Central Institute for the implementation of cyber laws.
- Establish a Cyber Law Tribunal for speedy trial of cases related to cyber laws.
- Organise National Conference for awareness of cyber law and safeguard against cyber-crime.
- Enable multi-factor authentication on government websites and ask the private firm for the same.
- Strong Password suggestion on the website only.
- Up-to-date software.
- Protection from identity theft.
- Education regarding cyberspace is a must in schools and colleges

Ultimately, if the Indian government takes all the necessary steps to prevent cybercrimes it is not only safeguarding the government from cyber-attacks and threats but also the public at large. Taking cognizance of all the steps mentioned above it can very well make the mission of 'Digital India' a true success.

CONCLUSION

I would conclude by saying cybersecurity is constantly evolving and with this, there is development in the field of technology which makes it even more important to have secure cyberspace. Intelligent people often misuse their minds to gain upper hand over others by doing such an act which would cause monetary loss to individuals as well as to the economy. India should take cybersecurity on the national agenda since military, scientific research, national missions, economy is somewhat connected to cyberspace, and all these things cannot be jeopardized in any manner. Today, India is becoming a start-up hub in the world, and cybersecurity is imperative for all the new tech companies to make India their base of operation. If India doesn't provide them with a safe working environment, then at some point, they might shift their base outside India.

We should not only aim but also prove to have better cybersecurity to make sure investors invest in New India. Many times, investors pull their money back if they hear news of constant cyber-attacks or threats. The Indian government is solely responsible to provide a robust cybersecurity system in India by introducing National Cyber Security Policy and various rules related to cyber law. That's how we are going to achieve full success in programs like 'Make in India' and 'Digital India'. Also, robust cybersecurity will help us attain peace, harmony, and stability not only nationally but also internationally.

REFERENCES

1. [Ben Tarnoff], [How the internet was invented], [The Guardian], (Jun. 20, 2022, 07:43 PM), <https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf>.
2. [Kaspersky], <https://www.kaspersky.com/resource-center/threats/deep-web> (Jun. 21, 2022, 06:10 AM).
3. [Anmol Mathur], [Cybersecurity: How is India Faring?], [The Economics times], (Jun. 24, 2022, 01:18 PM) <https://economictimes.indiatimes.com/industry/services/education/cybersecurity-how-is-india-faring/articleshow/90092428.cms>.
4. [The Times of India] <https://timesofindia.indiatimes.com/blogs/toi-editorials/another-reminder-that-india-needs-to-invest-more-to-combat-cyber-threats/> (Jun. 24, 2022, 01:48 PM).
5. [The times of India] <https://timesofindia.indiatimes.com/india/pegasus-spyware-used-to-hack-phones-of-journalists-politicians-in-india-report/articleshow/84531126.cms> (Jun. 25, 2022, 03:26 AM).
6. [Ananthakrishnan G], [SC order independent probe into Pegasus, says Govt can't get free every time 'national security' is raised], [The Indian Express], (Jun. 25, 2022, 04:02 AM) <https://indianexpress.com/article/india/supreme-court-pegasus-spyware-surveillance-verdict-7592853/>.
7. [Aryan Prakash], [Chinese hackers' bid to target India's power system near Ladakh blocked: Centre], [Hindustan Times], (Jun. 28, 2022, 09:15 AM) <https://www.hindustantimes.com/india-news/chinese-hackers-bid-to-target-india-s-power-system-near-ladakh-blocked-centre-101649324525345.html>.
8. [IBM Report], [X-force threat Intelligence Index 2022] Rev.3, 37 (2022), <https://www.ibm.com/downloads/cas/ADLMYLAZ>.
9. [Digital India], <https://www.digitalindia.gov.in/> (July. 02, 2022).
10. The Information Technology Act, 2000, § 66-B, 66-E, 72, No. 21, Acts of Parliament, 2000 (India) https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
11. [ICCS 2022], <https://iccs.fordham.edu/event/3531209d-0830-4915-a527-ca09a707d6cb/summary>, (July. 05, 2022).