CYBERCRIME AND THE LAW

Shivani Kumari*

ABSTRACT

This study examines the complex terrain of cybercrime, breaking down its various facets and examining how threats have changed in tandem with technological breakthroughs. Setting the scene, the introduction highlights the urgent need for new legal frameworks that can handle the never-before-seen difficulties brought on by cybercrime. It draws attention to how widespread cybercrime is and how crucial international cooperation is in thwarting these online dangers. A thorough historical analysis of cybercrime follows its genesis from the early days of computer technology to its present complex and widespread manifestations. From the early cases of illegal access to the creation of complex cyber espionage and the exponential rise in cybercrimes in the twenty-first century, this historical framework clarifies the dynamic nature of cyber dangers. The conversation emphasizes how devices are becoming more and more connected, how ransomware assaults are becoming more common, and how many cybercriminal networks are present on the dark web. A crucial component of cybercrime is the human factor, which clarifies the psychological effects on offenders and victims alike. Social engineering techniques are used by cybercriminals to take advantage of human weaknesses, which emphasizes the significance of education and awareness in reducing these risks. Since victims frequently experience extreme emotional pain, psychological support is as important as technology safeguards in helping victims cope.

INTRODUCTION

Cybercrime has become more commonplace in our quickly changing digital environment, posing an unprecedented challenge to judicial systems throughout the globe. Cybercrime includes a wide range of illicit acts, such as data breaches, identity theft, hacking, and online abuse. Cybercriminals' techniques also evolve with technology, thus it is critical that legal frameworks be up to date and properly handle these new dangers.

The legislative reaction is essential to combating cybercrime. Governments from all throughout the world have tried to stop these digital crimes by enacting several laws and rules. For

*BA LLB, FOURTH YEAR, SYMBIOSIS LAW SCHOOL, NOIDA.

example, the United States' Computer Fraud and Abuse Act (CFAA) emphasizes the safety of digital infrastructure by making unauthorized access to computers illegal. Similar to this, data protection is highly valued by the European Union's General Data Protection Regulation (GDPR), which imposes strict requirements on organizations that handle personal data[1].

HISTORY OF CYBERCRIME

Cybercrime's history is as complex and dynamic as technology itself, following a trajectory that reflects the development of digital environments and the subsequent appearance of illicit exploits therein. Cybercrime has its origins in the early stages of computer history. When computers were still in their early stages, in the 1960s and 1970s, there were reports of incidents of unauthorized access and system manipulation. One of the first documented cybercrimes occurred in 1971 when John Draper, often known as "Captain Crunch," exploited phone weaknesses by making free long-distance calls with a toy whistle from a cereal box.

Cybercrimes become more sophisticated as technology advances. Computer viruses were more common in the 1980s; one of the first notable examples of malware spreading across networked computers and causing extensive damage was the "Morris Worm" in 1988.

The 1990s were a critical decade for cybercrime due to the internet's explosive growth. Hacking occurrences increased during this time period, mostly due to curiosity and investigation rather than malevolent intent. But when personal data and vital infrastructure got increasingly entwined with the internet, cybercrime developed into a more profitable business. Identity theft, credit card fraud, and illegal access to private information increased in frequency[2].

CATEGORIES OF CYBERCRIME

There are 3 categories of cybercrime

- **Individual**

This category is also known as personal cybercrime. This kind of cybercrime is committed only against the individual.

[1] Caneppele S, Aebi MF (2019) Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice 13(1): 66–79.
[2] Goldsmith A, Brewer R (2015) Digital drift and the criminal interaction order. Theoretical Criminology 19(1): 112–130.

- **Property**

This cybercrime is committed against property like Mobile devices, Computers and other electronic devices.

- **Government**

Government cybercrime is the last and third category of cybercrime. These kinds of cybercrimes are directed at governments, which might include national, state, or municipal governments.

TYPES OF CYBERCRIMES

- **CYBER STALKING**

Cyber Stalking is persistent, unwanted internet monitoring or harassment of a person or organization. The victim of cyberstalking frequently experiences severe mental suffering, anxiety, and life disruption. It has the potential to worsen and may be coupled with physical stalking or other types of harassment. Several nations have laws and regulations that attempt to regulate and penalise cyberstalking behaviours in order to shield people from this kind of online abuse.

- **ARTIFICIAL INTELLIGENCE ATTACKS**

Artificial intelligence and machine learning techniques are used by AI-powered assaults to carry out and improve cyber threats. These assaults target, penetrate, and breach systems, devices, or networks using AI algorithms and automated procedures. The ability of these AI-powered assaults to quickly change, adapt, and get beyond conventional security procedures makes them a rising cybersecurity worry. Strong cybersecurity plans, more awareness, and the creation of AI-based security solutions are all necessary to combat these threats.

- **COPYRIGHT INFRINGEMENT**

The term "copyright infringement" describes the unapproved use, duplication, distribution, or alteration of intellectual property without the owner's consent. It entails going against the exclusive rights given to the author or proprietor of original works, which can include movies, software, music, books, artwork, and other kinds of creative expression. This infringement

happens when someone illegally uses copyrighted content. Legal repercussions for copyright infringement may include lawsuits, penalties, or injunctions.

- **CYBER HARASSMENT**

Cyber harassment is the practice of continuously intimidating, threatening, dehumanizing, or torturing a person or group using digital communication channels or online platforms. It involves unwelcome and repeated behaviour that makes the victim feel uncomfortable, afraid, or distressed emotionally. For the victims, cyberbullying may have serious psychological, emotional, and perhaps even bodily repercussions.

- **EAVESDROPPING ATTACKS**

Unauthorized surveillance or interception of confidential conversations between two parties is known as eavesdropping. When sensitive information is being conveyed across communication channels, such as phone conversations, emails, instant messaging, or data transmissions, the attacker secretly listens in on or gains access to it. Attacks using eavesdropping techniques seriously jeopardize security, secrecy, and privacy.

- **MALWARE**

Any programme that is specifically created to harm, interfere with, or get unauthorized access to computer systems, networks, or devices is referred to as malware, short for malicious software. It includes a broad spectrum of malicious software developed with malevolent purposes.

- **RANSOMWARE**

Malicious software known as ransomware is made to encrypt data or lock users out of their computers and then demand money (often in cryptocurrency) for the decryption key or to unlock the system. Striking a delicate balance between planning, reaction, and prevention is necessary while handling ransomware assaults. Prioritizing cybersecurity precautions and having a well-thought-out incident response strategy is crucial for lessening the effects of a possible ransomware attack.

- **PHISHING**

Phishing is a sort of cyberattack in which perpetrators utilize cunning strategies to fool victims into disclosing private information, financial information, or login credentials. It uses social engineering strategies to trick and control users. Individuals and organizations may greatly lower their chances of being victims of phishing attempts by remaining alert, exercising caution when communicating online, and asking questions to ensure that demands for sensitive information are legitimate.

- **ONLINE DEFAMATION**

The act of producing false, defamatory, or harmful remarks about a person or entity using online platforms in order to harm their reputation or character is known as online libel or slander. Online slander and libel can have serious ramifications, such as harm to one's reputation both personally and professionally, psychological suffering, and legal issues. Thus, it is essential to communicate responsibly and with integrity online in order to prevent hurting people by making false or defamatory claims.

- **CYBERTERRORISM**

In general, cyberterrorism is the purposeful and politically motivated use of computer-based tools, networks, or technologies to carry out assaults that attempt to disrupt, terrorise, or injure individuals, groups, or governments. Because cyberterrorism may cross national boundaries and impact global infrastructure and stability, it poses serious concerns. Governments, international organizations, cybersecurity specialists, and law enforcement agencies must work together to combat this danger by putting in place strong defenses, exchanging intelligence, and creating plans to stop, identify, and deal with cyberterrorist activity.

- **COMPUTER VANDALISM**

Computer vandalism, also known as cyber vandalism or cyber defacement, is the act of making unapproved changes or damaging websites, digital assets, or computer systems. This type of cybercrime involves people or organisations purposefully altering or vandalizing internet sites without authorization; the main motivations are usually to cause trouble, make a point, or show off their prowess. Computer vandalism is prohibited and can have dire repercussions, including

loss of confidence, financial fines, legal action, and reputational harm, regardless of the motivation.

- **XSS OR CROSS-SITE SCRIPTING**

Web applications are frequently vulnerable to a form of security flaw known as Cross-Site Scripting (XSS). It happens when a hacker inserts harmful scripts typically code snippets into websites that other people are seeing. When a programme displays user inputs on a web page without adequately validating or sanitizing them, a vulnerability occurs. Organizations and developers may limit the risk of XSS attacks and protect sensitive user data and online applications by fixing these vulnerabilities and putting strong security measures in place.

CYBER FORENSIC

Cyber forensics, sometimes referred to as computer forensics or digital forensics, is the use of analytical and investigative methods to collect and preserve evidence from digital data and devices. It entails the methodical inspection of digital material in order to find and evaluate information pertinent to legal or investigative processes.

Cyber forensics is essential for tracking down offenders, deciphering the chronology of events surrounding cyber incidents, and supplying vital proof for court cases. It calls for specific knowledge of different operating systems, networks, and software programmes, as well as expertise in data recovery, computer science, and digital inquiry. Furthermore, because of technological breakthroughs and the dynamic nature of cyber threats, it is always evolving, necessitating ongoing learning and adaptation on the part of those working in the sector.

WHO COMMITTS CYBERCRIME

Cybercrime can be perpetrated by a variety of people or organizations, and the reasons for it can vary depending on the goals, skill level, and intent of the offender. Research indicates that hackers and other cybercriminals are not as uniform a bunch as previously believed[3].

- **Variation among Cybercriminals:** There is variation among cybercriminals, particularly hackers. Their differing approaches, characteristics, and motives have

[3] CREST, 2015; NCA, 2017

resulted in the creation of many offender typologies, which are growing more intricate with time.

- **The demographic patterns:** Cybercrime does not follow the trend of traditional crime, where a higher level of education and occupation frequently lowers the risk. Employment and education in the IT field may potentially raise the risk. Additionally, there is a strong correlation between household composition and cybercrime.
- **Age and Demographic data**: Contrary to popular belief, cybercriminals come in a wide range of ages, defying the cliché of the juvenile hacker. Many hackers start out as young people. Contrary to the stereotype of youthful hackers, convicted cyber-dependent criminals typically tend to be older, even if white males make up the majority of the population.
- **Routes to Cybercrime:** Research points to a developmental pathway into cyber offenses, with evidence indicating a transition from computer games, online forums, and hacking activities to more serious cybercrimes.

Given the constantly changing nature of technology and its integration into daily life, these varied traits highlight the complexity of cybercrime and the necessity for nuanced approaches to understanding, preventing, and treating these offenses[4].

CONCLUSION

To conclude, Cybercrime poses a variety of risks in the connected digital world we live in, including viruses, con artists, and online intimidation techniques. The wide range of hazards is highlighted by phishing, malware, cyberterrorism, eavesdropping, ransomware, and defamation. These risks have serious repercussions and endanger people, companies, and the integrity of society. They result in monetary instability, compromised data, damaged reputations, psychological anguish, and interruptions to vital processes.

[4] Furnell S, Dowling S (2019) Cyber crime: a portrait of the landscape. Journal of Criminological Research, Policy and Practice 5: 13–26.