Page 315 - 324 **DOI:** *https://doij.org/10.10000/IJLMH.116726*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 1

2024

Evolution of Cyber Crime: Emerging Global Challenges

NITIN VASHISHTH[1]

ABSTRACT

When man first created the computer, he never would have imagined that the cyberspace he was building would become a hotbed of what is now known as cyber-crime. The requirement for internet connectivity has made it possible for cybercriminals to commit crimes more frequently and at a faster rate because they are no longer required to be physically present. Where as cybersecurity is essential to the information technology industry. One of the main problems of the modern world is securing and protecting information. On the one hand, the internet makes communication easier, but on the other, some people or groups abuse its power for illegal activities.

The notion of cybercrime, some specific forms of prevalent cybercrimes that are occurring prominently, issues facing cyber security on the newest technology, and a study of the individuals engaged and their motivations are the primary topics of this paper. Additionally, it focuses on the trends reshaping cyber security and offers suggestions to assist in curbing the rising number of cybercrimes and illegal cyber activity.

Keywords: *Cyber crime, Cyber security, Cyber War, Technology, Cyber Law.*

I. INTRODUCTION

The use of computers and the Internet are becoming indispensable in both our private and professional life, everyone in the modern world is either directly or indirectly involved in the cyber world. Like any other technology, computers and the internet can benefit humanity provided they are used responsibly and for the good of society; if not, they can be a scourge.

Worldwide, cybercrime poses a threat and is among the hardest crimes to identify and investigate.

The COVID-19 pandemic has caused a massive spike in internet usage and the need for people to restart working from home. Simultaneously, there is a rise in the use of technology for employment, education, and leisure, which involves routine data sharing with everyone

[1] Author is a Law Practitioner in India.

 [ISSN 2581-5369]

involved.[2]

These days, we share our information through technology on a variety of platforms, such as job applications, bank records, medical data, and e-commerce websites. However, sharing information on social media is the most significant of all. These days, in order to obtain many essential services—like health care, financial transactions, and the purchase of goods—we must provide information.

India is third among the top 20 countries affected by cybercrime, as per the FBI report[3]. 33,152 complaints have been submitted through the central government's national cybercrime reporting platform, leading to the filing of 790 formal complaints. In fact, a 2017 survey stated that cybercrimes have cost Indian consumers more than 18 billion US dollars. More than 27,000 cybercrimes were reported in the nation in 2018, a rise of more than 121% from the number of instances in 2016.

Every day, cybercrime is growing throughout the world. The primary challenge associated with cybercrime stems from its dynamic character due to the continuous advancements in digital technology. New strategies and tactics for cybercrime are consequently executed. The increasing interconnectedness of our society has led to a concerning increase in the frequency and complexity of cybercrime, which has made it crucial for legal frameworks to constantly adapt in order to successfully combat these threats.

(A) Objectives of the study

a) This paper seeks to unfold the evolving cyber crimes like cyber terrorism, cyber extortion, cyber warfare, cyber espionage, cyber bullying & exploitation.

b) The research attempts to examine the connection between cybercrime and national security.

c) The study aims to demonstrate that these offenses constitute serious threats to human rights.

(B) Methodology

This research work follows a doctrinal method. The paper provides a descriptive analysis of India's various cybercrimes. Secondary form of data is used about cybercrimes which has been taken from reliable sources. The data used here was gathered from a variety of publications, including books, articles, magazines, journals, and laws.

---

[2] *Google finds 350% more fraud sites amid Covid-19 - Atlas VPN* (no date) *atlasVPN*. Available at: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine/ (Accessed: 09 January 2024).

[3] *India's poor cyber awareness: Lack of board-buy in and digital...* (no date) *TSC*. Available at: https://thesecuritycompany.com/the-insider/indias-poor-cyber-awareness-lack-of-board-buy-in-and-digital-literacy-damaging-security-levels/ (Accessed: 09 January 2024).

 [ISSN 2581-5369]

II. CYBER ATTACKS

Cybercriminals carry out these crimes by taking advantage of various cyber threats. They utilise malware to take advantage of flaws in hardware and software design. The goal of DOSS attacks is to overload the targeted websites. One popular method for breaking through secured computer systems' defences and preventing them from operating normally is hacking. Theft of identities is also widespread. Every day that goes by, threats and vulnerabilities grow in number and kind.

Cyberthreats can be categorised according to the offenders and their intentions, for example :

1. Terrorism:

Cybercriminals now have a convenient online platform to carry out their destructive actions, and disseminate hate propaganda, and other activities. Minimal internet regulations, anonymity, a wide audience, quick information dissemination, and many more advantages made this possible. The mere mention of terrorism is enough to tingle one's spine, and it gets much scarier when you combine it with the word "Cyber".

The phrase "cyber terrorism" is contentious and still lacks a precise definition. Nonetheless, in simple words it is the use of the Internet for violent digital activities that cause or threaten significant bodily harm or loss of life to achieve political or ideological gains through intimidation or threat of death. Computer networks connected to the Internet will be seriously impacted in case of a cyber-terrorism attack. Tools including computer worms, malware, phishing, hardware techniques, programming scripts, malicious software, and much more are used to do this.

In the "Global Risk Report" for 2021[4] published by the "World Economic Forum", one of the biggest threats to humanity in the coming ten years is a breakdown in cyber security. With 749 million people, India holds the second-largest digital market in the world, behind China. In addition to the benefits of technology that India has seen recently, the country has also been the target of numerous terrorist attacks that were made possible solely by the availability of technology.

A few of the most deadly terrorist attacks that India has fallen victim to due to the improper use of digital technology are the attacks on URI, Pulwama, and the horrifying 26/11 Mumbai tragedy.[5] The attackers' significant use of digital telecommunication was uncovered during the

[4] *Global risks report 2021* (no date) *World Economic Forum*. Available at: https://www.weforum.org/publications/the-global-risks-report-2021/ (Accessed: 09 January 2024).
[5] Saigal, S. (2022) *Security conference on 26/11 attack anniversary calls cyberwar and cyber espionage as new threats*, *The Hindu*. Available at: https://www.thehindu.com/news/cities/mumbai/security-conference-on-2611-

 [ISSN 2581-5369]

Mumbai Attack investigation. The terrorists had obtained information regarding India's location, population, infrastructure, map, etc. from the internet. They even used digital platforms for monitor the movements of the “Indian Rescue and Defence Forces”, a cellular network for cordinating and communication, and "Google Earth" for carrying out their strategy.

CERT-In responded to 11,58,208 cyberterrorism-related threats in 2020. These comprised suspicious code, distributed denial of service attacks, ransomware assaults, phishing, data breaches, unauthorized network scanning and probing, website defacements, and website intrusions and propagation.

2. Extortion

A variety of cyber crimes are grouped together under the general name "cyberextortion." Cybercriminals or hackers who attempt to coerce a business or organisation into compromising its private information in exchange for a ransom is known as “cyber-extortion”. “Ransomware” and “DDoS (Distributed Denial of Service) attacks” are thus the two most prevalent forms of cyber-extortion. The word "ransomware" was initially used in the real sense after the introduction of cryptocurrencies such as Bitcoin in the year 2013. It began as introduction of the malicious "Cryptolocker" RWA, that used the "game-over zeus" botnet to extort more than $3 million. The first sophisticated Ransomware assault (RWA) and the father of the Zeus botnet, Russian hacker Evgeny Bogachevave, has a bounty of more than USD 5 million[6] and is countinously hiding from the authorities.

In addition to data loss caused by encryption, cybercriminals may profit from the sale of private information. 2020 saw ransomware attack India's home loan organisation, resulting in data loss. The company was in serious difficulties since it had misplaced the information pertaining to the amount it needed to reimburse its clients. To obtain the decryption key, it was required to pay a ransom of more than Rs. 50 crore in Bitcoins. The Times of India article claims that the case was never reported to police enforcement.

According to a recent edition of Forbes, ransomware extortions have surpassed USD 250 billion in 2021. Attacks impacting 2.5 million Internet of things are launched virtually every ten seconds (IoT). The fact that some of the most skilled cybercriminals make millions of dollars each month has caused this crime to become more industrialised. In 2021, its revenues will

attack-anniversary-calls-cyberwar-and-cyber-espionage-as-new-threats/article66187611.ece (Accessed: 09 January 2024).

[6] Jai Vijayan, C.W. (2023) *US sets $5 million bounty for Russian hacker behind zeus banking thefts*, *US Sets $5 Million Bounty For Russian Hacker Behind Zeus Banking Thefts*. Available at: https://www.darkreading.com/cyberattacks-data-breaches/us-sets-5-million-bounty-for-russian-hacker-behind-zeus-banking-thefts (Accessed: 09 January 2024).

 [ISSN 2581-5369]

surpass $6 trillion USD, which is over 2.5 times the size of India's economy.[7]

3. Cyber Theft

Cyber Theft incidents are becoming more frequent; claims of thousands of megabytes of data and intellectual property valued at millions of dollars being exfiltrated from the websites and network gateways of both public and commercial companies are widespread. The private sector asserts that it has not been impacted in the same way as NWs and the official websites in India have been compromised. It's also possible that the fact that government spending makes up 70% of R&D spending in India, which amounts to just 0.7% of GDP, means that intellectual property theft from private businesses is not a problem here. Additionally, businesses are hesitant to reveal any security breaches or data leaks for fear of being held accountable by their clients and losing the public's trust as a result.[8]

Law enforcement and intelligence organisations have requested legal and operational support from their governments in order to safeguard critical networks and launch a counter attack against cyber criminals and spies who frequently collaborate and most likely have official support. As seen by the ongoing incidents of government department servers being breached and records being leaked, offence is not always the best form of defence when it comes to cyber security.

4. Warfare

Although there is no universally accepted definition of cyber warfare, it has been observed that states may be targeting the information networks of other nations in order to eavesdrop on them and interfere with their vital infrastructure. It mostly refers to hacking for political purposes in order to carry out espionage and sabotage. This form of information warfare is occasionally related to traditional warfare.

It is commonly believed that state actors may have utilised non-state actors, such as hackers, in these attacks, even if there is no concrete evidence linking a state to them.[9] The US quickly updated its military doctrine and established the cyber wing under the "Strategic Forces Command". According to the US military's most recent official doctrine, cyberspace ranks fifth among the domains of combat, after land, air, sea, and space. The US has reserved the right to

[7] Sentonas, M. (2021) *Council post: Ransomware: Double the trouble in 2021*, *Forbes*. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/09/24/ransomware-double-the-trouble-in-2021/?sh=16169bd1275b (Accessed: 09 January 2024).

[8] *Nearly 73% of Indian mid, large companies hit by Ransomware in 2023* (no date) *The Economic Times*. Available at: https://economictimes.indiatimes.com/tech/technology/nearly-73-of-indian-mid-large-companies-hit-by-ransomware-in-2023/articleshow/105518876.cms (Accessed: 09 January 2024).

[9] Institute for Security Technology Studies.www.ists..dartmouth.edu/docs-cyberwarfare.pdf Similar

use all available means, including military force, to counter cyberattacks. Other nations will likely follow suit and implement equivalent military doctrines.[10]

The subject of concern if state actors in cyberspace should be subject to rules of behaviour is now being debated in multilateral conferences. The problem becomes highly complex because cyberattacks cannot be linked to a specific individual and affect various computer systems spread across several nations. The idea of digital deterrence is also under discussion, yet, considering the ease with which non-state actors could step in and the absence of acknowledgment, it is unclear whether this tactic will be effective in cyberspace. There is, however, continuous discussion between those who think the world is on the verge of cyber Catastrophe and those who think cyberwarfare is over exaggerated. Although there are sound arguments on both sides, the fact that more and more nations are establishing cyber commands means that cyber warfare as a concept is becoming unavoidable. Alongside these directives, efforts have been made to create relevant military doctrines. As a result, it is imperative to consider cyberwar rules, the applicability of the laws of armed conflict (LOAC) to cyberwar, and the implications of concepts like proportionality and neutrality in cyberspace.[11]

In the context of cyberwarfare, existing collective security regulations like Chapter 7 and "Article 41" of "the UN Charter" are insufficient, considering how quickly cyberattacks occur and how long it takes for decisions to be made and actions to be taken under these regulations.[12]

III. METHODS AND TECHNIQUES

- **Attack causing Denial of Service:** In this situation, the victim's device crashes because it receives more requests than it can process. Another kind of denial of service attack is the "Distributed denial of service attack", under which the offenders target in digits and widespread. such as Flipkart and Amazon.[13]
- **Trojan Attacks:** It is the "Trojan horse" where this term first appeared. In the context of cyber world, this refers to an unauthorised program that poses as an authorised programme in order to subtly take control of another system. The most popular way to install a Trojan is via email. For instance, a Trojan was planted in a film director's computer in the United States while she was chatting with a criminal who used the computer's webcam to collect

[10] https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_StrategySummary.PDF
[11] https://www.ca2.uscourts.gov/docs/jc_reports/2014/6_Cyber_War_and_the_Law.pdf
[12] *Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression (articles 39-51)* (no date) *United Nations*. Available at: https://www.un.org/en/about-us/un-charter/chapter-7 (Accessed: 09 January 2024).
[13] Anderson, P. (1982) *Shield, Amazon*. Available at: https://aws.amazon.com/shield/ddos-attack-protection/ (Accessed: 09 January 2024).

her naked photos. Then he began to harass the woman.

- **Salami Attacks:** This type of crime is typically committed with the intention of committing financial crimes in financial institutions. The fact that the alteration is so minute that it would typically go undiscovered characterizes this kind of crime. The Ziegler case, is the example of logic bomb which was placed into the bank's servers, taking a certain amount from the accounts and transfered the amount into a different specified account.[14]
- **Email Bombing:** Sending a significant amount of emails to the victim—who could be a person, business, or even mail servers—is referred to as Email Bombing. The ultimate goal of this is to cause the system or the data to crash.
- **Logic Bombs:** These programmes rely on instances. It suggests that these programmes are formed to execute only in response to a specific happening of an incident known as “trigger event”. The Chornobyl virus, could be called as "logic bombs" because they only turn operational on a certain date and are dormant for the entire year.
- **Internet Time Thefts:** Usually, someone else uses the victim's Internet browsing time during such kinds of thefts. To do this, you need to get an account identification and password.; for eg. in “Colonel Bajwa's case[15]”, the Internet time was consumed by someone else. This was maybe one of the first cybercrime incidents in India to be publicised. However the police were embarrassed by this case since it showed how little they knew about the nature of cybercrime.
- **Virus Attacks:** Programmes known as viruses, affix itself through a system or an attachment, replicate to further data, and ultimately infect network-connected devices. They mainly affect, alter, or destroy data from computers. Whereas the worms can attach themselves to any host. They just replicate themselves, often doing so until they occupy all of the memory space on a computer. An example of this is the “love bug virus”, impacted almost 5% of devices worldwide. Ten million dollars was reported as the loss amount.
- **Data Diddling:** This type of attack entails modifying raw data immediately prior to computer processing and then reverting those changes after processing is finished. When the electrical board was computerising the department, they encountered a similar issue with data diddling.
- **Web Jacking:** The word "hijacking" is the source of this phrase. These types of offences

[14] Chibueze, I.G.C. (2021) *Cyber crimes*, *MediaLaws*. Available at: https://www.medialaws.eu/cyber-crimes/ (Accessed: 09 January 2024).
[15] https://journal.lawmantra.co.in/wp-content/uploads/2015/05/251.pdf

provide the hacker access to and authority over another person's website. He might even alter or mutilate the data on the website. This could be done for financial gain or to achieve political goals. For instance, Pakistani hackers recently gained access to the MIT (Ministry of Information Technology) website[16] and posted offensive content there. Additionally, there was a web-jack of the Bombay Crime Branch website. The "gold fish" case was another instance of web jacking. In this instance, the website was compromised, resulting in the alteration of goldfish-related data. Additionally, a $1 million US ransom was requested. Web jacking, then, is the act of taking control of another person's website in order to obtain consideration for releasing it from that control.

IV. INTERNATIONAL CONVENTION

Cyberspace crimes are one of the types of international crime that are expanding the fastest in the twenty-first century. Cybersecurity is seen as a current hot topic in international law and is very significant when one talks about international security. Civil society access to a secure and safe internet is extremely crucial. Upon observing these difficulties, the global community has united, establishing organisations and formulating agreements to tackle the increasing number of cybercrimes.

(A) Budapest Convention

The Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention, is the most comprehensive and well-organized international agreement on cybercrime. It was adopted on November 8, 2001, by the Council of Europe's Committee of Ministers during its 109th session, and on November 23, 2001, it was made available for ratification in Budapest[17]. In 2003, it was expanded to include a “Protocol on Xenophobia and Racism Committed via a Computer System”. On July 1, 2004, the Convention came into effect. The Convention, which deals specifically with offenses against and the first international treaty on crimes committed via the Internet and other computer networks addresses the use of computer systems and data, including illegal access, illegal interception, data and system interference, computer-related fraud, child sexual exploitation material, and other network security violations. Its primary goal is to implement a common criminal policy that protects society from cybercrime, particularly through the adoption of suitable laws and the promotion of global collaboration. The Convention's main goals are to strengthen member-

[16] Ackoski, J., & Dojcinovski, M. (2012, June). “In Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012. MIT University.”
[17] https://www.coe.int/en/web/cybercrime/the-budapest-convention

state cooperation and harmonize their national laws.

The United States, Canada, Japan, the Philippines, and South Africa were among the observer states of the Council of Europe when it drew up the Convention. The main objectives of the Convention are to: harmonise the elements of domestic criminal substantive law that relate to offences and related crimes; provide provisions for the investigation and prosecution of cybercrimes and other offences committed using computer systems or other electronic means; and establish an efficient internal criminal procedural law system.

V. LAWS RELATED TO CYBERCRIMES IN INDIA

The following is a list of the different cyber activities that are illegal under the IT Act and the IPC:

(A) Cybercrimes as specified in the Information Technology Act:

"Tampering with computer source documents - Sec 65

Hacking with computer systems, data manipulation - Sec 66

Publication of obscene material - Sec 67

Unauthorised access to a secured system - Sec 70

Breach of Confidentiality and Privacy - Sec 72

Release of counterfeit digital signature certificates - Sec 73"

(B) Cybercrimes under IPC:

"Sending threatening emails - Sec 503 IPC

Sending Defamatory Email Messages - Sec 499 IPC

Forgery of Electronic Records - Sec 463 IPC

Bogus websites and cyber frauds - Sec 420 IPC

Email Spoofing - Sec 463 IPC

Web-Jacking - Sec 383 IPC

Email Abuse - Sec 500 IPC"

VI. CONCLUSION

Cybercrime is growing exponentially both in India and worldwide. Cyber terrorism, cyber extortion, cyber warfare, and exploitation of human rights are among the crimes committed in cyber space. These and other related crimes have all been carefully examined in this paper along

with the relevant legal framework within the framework of Indian jurisprudence. The Budapest Convention was also discussed in this paper.

The requirement for security in electronic networks creates new difficulties. Indian statutes and law enforcement bodies needs to keep up with the increasing number of cybercrimes and the expanding body of international jurisprudence around them. In the digital era, there are opportunities for growth for those who can best use information and technology. The COVID-19 epidemic has caused a mass exodus of knowledge into the cyberspace, making this adjustment more urgently needed. Government policies, specialised investigative agencies, and statute legislation will all play a significant role in safeguarding India's cyberspace.

Through legal awareness initiatives, the public should be given the necessary knowledge to protect themselves against the dangers of cybercrimes. The future of digitalization in India is perilous, and we must move this precipice towards safety and security concerning cybercrimes.

The necessity to enact proper regulatory legislative measures and strengthen the law enforcement apparatus to combat cybercrime head-on is evident in the growing scope of computer-related crimes. Handling cybercrime cases effectively requires a multifaceted strategy and concerted efforts by all law enforcement agencies.

Perhaps the best way to stop and manage cybercrime would be to have a single, internationally ratified cybercrime regulatory law. It also urges those who are susceptible to cybercrimes to take proactive steps to protect themselves. They need to be sufficiently informed about the seriousness and nature of these crimes, as well as the risks they pose. Naturally, the media must play a significant role in alerting the public to the potential risks and detrimental effects that cybercrimes may have on the victim or victims, the country, as well as the safety measures needed to combat this high-tech crime.

*****

 [ISSN 2581-5369]