Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cyber Terrorism: A Threat to Human Society

Samprity Halder[a]

[a]Hazra Law College, Kolkata, India

Received 17 August 2022; *Accepted* 04 September 2022; *Published* 10 September 2022

Technology in cyberspace has created varied options to commit crimes by dismantling the mechanization to initiate nefarious cyber-attacks. The identity of cyber terrorists is morphed by using fake identities to target any particular individual or any organization for their willful gain. In times of pandemic, cases of cyber-attacks reached the peak point as there were plenty of users working by, attackers fetched several tricks to demolish the functioning of the device and cripple the user by enforcing financial frauds. These kinds of cyber-attacks are affordable, suitable, and contactless, and low levels of risk factors are involved where the attacker is undetectable in the domain of telecommunications. The concept of cybersecurity is frustrating in view of Cyberterrorism. Indian society witnessed heinous attacks which violated several legislations preventing Cybercrime as well as several sections of the Indian Penal Code; however, the Government formulated strategies and policies to liquidate these offences. The UN is in a continuous motion to eliminate cyber terrorism in the global arena emancipating conventions, declarations, policies, and strategies directing nations to follow up the approach, while the EU and UK have designed strategies to strengthen their digital infrastructure. In this research paper, the author has pointed out several factors to combat cyber terrorism, clearly analyzed the structure of cyber hacking, and critical explanation of digital terrorism in the 21st century. The mental framework is slowly decaying by means of tremendous mental agony leading a miserable life and finding effective norms for sustaining a healthy life.

Keywords: *mechanization, nefarious, cybersecurity, cyberterrorism, domain, telecommunications, cyber hacking.*

INTRODUCTION

An indispensable form of attack with the illegal use of technology to steal information by raising conflicts among ministerial bodies and the general public. It endangers millions of people with "technological disability" and also weakens the IT structure to haul programming disruptions, the inability to perform legitimate tasks, and integrates social unrest. The Prime Minister, President, Chief Ministers, journalists, politicians, judges, military, and social activists are the prime targets of cyber terrorists who could easily break the technical algorithm where the data is stored. These cyber hackers work with such sophisticated technology that they are well aware of the nefarious concept of hacking the information in which no proof is discovered of the leaked information Cyber experts are however astonished and puzzled to find out possible measures to prevent malicious cyber-attacks.

The ignorant masses are not much aware of technology-based crimes such as *cyberbullying, cyber fraud, cyber stalking, cyber warfare, and cyber harassment*. Upon broadcasting the news on Television, social media, radios, and news channels, the public gets an edge to discuss the issue with varying opinions. In fact, the opposition parties in a democratic setup criticize the existing government by questioning the viability of internal security and the reasons for the failure to perform tasks by cyber experts. When an attack is violent in nature due to political instigation and the victim suffers from cyber threats either of physical or financial fraud. The destruction must be reasonably considered as an impact of cyber terrorism which can cause physical harm or spontaneous disruption of infrastructural belongings[1]. As technology is advancing and modifying with the help of artificial intelligence (AI) it is much easier for cyber terrorists to hack computer servers, delete relevant information from websites, password hacking, spamming emails, manipulate data, and seizure of bank accounts of general people. All these consequences of cyber-attacks have a tremendous effect on the social, economic, and psychological crisis in people's lives which dooms to be more vulnerable in recent years and the instances to lead a

[1] Robert Sheldon & Katie Terell Hanna , 'Cyberterrorism' (*TechTarget,* 19 Jan 2022) <https://www-techtarget-com.cdn.ampproject.org/v/s/www.techtarget.com/searchsecurity/definition/cyberterrorism?amp=1&amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_tf=From%20%251%24s&aoh=16594430671714&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.techtarget.com%2Fsearchsecurity%2Fdefinition%2Fcyberterrorism> accessed 02 August 2022

good and healthy life however captivated in the cage of cyber terrorism. Society needs to bear with every single cyber-attack unless they are fully exhausted and tired of combating e-criminals.

OVERVIEW OF CYBER TERRORISM IN INDIA

The poisonous roots of cyber terrorism were found in the 1990s with the emergence of information technology and internet services. With the advent of technological outlook, it has emerged into massive inventions of human-like robots, high-powered nuclear missiles, superfast bullet trains, single tap payments, etc. with degradation in technological lagging of cyber threats and attacks which have increased over the years and cybercrime was recognized as "*arms race of the 21st century*" with the occurrence of vulnerable electronic exploitations[2]. Indian Government thus consulted with Cyber experts to drill down the implementation of developments, strategies, and effective measures to be more cautious of cyberinfrastructure[3]. Ministry of Home Affairs (MHA) launched The Indian Cyber Crime Coordination Centre (IC4) for combating cybercrime and cyber terrorism. India's cybernetic technology is much weaker than countries like China, and Japan has well-advanced and furnished inventions with huge economic support.[4] Need for adopting hi-tech inventions to be equipped with the cyber giants and proper evaluation to tackle dangerous attacks. India ranked 12th on the Global Terrorism Index (GTI) among 163 countries in 2021.

[2] Yashasvi Yadav, 'Fighting cybercrime: How almost everything is under threat' (*Times of India,* 31 January 2022) <https://timesofindia-indiatimes-com.cdn.ampproject.org/v/s/timesofindia.indiatimes.com/blogs/voices/fighting-cybercrime-how-almost-everything-is-underthreat/?amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_tf=From%20%251%24s&aoh=16594529973397&csi=1&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Ftimesofindia.indiatimes.com%2Fblogs%2Fvoices%2Ffighting-cybercrime-how-almost-everything-is-under-threat%2F> accessed 02 August 2022

[3] Shiv Raman & Nidhi Sharma, 'Cyber Terrorism in India : A Physical Reality or Virtual Myth' (2019) 5(2) Indian J Law Hum Rev 133

[4] *Ibid*

INDIA HAS ADOPTED CERTAIN LEGISLATIONS TO SUPERVISE CYBER LAWS

Information and Technology Act, 2000: It deals with the storage of information, electronic governance related to communication, and regulation of certification. It also grants penalties for misrepresentation and breaches according to this Act[5].

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[6]: It protects every single data and sensitive information to maintain the secrecy of individuals which is bonded by the constitutional provision Right to Privacy under Article 21 of the Indian Constitution[7].

The Information Technology (Guidelines for Cyber Cafe) Rules, 2011[8]: The internet provided at cybercafés must register to the guidelines mandated under this Act. It should also maintain a record of the user's identity, the data limit used by the user, and for what purpose it has been used.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules 2021[9]: This Act came into being to regulate the privacy of the users, inform users about actions regarding non-compliance with rules and regulations, instruct users not to install any technical configuration, and also report cyber security incidents in accordance with the Information Technology Act.[10]

Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties), Rules 2013[11]: CERT is an agency of computer experts who provide protection against any cyber threats, any loss or dissemination of information, support

[5] Information Technology Act 2000

[6] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

[7] Vinod Joseph & Ors, 'A Review Of The Information Technology Rules, 2011' (*Mondaq*, 19 March 2020) <https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-> accessed 03 August 2022

[8] Information Technology (Guidelines for Cyber Cafe) Rules 2011

[9] Bhumika Indulia, 'The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules 2021' (*SCC Online*, 26 May 2021) <https://www.scconline.com/blog/post/2021/05/26/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-2/> accessed 03 August 2022

[10] *Ibid*

[11] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013

for the protection of databases, and also aimed to provide high-security functioning. It builds configuration in the system and ensures internal and external protective tools against current threats. Spontaneous support is provided to safeguard the economy, law, industry, communication, and defence[12].

Indian Penal Code, 1860: The Indian Penal Code (IPC) enshrines cybercrimes under certain Section 379[13], 354C[14], 354D[15] , etc which include hijacking of stolen devices, stolen data, voyeurism, stalking, and other grievous offences resulting n imprisonment or fine or both.

The inductive growth of Cyber-attacks has tremendously increased while in recent years it is seen every single day thousands of people are being attacked by cyber attackers. According to NCRB, In 2016 India registered, 12317 cases and in 2020 it increased to 50035; it means India recorded 136 cybercrime cases per day[16]. A rise of 3.3% in 2019 and 3.7% of cases were recorded in NCRB data[17]. A maximum of 60.2% of cub cyberbullying cases were recorded in 2020 according to the data Of the Ministry of Home Affairs, with a sharp rise in data in 6.6% cases of sexual exploitation and 4.9% of extortion. The state of Uttar Pradesh followed by Karnataka registered undoubtedly a sharp increase in cybercrime over 50 thousand cases[18]; [16.2%] of cases were in favour of Karnataka, Telangana with [13.4%] of an upsurge of cases, Assam [10.1%] and Maharashtra records [4.4%] in the country[19]. 842 cases of online offences, among which 738 were

[12] Peter Sullivan, 'Computer Emergency Response Team (CERT)' *(Tech Target* , 18 March 2021) <https://www-techtarget-com.cdn.ampproject.org/v/s/www.techtarget.com/whatis/definition/CERT-Computer-Emergency-ReadinessTeam?amp=1&amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_tf=From%20%251%24s&aoh=16606223299956&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.techtarget.com%2Fwhatis%2Fdefinition%2FCERT-Computer-Emergency-Readiness-Team> accessed 03 August 2022

[13] Information Technology Act 2000, s 379

[14] Information Technology Act 2000, s 354C

[15] Information Technology Act 2000, s 354D

[16] IndiaSpend , 'India registered 136 cybercrime cases every day in 2020: NCRB data' (*Business Standard,* February 2021) <https://wap-business--standard-com.cdn.ampproject.org/v/s/wap.business-standard.com/article-amp/current-affairs/india-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007_1.html?amp_js_v=a6&amp_gsa=1&usqp=mq331AQKKAFQArABIIACAw%3D%3D#aoh=16595444489734&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s&ampshare=https%3A%2F%2Fwww.business-standard.com%2Farticle%2Fcurrent-affairs%2Findia-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007_1.html> accessed 03 August 2022

[17] *Ibid*

[18] *Ibid*

[19] *Ibid*

only about transmitting sexual pictures, the discourse led The Ministry of Women and Child Development (MWCD) to address several preventive measures to protect society against cyberbullying, sexting, child pornography, and objects related to sexual abuse of children[20].

VARIOUS CASES OF CYBER ATTACKS THAT SHOOK EVERY NOOK AND CORNER OF INDIA ARE AS FOLLOWS

26/11 attack: India witnessed a terrific cyber-attack on 26th November 2008 in Mumbai's Taj Hotel. The Pakistani terrorists hijacked the computer systems of the Taj Hotel, Leopal Café, Shivaji Maharaja Terminus, and other places. After having access to all information and people being targeted, the blast occurred in which Pakistani terrorists are linked to hackers at every point in time. This incident shook the Indian Government that cyber security needs to be stronger.

Ahmedabad Bomb Blast: A severe bomb blast took place on 26th July 2008 injuring 70 people. The terror group named Indian Mujahedeen Islamic Militant Group warned the news agencies by spamming emails and threatening the CM of Maharashtra residents of Gujarat and Businessman Mukesh Ambani. The blast was so intense and heinous that every citizen today also dared to believe it.

UIDAI Aadhaar Software Hacked: A massive breach of data of about 1.1 billion Aadhaar holders in 2018. The hackers leaked Aadhaar Card numbers, bank accounts, IFSC codes, and personal information on forums so that everyone could see others' details.[21] The whole cyber security mechanism failed to perform its operation while the sellers engaged in illegal activities of sharing information with any person by charging rates.[22]

CASES LAWS

Shreya Singhal v Union of India [23]

[20] *Ibid*

[21] Kratikal, '5 Biggest Cyber Attacks in India' *(Kratikal Blogs,* 1 November 2019) <https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/> accessed 04 August 2022

[22] *Ibid*

[23] *Shreya Singhal v Union of India* AIR 2015 SC 1523

Two women have been arrested for offensive comments on Facebook and made liable under Section 66A[24] of the Information Technology Act which held that the use of any sources of communication, consisting of offensive data, inconvenient, worrying, incites fear or maliciousness. However, it clearly challenges the constitutional validity of freedom of speech and expression and proved a violation of Article 14[25] of the Constitution. The Supreme Court held that Section 66A may restrict any form of communication with a mere chance of advocacy or discussion of a particular issue that intends to be offensive and cause public disorder. Section 66A condemned abusive language that could annoy people but does not affect the reputation of the people at large. The Apex Court struck down the restrictions relating to the speech delivered in online mode, thereafter violating freedom of speech under Article 19(1)(a)[26] of the Constitution. It marked a clear distinction between the information delivered by electronic communication and information transmitted by other means forms of speech that actually safeguarded Article 14 of the Indian Constitution.

Avinash Bajaj v State (NCT) of Delhi[27]

Avinash Bajaj the CEO of the Bazee.com website deals with sale commissions and makes money from advertisements was arrested under Section 67[28] of the Information Technology Act, 2000 for broadcasting cyber pornography on the website. The Court held that Bazee.com was not the platform for viewing pornography but gathering content indicates cybercrimes attributed to others other than Bazee.com. The defendant bears only a service provider but not because of the content. The analysis confirms that no clippings of porn are available on the Bazee.com portal. The suspected crime can be determined and protected from unauthorized access, no specific evidence was found that pornographic content is unintentionally put on the website for financial gain. The website was itself in a situation to close its loopholes that were discovered selling pornographic content creators.[29]

[24] Information Technology Act 2000, s 66A
[25] Constitution of India, art 14
[26] Constitution of India, art 19(1)(a)
[27] *Avinash Bajaj v State (NCT) of Delhi* (2008) 150 DLT 769
[28] Information Technology Act 2000, s 67
[29] *Ibid*

Hakkam v State of Kerala

A text message was received by the Sub Inspector of Ernakulam Town North Police Station from the mobile number of the accused which reads *"we will blast bombs in different parts of Kerala in 28 hours, all bombs will blast"* the crime was registered under Section 66(F)[30] of Information Technology and also Section 506 of the Indian Penal Code. Through the message of the petitioner, it amounts to the offence of cyber terrorism inciting fear and terror amongst the general public.[31] The High Court of Kerala held that the petitioner shall furnish an assurance of Rs. 1,00,000/- with two solvent sureties, the petitioner shall report to the Investigating Office every two months until the last report of the case is filed and the petitioner shall make him accessible whenever needed in any kind of interrogation by the Investigating Officer.

Nasscom v Ajay Sood & Others [32]

Nasscom is a premier software association where the defendants served as a placement agency involved in recruitment. To make hold of personal data, the defendants sent emails to third parties in the name of Nasscom and used the trademark name illegally; misrepresenting on behalf of the software company.[33] The Court held the concept of phishing laid down a benchmark in India's legislation and penalized phishing in terms of misrepresenting the trademark and the origin of the email causing grievous harm not only to the customer but also to whose name the private data and passwords were breached. It was also held that phishing is an act to tarnish the plaintiff's privacy as it is an effective asset.

It is, however, analyzed, that phishing is a type of internet fraud where passwords, emails, and personal data are misrepresented by any third party for the benefit of an illegitimate party. For example- common phishing scams include bank frauds, disclosing a person's identity, sharing of OTPs, and sharing of other confidential information violating Intellectual Property rights.

[30] Information Technology Act 2000, s 66F

[31] *Ibid*

[32] *National Association of Software and Service Companies v Ajay Sood & Ors* 119 (2005) DLT 596

[33] *Ibid*

INTERNATIONAL OUTLOOK OF CYBER TERRORISM

Cyber Terrorism is a worldwide threat to millions of people living around the globe. With the increasing trend of computer networks and the internet, the sustainability of cyberspace has fared well in the long run. The introduction of 'information and communication technology (ICT), 'virtual private networks (VPNs), and 'internet protocol (IP) have glanced at the technological phenomenon. Digital surveillance has a wider aspect in terms of 'international law' and 'foreign security' which pervades the prospects of 'digital rights to the users, by weakening the mechanism through 'authoritative regimes', 'repression', and 'criticizing the domain' which ultimately gets diverted in the international policy. Discussions related to cyber terrorism are held up by the United Nations Group of Governmental Experts (UN GGE) for administering the developments in Information and Technology; another organization UN Open Ended Working Group (OWEG) was introduced for providing information security in cyberspace.[34]

The UN Charter in the fundamental principles has agreed to protect the rights of individuals with a conscience to *humanity, peace, mankind, sovereignty, determination, and reference* to the implications related to international law and the cyber domain. The international rules and principles are adhered to in consideration with International Humanitarian Law (IHL) in compliance with cyber-specific operations. The approach which enables quantitative or qualitative analysis of intervention with raising violations of cyber activity had to result in legal consequences.[35] The vulnerability and conceivably of the germane phenomenon with a view to determining the fundamental data is breached and the attack caused by which State to design its technicality of the framework on which it is based upon, attributing to protection from the harmful and erroneous threshold with issues from international community guidelines.[36]

[34] Denis Broeders & Ors, 'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy' (*Taylor & Francis Group*, 2 June 2021) <https://www.tandfonline.com/doi/full/10.1080/1057610X.2021.1928887> accessed 04 August 2022

[35] *Ibid*

[36] Macro Benatar, 'Cyber Warfare' (*Oxford Bibliographies*, 2014) <https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0087.xml> accessed 04 August 2022

According to Cisco, 'data distributed denial-of-service (DDoS) attacks in 2020 with 'NETSCOUT Threat' reports 4.83 million attacks which all 26,000 attacks per day; according to Verizon's 2020 Data Breach Investigations Report (DBIR) attacks rose to 86% in 2020[37] ; 36 million data have been leaked in the initial months of 2020.[38] The U.S. Healthcare Cyber Security Market 2020 recorded that more than 90% of healthcare organizations[39] have faced the crisis of data breaching[40]. A report by INTERPOL indicates that alarming rates of spam messages,[41] malicious malware, and malicious domain all resulted due to COVID-19 which poses a threat to the arena of cyber-centric operations.[42]

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19" – Jurgen Stock. The Cyberthreat Defence Report (CDR) indicates that 89.7% of U.S. organizations experienced terror within a year. The cyber-attacks from the Centre for Strategic and International Studies (CSIS) were first analyzed by Specops Software. The government hub 'National Cyber Investigative Joint Task Force (NCIJTF) leads the force with cyber threat agencies and performs operations for sanctioning a smooth manner of cyber control in true hands. The U.S. Commission on the appraisal of Critical Infrastructure held cyber-terrorist targets on banks, military, and power plants and caused damage to air traffic[43]. The assessment of the Cyber Security and Infrastructure Security Agency (CISA) according to the Russian Government intended that cyber offences are aligned to suppress the political phenomenon and issues related to cyber espionage.[44] Iranian cyber army engages superior technologies to boldly defeat cyber warfare with the effect of independent hackers and strategies to tighten over the cyber tension;

[37] John Maddison, 'Cybersecurity Statistics' *(Fortinet,* 18 February 2022) <https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics> accessed 04 August 2022

[38] *Ibid*

[39] *Ibid*

[40] 'Data breaches have lasting financial effects on hospitals , report suggests' *(Hannah Mitchell)* <https://www.beckershospitalreview.com/cybersecurity/data-breaches-have-lasting-financial-effects-on-hospitals-report-suggests.html> accessed 04 August 2022

[41] *Ibid*

[42] 'INTERPOL report showing alarming rate of cyberattacks during COVID-19' (*Interpol*) <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19> accessed 4 August 2022

[43] 'What We Investigate' (*FBI*) <https://www.fbi.gov/investigate/cyber> accessed 04 August 2022

[44] *Ibid*

several website attacks have been rescinded, as Mowjcamp, MOBY Group[45]. EU and the European External Action Service (EEAS) enhancing reliable services of cyber security and also rendering strategies for 'digital resiliency' to protect against cyber threats,[46] safeguards communication, data quantum encryption, and ensure functioning policy.[47]

International Organizations combat cyber threats by highlighting the nation's effective security and incorporating policy reforms with the intent of defending the brutal attacks which terrify the country's internal security. Treaties are signed hereby with international cyber security organizations to affirm the multilateral ratification of policies. Contingency for formulating attacks by cyber terrorists needs an overall revolution with mitigating forces of swaying experts to tackle the risky situation by not affecting the nation's policy. The misuse of infrastructural potentialities should be taken into account to restore the difficulties in terror attacks.[48]

***Several cases of Cyber terrorism and Cyber-attacks which shook human society are as follows*:**

- The deadly WannaCry ransomware attack affected enormous computers worldwide and disabled the Microsoft Windows operating system, a hacker group named The Shadow Brokers had stolen the Windows System[49].
- In 2021, the Health Service Executive ransomware attack on Ireland the technical activities were shut down, hospital evictions, medical data breached, patient's health records were breached, and hospital accounts were wiped off; the hacker gang named Wizard Spider attacked the Health Department.

[45] 'History of Iranian Cyber Attacks and Incidents' (*United Against the Nuclear Iran*) <https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents#> accessed 04 August 2022

[46] *Ibid*

[47] Ben Flanagan, 'Former CIA chief speaks out on Iran Stuxnet attack' *(The National News,* 15 December 2011) <https://www.thenationalnews.com/business/former-cia-chief-speaks-out-on-iran-stuxnet-attack-1.392917> accessed 06 August 2022

[48] *Ibid*

[49] Sama Al-Kurdi, 'The 10Biggest Cyber Attacks in History' *(Albawaba,* 26 June 2021) <https://www-albawaba-com.cdn.ampproject.org/v/s/www.albawaba.com/amp/business/10-biggest-cyber-attacks-history?amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_tf=From%20%251%24s&aoh=16605713859142&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.albawaba.com%2Fbusiness%2F10-biggest-cyber-attacks-history> accessed 06 August 2022

- The Chinese hackers attacked the tech giant Google by breaching data with suspected agents, spies, and hackers who ultimately leaked the data into the public domain.
- The disastrous NASA Cyber Attack was executed by James Jonathan to shut down the connection for about 21 days and malicious software deleted several projects and plans which costs billion[50].
- The cyberattack on Ukraine's Power Grid resulted in a power loss for household consumers which was done by the Russian hackers to dismantle the electric supply[51].
- The U.S. government and organizations were targeted to destroy the information received from SolarWinds. A massive supply chain attack infected the software of SolarWinds leading to exploiting vulnerabilities. This attack was done by a Russian hacker group named APT29.
- The malicious attack of Stuxnet in Iran physically damages the infected devices and crushed the nuclear program was attacked by malware which destroyed the entire nuclear facilities[52].

THE DIRE NEED FOR CYBER EDUCATION

Education not only entails bookish knowledge but also the need for imparting practical applicability of mindset. In this 21st century each and every individual have an account on the social media platform to connect with friends, family, and many more; what if someone's social media account is hacked? – any prudent person with knowledge of hacking would immediately report that account or change the password of signing in to that account; but if the person is not aware of any such technological disability would either delete the account from the device or switch to some other social media platform. The education of cyber knowledge relating to computers, online scams, hacking, fraud calls, cyber-attacks, spamming emails, etc. needs to be cultivated among students, teachers, and working professionals so that they could easily learn to operate social media in the advent of cyberspace.

[50] *Ibid*

[51] *Ibid*

[52] Ben Flanagan (n 47)

Ensuring the privacy of information: Maintaining the privacy of the information is of utmost essential for protecting an individual from any cyber threat. Especially children should make sure not to disclose any confidential information, or personal identity and also not access authorized websites on the internet.

Providing technical skills relating to cyber security: Children should be provided classes on cyber security and management which includes technical skills for identifying the cyber threat and generating possible ways to get rid of it. Proper use of technicalities adheres to the cyberspace environment.

Awareness for cyber education needs to be enhanced: Programmes and awareness campaigns relating to cybersecurity cybercrime time need to be organized with help of projectors, short films, and documentaries which would engage maximum participation, and the interest in being e-safe will be aroused.

Cyber experts and ethical hackers need to be called upon: Cyber experts are the lifelines of the cyber arena who provides methodologies of being safe and also not being attacked by cyber terrorists; whereas ethical hackers would outline the structure that areas where cyber criminals lay trap and effectual remedies to get rid of it.

Using apps, devices, and social media which have encrypted data: Authenticate apps, social media, and websites that ensure data protection to the users shall be used only by which the confidentiality of the users is strictly maintained.

The need for cybersecurity and education is increasing in developing countries while underdeveloped countries severely lack cyber education, advanced technology, software mechanism, and cyber security which ultimately exposes them to deadly espionage and ransomware attacks. According to UNICEF International Telecommunication Union (ITU), two-thirds of the world's school children do not have internet facilities in their homes[53]. UNICEF and ITU have globally launched Giga spreading its branches to 30 countries, to connect every

[53] UNICEF, 'Two-thirds of the world's school – age children have no internet access at home, new UNICEF – ITU report says' <https://www.unicef.org/eap/press-releases/two-thirds-worlds-school-age-children-have-no-internet-access-home-new-unicef-itu> accessed 08 August 2022

school with internet facilities aiming to universal internet access to students which widens the boundary of digital sufficiency; promoting safe and secured internet facilities.[54]

DECODING THE STRUCTURE OF CYBER ATTACK

The rapid expansion of technology, intelligence, monetary availability, and structural developments have created a wholesome economy to function and administer its own rules and regulations. Among all these positive effects, negativities also spread their roots in the field of telecommunications with the help of cyber intruders who are profusely ready to stab users online. When the cyber attackers attack the users globally it is termed an *un-targeted cyber attack* which includes, sending a huge number of emails to the public to disclose sensitive information; cyber hackers setting fake websites intending users to visit it; malware functioning links which ultimately disseminate the software of the device and attacking the swathes of the internet. Another way to attack users individually is termed a *targeted cyber-attack* in which the victim is targeted and the hacker performs deadly operations to spoil the functioning of a particular system which includes, sending emails to a particular organization that contains malicious software to download the application; disconnecting the server to perform any task; supplying a bot attack which deletes every single information and deploying a DDoS system attack.

STAGES OF A CYBER ATTACK

Critical infrastructure of cyber-attack which follows a hierarchical format: -

Setting the target for the attack: The hackers set the target for a vulnerable attack by sending phishing emails, and injecting malware. They collect detailed information through online resources and try to access the company's website to make hacking easier.

Gathering information from the company's venture: Attackers would access the information from the company's vendor and then create a fake website by that name to access the whole information.

[54] *Ibid*

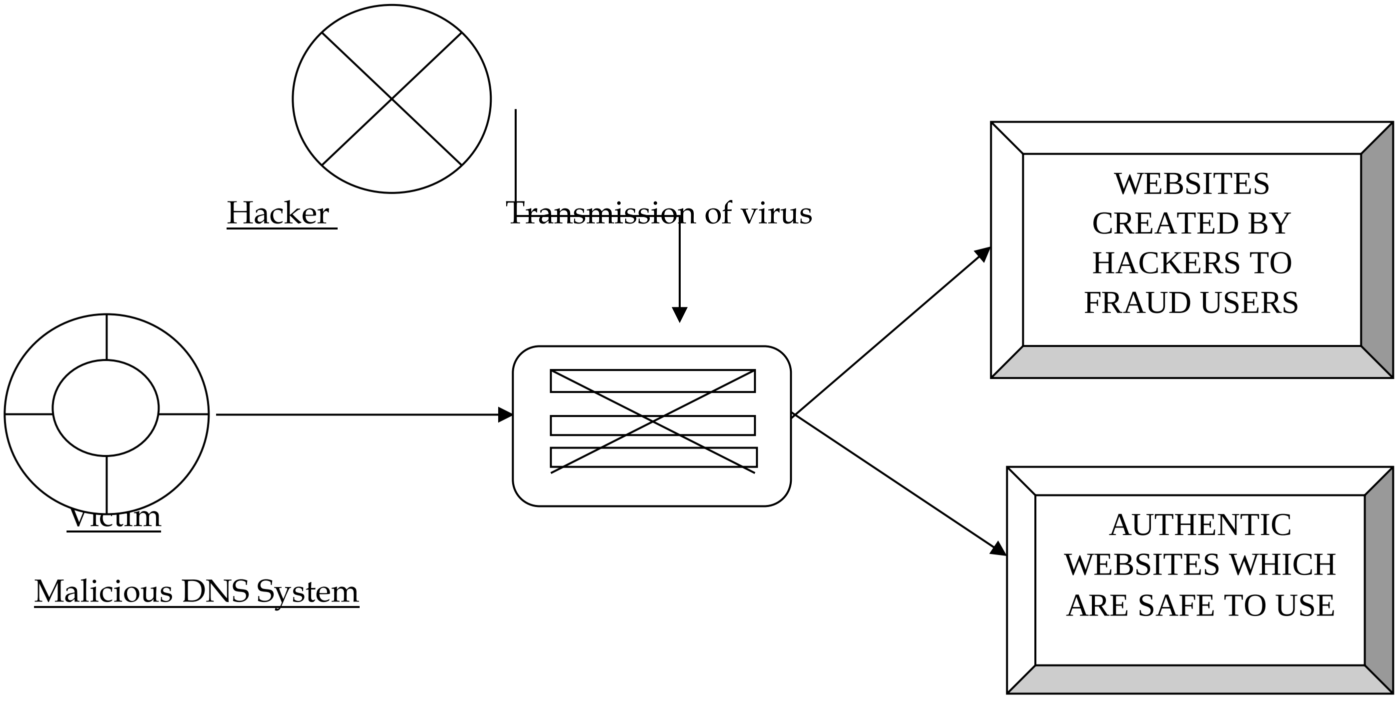
Bombarding the attack: This phase would contain sending phishing emails, fake links, and attachments which contain viruses that could easily destroy the system's functioning ultimately gaining benefit to the hackers.

Damaging the security environment: Accessibility of usernames, passwords, bank accounts, and delivering emails would ensure the fullest access over a company and the concept of security is totally exhausted in this phase; as the hackers control the flow by which the system is connected.

Installing a supportive work base: The hackers would have regular access to the network by damaging the firewall administration which won't be able to detect any software accessing the network of the device.

Effective mode of command: In this phase, the hackers would be able to access the network and even administer emails as it would have a greater aspect to restore the data without possibly harming the IT feature.

Fulfillment of hacker's intention: In this stage, the hacker's intention has been achieved the actual purpose to intend to steal products, designs, the formula for functioning of a machine, financial gain to steal a huge amount of money, deleting company orders, setting network traffic or shutting down of a server and wiping medical records from hospital's website to cause hectic trouble.


Hacker
Transmission of virus
WEBSITES CREATED BY HACKERS TO FRAUD USERS
Victim
AUTHENTIC WEBSITES WHICH ARE SAFE TO USE
Malicious DNS System

The above diagram depicts DNS (Domain Name System) hijacking where the malware replaces the router's DNS with malicious settings. Once the user's server is hijacked, even if the correct URL address is entered the user will be redirected to fake websites which will cause unusual tasks.

IS HUMAN SOCIETY SAFE?

The whole world is utterly troubled and frustrated with - Cyber aggression which has become an essential fact of today's human lives. Every single day cyber-attacks took place in any corner of the globe and the ultimate sufferer is human society. The technical human criminal possesses a great number of intellectual abilities to operate crime via machines. There has been a significant rise of cases during the covid-19 pandemic, as the whole world is dependent on technology for working purposes, teaching students, medical transcription, and attending online meetings from one hemisphere to another hemisphere; the attackers get an opportunity to act as an intermediary between the user and network and cause unavoidable issues that prevent user access to information, the anonymous attack has been the safest way to steal vital information without any hesitation. The cyber-terrorist and hacker groups created a mass terrorist attack in Iran and Palestine which was fatal in its conventional nature and led to the loss of a huge population deficit destroying the society with increased levels of anxiety, stress, threat perception, suicidal thoughts, and phases of depression, feeling of insecurity and mode of liberty are willfully neglected. Also, the war between the Americans and Europeans has been enigmatic due to the resiliency of cyber terrorists with the due radical perspective of Western confluence which resulted in drawbacks and disarmament[55].

The State-Trait Anxiety Inventory (STAI) defines the level of stress and anxiety which is raised due to the intense excavation of cyber threats and deadly autopsy from cyber terrorists resulting in suicidal interceptions which ultimately kill humans in no time. These kinds of constant attacks can lead to emotional dysfunction, psychological disability, being utterly depressed, lack of interest in activities, leading a half-dead life, and zero social engagements or interactions. To

[55] Michael L Gross & Ors, 'The psychological effects of cyber terrorism' *(Taylor & Francis Group ,* 4 August 2016) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589/#!po=84.5238> accessed 08 August 2022

increase the call for mental disabilities, the most disastrous and deadly process is political extravaganza ultimately degrades the democratic setup in the video of cyber terrorists which results in fear, anxiety, intense depression, lacking interest in daily activities, no stability of financial endowments, feeling of self-love is well wiped off, sense of helplessness, loss of sustainability of being alive, suicidal attempts makes a person more vulnerable, rendition of thoughts, zero social engagements and socio-cultural aspect itself becomes void with the perception of threat which eventually leads to *killing of human mentality in no time* [56].

The Protection Motivation Theory (PMT) poses a threat that potentially creates danger and the severity of danger, into one's mind to be vulnerable in nature where the individual is convinced of engaging in suspected behaviour. The factors of threat perception result in threat vulnerability, threat severity, response efficacy, and other adaptive behaviours, however, to depict the potential response from the lens of PMT for interpretation of cyber-attacks would possibly result in high levels of variations. The cognitive process involves the efficacy of risk control to bear the fear state of mind, and suggest preventive measures by performing risky tasks which could lower the efficacy of anxiety; when the mode of the effectiveness of threat grows to intrinsic in relativity individuals suffer from the aversion of threat creating negative impact[57].

Society is beheading towards insane suffering from which there is no end. Conditions got worse day by day with much tolerance of reforming but still, the dangerous surprises would prompt a life full of insecurities, privacy less, and fewer social intrusions.[58] The sense of helplessness with lacking knowledge in individuals raises the intensity of cyber-attacks, leading to much ignorance to be security attentive, and difficulty in understanding technological threats. Need to focus on the socio-psychological aspects which would follow crucial factors for a better analysis of the threat. Saving human civilization is more important than safeguarding technology- is there any validity in protecting the internet, if there is no existence of humanity?

[56] *Ibid*

[57] Maria Bada & Jason RC Nurse, 'The Social and Psychological Impact of Cyber- Attacks' (*Researchgate*, 2019) <https://www.researchgate.net/publication/338313135_The_social_and_psychological_impact_of_cyberattacks> accessed 08 August 2022

[58] *Ibid*

The existence of both is equally important to maintain balance; *one cannot function in absence of the other.*

POSSIBLE STRATEGIES TO ERADICATE CYBER TERRORISM

Cyber security is enhanced with several techniques by means of delineating digital terror from human lives.[59] The UN General Assembly adopts a resolution on cyber security that focuses on countering information and communication technologies for criminal purposes and elaborates on numerous policies on international conventions global to end cyber-related crime on a high note[60].

Preventive measures for eradication of cyber terrorism:

- Using a strong password by the user with a mixture of uppercase letters, lowercase letters, numeric and special characters would ensure privacy to protect from cyber-attacks.
- Updating the software of the device is essential to secure the data and prevent malicious attacks which reduce the risk of vulnerable attacks.
- Installing antivirus in the device will more sufficiently detect the type of virus, a worm which will automatically be erased by running a smart scan.
- Using authenticated apps while browsing on the internet which has an encrypted connection using a modern cypher suite.
- Do not share OTP, PAN number, Aadhaar Card number, ATM Pins, or passwords with anyone; failing it may render it a severe loss.
- The multi-factor authentication provides an excellent way to prevent unauthorized access to the account. Using two-step verification methods such as face unlocking as well as fingerprint locking constitutes tough access for hackers.
- VPNs (Virtual Private Networks) protect the identity of the user when it uses a public network or Wi-Fi, still keep the data private from the pyres, it also hides the IP address

[59] 'A UN Treaty on cybercrime en route' *(United Nations,* 4 May 2022) <https://unric.org/en/a-un-treaty-on-cybercrime-en-route/> accessed 09 August 2022
[60] *Ibid*

of the user browsing on the internet, and data throttling is well managed and the network scalability is well accessed.

- Installing Firewall into the system acts as a barrier between the trusted network and an unauthorized network, allowing non-threatening traffic in and keeping dangerous traffic out.
- Sensitive Data Shield is made to scan private documents containing information and to secure them against unauthorized sources.
- Companies and organizations need Antivirus Software in the system so that it is immune to viruses and malware infections to provide additional protective features.
- Every employer in the company should be aware of cyber issues and restrict from clicking any unnecessary mail which itself is malware and careful handling of the sensitive information is needed.
- CCTV cameras need to be regularly monitored so that they might get hacked by the attackers only on your systems, without having control over the network.
- Government should take serious steps for the emancipation of cyber security programs in the country which could lower the intensity of the cyber-attack.
- Children should be enrolled in cyber assistance courses to develop the ability to protect themselves from any cyber harm while browsing websites on the internet.
- Cyber experts and consultants should organize events, workshops, work drills, and boot camps in schools, universities, and workplaces to effectively deal with cyber threats and quick steps to follow in a rogue situation.
- Special Cyber Response Team would be set up by the Government in cyber-terrorist attacks to respond in an emergency situation.
- Cyber helpline numbers should be made accessible at all times for any assistance of the public whenever there is bank fraud, cyberbullying, and spying on social media.

The Indian Government has undertaken some policies for the eradication of cyber-crime:

- The Establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC) for the protection of critical information of the citizens to safeguard confidentiality[61].
- Launching of Cyber Swachhta Kendra by the Central Government to scan, detect and clean malicious botnet infections to maintain a safe and secured cyber environment[62].
- The guidelines issued by the training programs and Chief Information Security Officers (CIISOs) of the Government's security attack.
- The SKOCH event of the National Cyber Security Coordinator would enable a fund for about $5 million for the purpose to resolve cyber-attacks and cyber terrorism through the huge economic effort[63].
- Drafting and formulation of a Crisis Management Plan for combating cyber-attacks and trying effective manners to fulfill the objectives of the drive.

International strategies and policies have been adopted to adjudicate cyber terrorism:

- UN prepared a strategy named National Cyber Security aims to develop cyber security protection of information which promotes good internet governance, it further recommends to all sectors of the economy, society, and various departments a sustainable approach to providing protection in the advent of raging threats[64].
- The National Cyber Security strategy of the UK defines strengthening the UK cyber ecosystem; building a resilient and prosperous digital UK by reducing cyber risks; leading in technologies vital to cyber power; advancing global leadership and influence for a more secure and open international order with the expertise of industrialists; detecting, disrupting and deterring the adversaries to enhance UK security and through cyberspace to an integrated course of the UK's infrastructure[65].

[61] PIB, 'Steps Taken to Deal with Cyber Crime and Cyber Security' (*Press Information Bureau* ,17 July 2019) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226> accessed 10 August 2022

[62] *Ibid*

[63] *Ibid*

[64] 'National Cyber Security Strategy 2016-2021' (*UK*, 7 February 2022) <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#annex-b-nis-regulations--national-strategy> accessed 10 August 2022

[65] *Ibid*

- The EU Cybersecurity Strategy was an imperative ingredient of Shaping Europe's Digital Future and the EU Security Union will help to brace the resiliency against cyber threats and ensures all citizens are reliable with digital services.[66] It allows upgrading the international norms in the field of cyberspace, and strengthening cooperation to promote a global, open, stable, and secure cyberspace in accordance with human rights, fundamental rights, and the fundamental freedom to maintain the democratic structure[67].
- Iran and Russia have signed a joint agreement on cybersecurity cooperation including technology transfer, and mutual cooperation on building norms to conduct cybersecurity events[68].
- UAE passed new laws aiming to curb the practice of hacking, identification of threats, and increasing attacks leading to violation of criminal laws whereas, other Middle East countries have also regulated the sphere of cyberspace with coordination at the international level[69].
- The International Governance Forum (IGF) is an international convention aiming to discuss the severity of the attacks by encouraging several States to install hostile measures which could protect human rights which could give fair justice to the concept of democracy; also focuses on strengthening the digital network with stringent mechanisms.

CRITICAL INTERPRETATION

The evaluation of the digital era has significantly attracted hi-tech cyber offenders, and cyber terrorists in accordance to cyber criminologists, cyber researchers, and legal cyber advisors have analyzed the nature, causes, implications, disorder, and growth of its rise. The AI interface made advancements in sectors of e-commerce, agriculture, banking, defence, and communications which aggravated the lifestyle of the people while it gives an edge to digital offenders for

[66] 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' (*European Commission*, 16 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> accessed 12 August 2022

[67] *Ibid*

[68] Clement Gibon, 'In Middle East cyberattacks, targeting vulnerable populations are on the rise' (*Equal Times,* 4 May 2022) <https://www.equaltimes.org/in-the-middle-east-cyberattacks#.YvO5NhlX6Nw> accessed 12 August 2022

[69] *Ibid*

hideouts into the structural framework of the country. Endorsing stringent laws, legislations, and regulations, however, do not account for the crimes non-functional but muffle the flames of e-crime towards extinction.

The critical infrastructure system has impacted the workings of the nation's security, indicating an upsurge in threat intensity of physical and cyber-attacks and a futuristic electrical network. Strict dependency on the nature of the system has led to quantifying the object of attacks in the infrastructural misbalances. The operating environment is potentially vulnerable to attacks with the usual preventive methods of securing data and managing the mechanism of the defence network. As the network facility is endorsed about causing damage with a malware attack or conducting sabotage to penetrate the supply chain of viruses to make the situation even worse. The development of healing systems would consider automated recovery, quick response, and self-detection of critical attacks.

The paradigm of the cybersecurity community has helped to ratify the security and privacy-related issues, achieving internet-friendly accessibility to use intrinsic methods barring any complexity or outward shifting the curve to ensure the protection of particulars. Approaches to discover new ideas and thoughts without taking help from the internet could initiate deep learning activities, 'enthusiastic to understand any issue by means of practicality' and the traditional environment of not focusing much on computing tactics assures strong reliance on socio-cultural aspects to gather opportunities in a systematically better manner. The global focus and dependence on the internet have led to the breakdown of digital management that thwarts the increasing aggregate of cyber offenders.

Human mentality is fully engrossed in inventing much-sophisticated technology at every point of time; as every single work will be done by robotics- will ruin the traditional concept of 'manual work' leaving civilization on an isolated island with bounds of mechanization infrastructure; for example- the modernized concept of ordering food online has been reliable on the other hand, if the order was misplaced and got cancelled, technology fails to comply its accurateness whereas, human labour is much convenient, cheaper, time-saving and accurateness is well maintained.

CONCLUSION

The laws do not ensure proper eradication of the problems, its importance is bounded within the ambit of legalizing the law in terms of paper rather than, implementing it at grass-root levels for removal of cyber-crimes from society. It is the duty of the citizens to 'raise their voices against the cyber-attacks and mass protests of citizens demanding 'secured privacy. The burgeoning cyber intelligence has seen rapid expansion in the context of updated developments around the globe. With the combination of expertise, skills, abilities, and knowledge in the pitch of virtual society, a team of counter-cyber terrorism can build a mechanism of prevention of cyber terrorism attacks, understand threat perceptions, and direct effective principles to combat cyber terrorism at greater range. Outdated laws which deal with cyber terrorism are not sufficient to administer the huge crux of technological progress hence, the formation of advanced laws with severe penalization will lead to the stabilization of cybercrimes. The complex programming language is used by cyber hackers to modify the internet culture with intense mental intent. Focus on the mental hygiene of cyber attackers should be broadly researched to essentially treat them with psychological medications.

It is analyzed that technology-based violence should come under the umbrella of "ruthless inhumanity" as treating a serious issue for its illegality in nature. Proximity to the target is variable in geographical territories where there is an abundance of operating companies, official bungalow renowned institutions, and a large population with the availability of resource choices for constituting cyber-attacks. Various cases of cyber-attacks get unreported by the news channels when the scam is executed by means of political tensions. The disastrous nature of the cyber-attack is because tremendous mental pain is sustained in hemorrhage rather than physical disruption, it acts as a "silent killer" to target the soft corners of the individuals. This type of violence only brings hatred, fear, dis-attachments, misconceptions, ill-social life, and prejudices. Humanity in this way adopts the negative culture to attack each other technically, as a means to satisfy personal grudge or revenge. Strengthening the principles of truthfulness, socializing, mankind, sense of cooperation, coordination for better civilizing the society and curbing the digital problems. The beauty of mankind is seen in the horizontal landscape with an open environment where it is free from any digital intrusions, leading a happy and prosperous life with less interference in the digital world.