DE JURE NEXUS LAW JOURNAL

Author:
Abjot Kaur
Punjabi University, Patiala, Punjab
1st Year.

NATIONAL SECURITY ISSUES IN CYBERSPACE

ABSTRACT

In the previous decade, technology has allowed everyone to experience its pinnacle. As a result of the epidemic, there has been a shift from robust security in-premise networking to residential Wi-Fi and personal devices. The hazards associated with malware, Internet protocol modification, hacking, and DDoS, amongst many other things, are typically heightened due to skill gaps and a lack of expertise in the sector. As a result, it is crucial to comprehend the cyber threats that countries all over the world are facing. Almost every piece of equipment in today's society is connected to the internet, and there is a good probability that it will be hacked. Today, there are many new criminal activities that take place in cyberspace, where cyber criminals commit cybercrime from anywhere in the world. Nowadays, cyber-crime is usually used to obtain sensitive information or to commit financial crimes.

There is currently a plethora of cyber acts available to aid in the fight against cybercrime. There is a lot of international collaboration between countries to combat cybercrime, including seminars, joint workshops, and other activities. These factors aid nations in the development of their cyber-security teams and the creation of a more secure cyberspace for their individual countries.

KEYWORDS

Cyberspace, Cybersecurity, Technology, Cyber Crime, Network, Hacking, Cyber Acts

INTRODUCTION

As a result of technical breakthroughs, the world has altered tremendously. Through various social networking sites, the Internet has made various things significantly easier for us, whether it be communication or access to information. While it's amusing how technology can make the globe feel more linked, it also brings with it an obvious evil in the shape of these platforms' susceptibility. We live in the Information Age, where data is as essential as breathing. This information era revolves in the arms of Cyberspace, a virtual realm created by humans. However, while it has permitted easy access, it has also posed security dangers to vital, public, and defence infrastructure in the form of numerous forms of malware. Previously, the fear was that a simple virus would slow down the system's efficiency, but this has evolved into extremely sophisticated software that may inflict major devastation not only to the system, but also to human people and the nation's security.

Cybercrime is actually making headlines around the world, inflicting havoc on companies and organizations. The most prevalent sorts of cyber theft are security breaches, identity fraud, monetary fraud, and online time theft. Despite the fact that cybersecurity is improving every day, hackers are continuously upping their game and finding new ways to get around it. This emphasises the importance of not only better cybersecurity technology but also strong cyber legislation. To minimize cybercrime and hackers' attempts, officials must be informed of any cybersecurity holes and correct them in actual time. To address the mounting risks around the nation, consistent efforts and constant attention are essential. The financial, bureaucratic, defence, public service, and social infrastructures of a country determine its well-being, and this infrastructure is completely reliant on the internet in the modern period. It is now obligatory to secure cyberspace in order to preserve national security, as cyberspace protection is no longer an option, but rather a need.

CYBER WARFARE

There is no universally accepted definition of the phrase "cyber warfare" as such but it has been used interchangeably with the term "cyber-attack." Cyber warfare is defined as a network-based battle in which technology is used to disrupt a certain state's activity. With the explicit objective of assaulting information networks for strategic or military purposes, of a state. The

damage might take several forms, including targeting the country's significant infrastructure, such as its major dams, disrupting transportation by disabling time systems, or targeting the country's communication system, all of which would certainly cause mayhem. Phishing, virus assaults, denial of service attacks, and are some of the prevalent types of cyber-attacks.

The assaults could be carried out by a state or even certain international organizations with the goal of harming and damaging the digital infrastructure of the other country. The primary goal of such attacks is to degrade the adversary's digital infrastructure, causing harm and disruption throughout the region/state. In 1998, the Tamil Tigers, a group of Tamil militants, "sent over 800 e-mails to Sri Lankan embassies - We are the Internet Black Tigers, and we're doing this to interrupt your communications," the emails said. It was the first known terrorist strike on a country's computer networks, according to intelligence officials.

Malicious code or rationale is used to change the genuine data files in order to carry out a cyber-attack. As a result, data will be exposed. Documentation and identity theft are among the consequences of compromised data, as are deception, exploitation, malware, distributed denial of service, hardware theft, and intellectual property theft, etc.

TYPES OF CYBER ATTACK

Warfare is no longer waged with troops, weapons, and missiles; instead, warfare is all about information or data strangling. Financial frauds, extortion, stealing infringing content, unlawful obscene subject matter, virus attacks, cyberbullying, and racial violence targeting minorities and LGBTQ community are all examples of these types of attacks. Cyber-attacks primarily target information or data on a number of systems, including financial institution sites, journalism and media websites, army agency websites, and official websites.

An interruption of the legitimacy or security of information or data is what a network assault or cyber-attack is all about. During the hacking procedure, insecure systems and systems with insufficient security protocols are inspected. After the hacking is completed, the compromised system operates as a spy and affects the networks of other devices. It can be controlled remotely by the attacker, and orders can be sent to it.

There are three main categories of attack[1]:

- **Volume-based Attacks**: This type attacks use high traffic to inundate(flood) the network bandwidth.
- **Protocol Attacks**: These attacks focus on exploiting server resources.
- **Application Attacks**: Application attacks are considered to be most sophisticated types of attacks and focus on web applications and are the most serious type of attacks.

CYBER SECURITY

Cyber security is a technique for preventing unwanted exposure and vulnerabilities to computers, networks, applications, and personal information. It is the process of safeguarding and defending data as well as other communication devices against unwanted access, modification, or exploitation. It covers methods for safeguarding systems, networks, programmes, and preventing unauthorized access or assaults that could harm or damage them in any manner. In essence, cyber security is a technological technique to protect systems from these kinds of threats.

SIGNIFICANCE OF CYBER SECURITY

- Cyber security recognizes all of a digital system's or program's weaknesses and dangers.
- It determines the root source of such flaws, corrects the flaws and dangers, and protects the network.
- It works to ensure that the Enterprise security attributes are realized and preserved.
- Individuals' possessions are safeguarded against a variety of cyber security threats and stay unharmed.
- Authenticity, privacy, and accessibility are all maintained.
- The necessity of safeguarding networks, servers, and programmed from assaults, harm, and unauthorized access is comparable to an institution's regular tasks.

ELEMENTS OF CYBER SECURITY

Encounters with data systems have a susceptibility that can be easily exposed to launch a

[1] Available at URL : https://www.esecurityplanet.com/networks/types-of-ddos-attacks/ accessed on 19/01/2022

devastating cyber attack. Various features are required for a robust cybersecurity system. Hereunder are the components[2] :

- **Application Security:** Users, their data, and their interests are all protected by web application security. Application security assists in defeating any attempts to circumvent the permission constraints specified by the software system or program's security regulations.
- **Information Security:** Information security refers to the protection of critical material from unauthorized access, use, or harm of any type. Privacy, authenticity, and accessibility are the properties that define information security.
- **Network Security:** The goal of network security is to keep the network and data usable and reliable. A network penetration test is used to evaluate a system's and network's vulnerabilities.
- **Business continuity planning:** Business continuity planning (BCP), also known as disaster recovery, is about being ready for any type of interruption or cyber threat by quickly assessing hazards to devices and understanding how they might affect operations and countermeasures.
- **Operational security (OPSEC):** Operations security is a term used to describe how an organization's operations are protected. It locates critical information and resources in order to hunt down risks and weaknesses in the befitting manner.
- **End-user education:** As operator error is among the leading causes of data theft, it is critical for businesses to educate their personnel on cyber security. Every individual should understand the most frequent cyber dangers and be able to respond to them.

CYBER SECURITY: INDIA'S SITUATION

While discussing the Indian situation, we must include cyberterrorism in particular. Because India has the world's second-largest viewership, cyber-threats are also significant. Contributing to the danger, India is bordered by regional rivals such as Pakistan, China, and Bangladesh, all of whom actively support and promote terror groups from all over the world in an attempt to destabilize the country. Since Indians have such a significant online presence, they are sadly

[2] Available at URL : http://www.crossdomainsolutions.com/cyber-security/elements/ , accessed on 19/01/2022

more susceptible to cybersecurity attacks due to their lack of awareness about cybersecurity and its defense.

Mr. Shringla Foreign Secretary of India, speaking during a UNSC debate on "Maintenance of International Peace and Security: Cyber Security," identified concerns for global Internet networks by saying that "Some States are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism". Other problems, he noted, include terrorists' use of cyberspace to "spread virulent propaganda, inspire hatred and violence, recruit youth, and raise funds," along with nations' and terrorists' capacity to enter networks.[3]

Cyberterrorism poses a significant threat to national security since it is the only tool capable of attacking a nation's emotional, social, governmental, and economical health in a single tap. Cyberterrorism efforts and attacks have increased dramatically in recent years, likely to take the form of dangers to the country's essential services, including nuclear programs, military amenities, financial sector facilities, and local distribution infrastructure.

Terrorists no longer require a geographical venue to educate and hire people to carry out their heinous intentions; instead, they can simply snoop into cyberspace and abuse the countries' monetary, political, military, security, and government infrastructure functions. Mr. Ajit Doval, India's national security advisor, recently claimed "the next generation war will be a civil society battle that will take place in cyberspace".

India's cyber-intelligence capabilities seem to be limited. For such a greater level of cyber situational awareness and to assist it create a larger scope of its own in the coming, it usually relies on cooperation with the United States, the United Kingdom, and France. A robust start-up ecosystem and a vast skilled workforce are two of the digital economy's assets. In boosting national cyber security, the private sector has gone ahead of the government.

To keep a watch on social networks in India, cybersecurity experts have proposed the develo pment of an independent regulatory organisation similar to the Securities and Exchange Boar

[3] Available at : https://www.thehindu.com/news/national/some-states-using-cyberspace-skill-to-execute-cross-border-terror-shringla/article35040491.ece ,accessed on 19/01/2022

d of India (SEBI) and the Telecom Regulatory Authority of India (TRAI).

The independent organisation should be given the authority to respond on a daily basis and to impose graduated penalties for violations of cyber regulations[4]

CAUSES OF CYBER INSECURITY

There are various sources of insecurity in cyberspace. Some causes of cyber insecurity are as follows:

- **Spy organizations:** In order to gain information, records, sites, and useful insights, spy agencies deploy surveillance methods. Cyber espionage resources are sometimes exploited for destruction, and the undetectable aspect of these actions, as well as the regulatory issues, make them perfect for intelligence agencies. They utilize malware as a weapon, and espionage has become a two-sided issue: legitimate for one nation and immoral and unlawful for another whose assets are manipulated with or stolen.
- **Hacktivists:** In this era in today's time political PR management has taken over all over the world and some groups get paid for politically charged cyber-attacks on opponents, they dump email servers with thousands of mails and try to strangulate mail delivery algorithms and they also hack into websites of opponents to flood it with political texts and messages.
- **Frustrated Individuals:** Individuals' major source of Computer infractions is the disgruntled internal operating from within an organization. They might not even need a great deal of information regarding computer outages because their knowledge of a disaster system enables them to gain unrestricted access to the system in order to damage it or steal data from it.
- **Terrorists and criminal organizations:** Cyber methods are used by criminal organizations and terrorists' groups for hiring, coaching, and funding unlawful things. Online rings such as drug mafias, arms deals, and trafficking are common, and profound frauds and personal photos and equipment have recently been formed for fraud.

GLOBAL CYBER SECURITY INDEX(GCI)[5]

[4] Available at : https://www.thehindu.com/news/national/kerala/regulatory-authority-for-cyberspace-demanded/article37461255.ece accessed on 19/01/2022

[5] Referred from : https://m.economictimes.com/news/defence/india-breaks-into-top-10-countries-on-uns-index-measuring-commitment-to-cybersecurity/articleshow/83962167.cms accessed on 19/01/2022

The GCI is a reliable indicator of a country's engagement to cybersecurity on a worldwide scale. India has been rated 10th in the Global Cyber Security Index (GCI) 2020 by the United Nations' specialized body for information and communication technologies, the International Telecommunication Union (ITU).

India has jumped from 47th rank in the previous edition of the ranking to join nations such as the United States, the United Kingdom, France, Singapore, and Russia in the top ten. China and Pakistan, which are neighbors, were placed 33 and 79, respectively. India's ranking of 10th is a substantial improvement over the index's previous edition, published in 2018, when it was rated 47th. Since the outbreak of the epidemic, India has seen an increase in cyber-attacks. To establish an overall score, India and other countries were assessed based on five pillars: legal, technical, organizational, capacity development, and cooperation. Twenty indicators were measured by asking the countries 82 questions. India received a 97.49 out of 100.

CYBER ATTACKS FACED BY INDIA

Cyberspace and cyber-attacks both are progressing at the same rate all over the world. Recently in Jan,2022 Ukrainian government websites faced cyber-attack amid tensions with Russia. During the period of coronavirus-induced lockdown, India was subjected to heightened cyber-attacks from foreign countries, particularly China and Pakistan. India has faced various cyber-attacks. Some of the cyber-attacks that India had to face are as under:

KUDANKULAM NUCLEAR PLANT CYBER ATTACK[6]

India presently has eight nuclear-capable reactors in operation, the largest of which is the Kudankulam nuclear plant. India's largest nuclear reactor, Kudankulam, installed with two Russian designed and supplied Water-Water Energy Reactors has already been the target of a cyber-attack in 2019.There was no critical damage caused by the blow.The parent corporation, Nuclear Power Corporation of India Limited (NPCIL), admitted to a security compromise within 24 hours. KNPP was targeted by malware, according to the NPCIL statement, which was discovered by the Indian Computer Emergency Response Team (CERT-In). According to

[6] Available at: https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf accessed on 19/01/2022

the Department of Atomic Energy's (DAE) investigation, the malware infected a user's personal computer that was connected to an internet-connected network for administrative functions.

AIR INDIA DATA BREACH

Travelers' private information was leaked as a consequence of a hack on the systems of airline data service provider SITA. Between August 2011 and February 2021, when SITA notified the airline, the information was collected. Singapore Airlines, Lufthansa, Malaysia Airlines, and Cathay Pacific were all impacted by the cyber-attack on SITA's passenger service system.

COSMOS BANK CYBER ATTACK IN PUNE

Cosmos Bank in Pune was the target of a recent cyber assault in India in 2018. When hackers stole Rs. 94.42 crores from Cosmos Cooperative Bank Ltd. in Pune, it shocked the entire banking sector in India. Hackers gained access to the bank's ATM server and stole the personal information of a large number of visa and rupee debit cardholders. Money was wiped out, and cyber gangs from as many as 28 nations withdrew the funds immediately, they were notified.

IMPORTANT CYBER LAWS IN INDIA

Cyber security is a problem for every government in the world, even our own. India is particularly vulnerable to cyber security threats, and it is vital that it takes full responsibility for these. There are various provisions in law in India for cyber security and also schemes and policies are formulated by the government for protecting cyberspace. When it comes to cybersecurity, there are four main laws to consider in India.

- **Information Technology Act, 2000**[7]

  The Information Technology Act of 2000 addresses a variety of new era

[7] Referred from: https://www.infosecawareness.in/cyber-laws-of-india accessed on 19/01/2022

offences that have arisen as a result of digital exploitation**.**

These are some of its components that aim to empower Web users while also seeking to defend cyberspace**.**

- *Section 43A* deals with data protection at corporate level.
- *Section 65* deals with the tampering of digital files.
- *Section 66* deals with using the password of others.
- *Section 66D* deals with fraud using digital resources.
- *Section 66E* deals with publishing personal photos of other people.
- *Section 66F* deals with acts of cyber terrorism.
- *Section 67* deals with *publishing* child pornography.
- *Section 69* deals with the power of the government to block the internet sites.

- **Indian Penal Code (IPC) 1980[8]:**

  The IPC's main section on cyber scams is as follows:

  - Forgery (Section 464)
  - Forgery pre-planned for cheating (Section 468)
  - False documentation (Section 465)
  - To represent a morphed files as original (Section 471)
  - Damage of Reputation (Section 469)

- **Companies Act of 2013[9]:**

  The Companies Act of 2013 gave the SFIO (Serious Frauds Investigation Office) the authority to prosecute Indian corporations and their directors.

  SFIOs have also become much more proactive and harsh in this area after the notificat ion of the Companies Inspection, Investment, and Inquiry Rules, 2014. All regulatory compliances, especially cyber forensics, e-discovery, and cybersecurity diligence, are well-covered by the legislature. The Companies (Management and Administration) Rules, 2014 establishes tight requirements for corporate directors and executives in terms of cyber security commitments.

- **NIST Compliance[10]:**

[8] Available at: https://www.appknox.com/blog/cybersecurity-laws-in-india accessed on 19/01/2022
[9] Supra Note 8
[10] Supra Note 8

As the most trusted global certified organization, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS), which provides a standardized security strategy.

CONCLUSION

On a worldwide scale, cyber law is still in its early stages of development. Its development necessitates a favorable atmosphere. To deal with the difficulties linked with cyber jurisdiction, international cooperation is critical. For better application of cyber laws, there must be consistency between national and international rules. Shri Narendra Modi, India's Prime Minister, has long advocated for a "Computerized India". But there is also a rapid increase in cybercrimes. In the first half of 2021, the nation saw over 6.07 lakh cyber security breaches. The Internet has no boundaries, and the attackers can fulfill their motives while sitting in different corners of the world. There are gaps in the law, thus globally binding laws are needed to be formulated to tackle cyber warfare.