CHALLENGES IN INVESTIGTING AND PROSECUTING CYBERCRIMES AS INTERNATIONAL CRIMES

Legal Upanishad Journal (LUJournal.com)
Vol 1 Issue 3 | December 2023 | pp. 177-186

Mehavarshni S, Law Student, SASTRA Deemed University, Tamil Nadu
Vishnu Praba B, Law Student, SASTRA Deemed University, Tamil Nadu

ABSTRACT

The most recent security threat in the globe today is cybercrime, which stands out from all other threats. It is obvious that combating cybercrime involves expertise and cyber security skill sets since monitoring cybercrime is extremely difficult given how globally connected the Internet is. This paper attempts to talk about the challenges in investigating cybercrimes as international crimes and the implications in prosecuting those crimes as there is no defined law for cybercrimes at the international level. The ability of international law enforcement organisations to combat these kinds of crimes on a global scale is then discussed, followed by the countries' contributions to the global development of cyber laws and the difficulties in conducting legal and practical investigations into cybercrimes.

Keywords: *cybercrime, globe, international law, investigation, prosecution, laws.*

1. INTRODUCTION

Cybercrime is a broad spectrum of illegal activities performed in the virtual world, this includes actions such as hacking, financial fraud, phishing attacks, cyber espionage, and Distributed Denial of service attacks. Cybercrime is a transnational crime that transcends national boundaries, Effective cybercrime investigation and prosecution require close cooperation between public and private parties. State governments have the capacity and authority to specify and uphold the obligations and liabilities of their inhabitants via jurisdiction. "The Extradition Act, 1962"[1] governs the extradition procedure in India. Conventions, treaties, or mutual agreements may serve as the basis for the extradition. The lack of cyber security experts in the world makes it challenging for organisations and law enforcement agencies to locate and hire people with the knowledge and abilities needed to look into cybercrimes, Law enforcement organisations must strengthen their national capability in cybercrime investigations to meet these difficulties. Law enforcement, attorneys, and specialists in digital forensics frequently need to adjust and provide new approaches to these problems. As cybercrime is a worldwide problem, investigations become more complex because it can be difficult to retrieve evidence from service providers based abroad due to a lack of international standardisation of evidential criteria and harmonised national cybercrime legislation.

2. CYBERCRIME: MEANING AND CONCEPT

The word "cybercrime" has become widely used to describe a wide range of illegal actions committed in the virtual world in the quickly changing digital age. The concept of "cybercrime" is broad and includes any illegal activity involving a computer, network, or other digital equipment[2]. It encompasses a wide range of illicit operations, including ransomware, malware assaults, phishing, hacking, fraud, theft, transmission of child pornography, cybersex trafficking, and ad fraud. Cybercrime is a threat to people's security and financial stability that has grown frighteningly common in a society where the majority of transactions are done online via digital platforms. Because of the global reach of cyber criminals, victims, and technology infrastructure, cybercrime goes beyond national borders.

[1] Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India)

[2] Apoorva Bhangla and Jahanvi Tuli, *A Study on Cyber Crime and its Legal Framework in India*, 4(2)INT'L J. L. MGMT. & HUMAN. (2021)

The ability of technology to take advantage of security flaws in both personal and corporate settings enables cybercrime to take numerous forms and to constantly change. Computer-based versions of financial crimes, such as ransomware, fraud, and money laundering, as well as crimes like stalking and bullying, are easier to do due to the internet's speed, convenience, obscurity, and lack of boundaries.

Cybercrime can include copyright violations, system interferences that harm network availability and integrity, and unlawful data interception[3]. It can be executed by people or organisations with different degrees of technical proficiency, ranging from those who take advantage of human flaws to highly coordinated international criminal organisations possessing competent developers and pertinent knowledge. Because a cybercriminal need not be physically present to commit a crime, the volume and speed of cybercrime activities have increased due to the necessity of internet connectivity. Identity theft, phishing, ransomware attacks, and fake emails are examples of common cybercrimes. These crimes don't always require a high level of technological competence and frequently take advantage of human flaws. Cross-border attacks by cybercriminals can be carried out via the internet, making it challenging to identify and bring them to justice. Because of the accessibility of virtual places, cybercrime has grown commonplace and has resulted in substantial harm and financial losses. Some of the common types of Cybercrimes, challenges in prosecuting Cybercrimes as international crimes and the reason for mentioning Cybercrime as international crimes are explained below.

3. TYPES OF CYBERCRIME

3.1 Hacking and unauthorized access

Hacking, or unauthorised access to computer systems, is one of the most common types of cybercrime[4]. Cybercriminals use a variety of strategies, including malware, phishing, and brute-force attacks, to enter networks and systems without authorization. Once inside, they might use ransomware to force victims to pay them money, steal confidential data, or interfere with operations.

[3] Showkat Ahmad Dar and Dr. Naseer Ahmad Lone, *Cyber Crime in India*, 43(4)SAMBODHI (2020)

[4] *Id.*

3.2 Financial Frauds

Identity theft is a common cybercrime in which thieves steal and use people's personal information to commit financial crimes. Credit card numbers, login credentials, and social security numbers are just a few examples of the stolen data. Cybercriminals utilise this data to carry out a variety of financial fraud schemes, including starting false accounts, making illegal transactions, and draining bank accounts. Beyond just financial losses, victims frequently have to endure a difficult process to have their corrupted identities restored[5].

3.3 Phishing Attacks

Cybercriminals use phishing, a deceitful technique, to persuade people into disclosing sensitive information, such as login credentials or bank account information. Usually, these attacks involve emails, texts, or websites that look authentic and pose as reliable sources. Phishing attacks frequently take advantage of human psychology by manipulating their target into doing things that will benefit the attacker by playing on their sense of importance or trust. Phishing techniques are becoming increasingly advanced and common as technology progresses.

3.4 Cyber Espionage

Cyber espionage has emerged as a common and alarming cybercrime in the context of nation-states and geopolitics. Hacking into other countries' digital infrastructure is a technique used by state-sponsored actors and individual cybercrime organisations to get trade secrets, private data, and other advantages. Cyber espionage is a complex and varied danger on the international scene, with motivations ranging from geopolitical influence to commercial gain.

3.5 Distributed Denial of Service (DDoS) Attacks

DDoS attacks entail flooding an opponent's web services to prevent users from accessing them. Cybercriminals accomplish this by overloading the target's servers with traffic, which interferes with regular business activities. DDoS assaults can be employed for many different things, such as competition sabotage, retaliation, or serving as a diversion from other cybercrimes.

[5] Apoorva Bhangla and Jahanvi Tuli, *supra* note 2

4. WHY CYBERCRIMES SHOULD BE TREATED AS INTERNATIONAL CRIMES?

Almost cybercrime is a transnational crime that transcends national boundaries, it ought to be handled like any other kind of criminal activity. Cybercriminals can operate from any location in the world, and the global impact of their actions can be felt by people, companies, and governments. It is challenging for local law enforcement agencies to look into and solve these crimes due to the absence of standardised national cybercrime laws, international standardisation of evidentiary requirements, mutual legal assistance on cybercrime matters, and timely collection, preservation, and sharing of digital evidence between countries. In order to effectively combat cybercrime, international cooperation is necessary. A legal basis for international collaboration is provided by the Convention on Cybercrime, which includes both general and specialised provisions. These include the duty on the part of nations to collaborate as much as possible, immediate action to preserve data, and effective mutual legal support. Numerous more Council of Europe treaties on international cooperation in criminal affairs supplement the Convention. In order to tackle cybercrime, Interpol is essential for fostering cross-sector collaboration and facilitating international law enforcement cooperation. Effective cybercrime investigation and prosecution require close cooperation between public and private parties. However, there are currently difficulties in looking into these crimes since there is a lack of specialised knowledge for the investigation and primarily because there is not sufficient appropriate international law to deal with these crimes. In the next part of this article let’s look at the major challenges in prosecuting Cybercrimes.

5. CHALLENGES WITH EXTRADITION AND JURISDICTIONAL BOUNDARIES

State governments have the capacity and authority to specify and uphold the obligations and liabilities of their inhabitants via jurisdiction, which is connected to sovereignty. Cyberspace, in particular, the information and communications technology (ICT) infrastructure of states, is subject to territorial sovereignty. When outsiders use ICT in foreign nations without the host nation's or its law enforcement officials' knowledge or consent, state sovereignty may be breached. Other variables, like as the nationality of the perpetrator, the victim, and the effects of the cybercrime on the interests and security of the state, determine the jurisdiction for cybercrime. The word "extradition" originates from the Latin "extradere," which means "delivery of fugitive," "surrender of criminals," or "handing over of criminals." The international mechanism for the timely repatriation of criminals from other nations is extradition. Extradition is a bilateral process in which an accused person is turned over to a second country upon its request so that the other nation can decide whether to prosecute him for an offence he committed within its borders.[6] In the case of Gary McKinnon v. United States[7], British hacker Gary McKinnon was charged with breaking into computer networks used by the Pentagon and NASA. The difficulties with extradition and cross-border jurisdiction in cybercrime cases are best shown by this case. After the US requested McKinnon's extradition from the UK, a ten-year legal dispute ensued. The UK government ruled in 2012 that McKinnon's health would prevent him from being extradited. In the case of R v. Love[8], British hacker Laurie Love was facing extradition to the US on allegations of breaking into US government networks. Concerns regarding the consequences of extradition in cybercrime cases for human rights were brought up by this case. It also highlighted the difficulties in fostering global collaboration and the possibility of conflicting legal norms.

The flexibility of the extradition procedure fosters mutual trust and confidence and helps to strengthen the relationships between the countries involved. Typically, the country where the crime has been committed is in a comfortable position to adjudicate due to easy access and the presence of evidence. In addition, extradition ensures that "no crime goes un-adjudicated and to bring the offender to justice." The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, is the first international treaty that aims to combat cybercrime, or Internet and computer crime, by harmonising national laws, enhancing investigative methods, and fostering international cooperation. It is also the first treaty that allows for the extradition of offenders for cybercrimes, and it can only be permitted "when an offence is a punishable at least with severe imprisonment of One year or more under laws of both of the countries and both are the party to the pre-commission of the alleged offence, a bilateral treaty for the extradition of offenders. Further extradition is permitted if the commission of criminal offence is established in accordance with the terms and provisions of the Budapest Convention.

[6] Shiv Raman., *Cyber Crimes and Extradition Issues in India*, 15(11) J. ADVANCES & SCHOLARLY RSCHS. ALLIED EDUC. (2018)
[7] McKinnon v. United States, Civil Action No. CCB-12-179, (D. Md. Mar. 5, 2012)
[8] R. v. Love (R.J.), (1995) 174 A.R. 360 (CA))

"The Extradition Act, 1962" governs the extradition procedure in India. Conventions, treaties, or mutual agreements may serve as the basis for the extradition. At the moment, India has extradition agreements with around 39 nations. Important nations like India have refused to ratify the Budapest Convention since they were not involved in its preparation. This refusal has occurred since the Convention came into effect. Russia has consistently declined to assist in law enforcement investigations pertaining to cybercrime and opposes the Convention, claiming that its acceptance would violate Russian sovereignty. It is the first legally binding multilateral measure to control cybercrime. Following a spike in cybercrime in 2018, India has begun reevaluating its position on the Convention; however, worries about exchanging data with international agencies still exist.

6. LACK OF RESOURCES AND EXPERTISE TO CONDUCT WORLDWIDE INVESTIGATION

Cyber threats are ever-changing and getting more advanced. Sustaining a high level of proficiency and continuous training is necessary to stay updated on the most recent strategies and methods employed by cybercriminals[9]. The lack of cyber security experts in the world makes it challenging for organisations and law enforcement agencies to locate and hire people with the knowledge and abilities needed to look into cybercrimes. Since cybercrimes frequently cross national boundaries, working with law enforcement organisations abroad is essential. Proficiency in managing the legal and jurisdictional complexities of global cybercrime inquiries is crucial. Effective cybercrime investigations frequently call for the employment of specialised digital forensics instruments, which can be costly and require training to operate correctly.[10]

An investigator would find it challenging to carry out a thorough investigation in a foreign nation if they are not fluent in the local language because a lot of information could be missed if they are unable to comprehend the data being gathered. In a similar vein, a cybercrime investigator needs to have an understanding of the "language" that machines use to analyse data and converse with one another. The ability to identify the language in which written evidence is written is helpful even if an investigator in the field may not be fluent in

[9] Raksha Chouhan, *Cybercrimes: Evolution, detection and future challenges*, 10(1) IUP J. INFO. TECH. (2014)
[10] Kai-Lung Hui, Seung Hyun Kim and Qiu-Hong Wang, *Cybercrime Deterrence and International Legislation*, 41(2) MIS QUARTERLY (2017)

all spoken languages. This is because written evidence may be important and will undoubtedly aid the investigator in locating a translator.

The number of cybercrime cases that national specialised units in any specific nation investigate is limited. Such a practice is rendered useless by the widespread use of information and communication technologies in criminal investigations. In addition to the limited capabilities of law enforcement, cybercrime investigators have a short lifespan of competence. Law enforcement organisations must strengthen their national capability in cybercrime investigations to meet these difficulties. Additionally, they must endeavour to increase the world's ability to fight cybercrime by exchanging information with international partners and educating foreign law enforcement officials about cybercrime. Investigating cybercrime presents a number of difficulties for law enforcement organisations. The inability of these agencies to carry out these kinds of investigations is one of the primary challenges. The capacity of law enforcement to look into cybercrime varies by nation and even between its authorities.

7. DIFFICULTY IN CONDUCTING LEGAL AND PRACTICAL INSTIGATIONS IN CYBERCRIME

Because of the peculiar characteristics of these crimes and the digital environment in which they take place, prosecuting cybercrimes presents a number of practical and evidentiary difficulties. Law enforcement, attorneys, and specialists in digital forensics frequently need to adjust and provide new approaches to these problems. These are some of the evidential and practical difficulties facing cybercrime prosecutions. Legal and practical investigations are faced with several obstacles due to the nature of evidence in cybercrime. Reconstructing digital evidence accurately and entirely can be difficult since information frequently circulates over several real and virtual spaces, including cloud services, personal network-attached storage devices, and online social networks. An important difficulty for investigators is the diversity and dispersion of evidence, which necessitates greater skill, resources, and time to handle and maintain efficiently. The number and complexity of digital evidence also make management, processing, and storage challenging, which makes the investigation process even more difficult. For digital evidence to be admitted in court, it must be kept private and trustworthy. However, this creates another problem because improper guidelines or justifications may cause electronic evidence to be rejected.[11] Furthermore, safeguarding and preserving digital evidence is severely hampered by the possibility of data breaches, cyberattacks, and manipulation. Finally, because cybercrime is a worldwide problem, investigations become more complex because it can be difficult to retrieve evidence from service providers based abroad due to a lack of international standardisation of evidential criteria and harmonised national cybercrime legislation. To overcome these obstacles, better international cooperation upgraded digital evidence management systems, and the creation of appropriate standard formats and abstractions to handle the complexity of cross-border cybercrime investigations are all necessary.

The next problem is the maintenance of the privacy of user data while giving it as evidence. There are numerous factors contributing to the difficulty of protecting the privacy of data used as evidence in cybercrime investigations. First off, since digital evidence frequently includes private and sensitive material, its growing amount and diversity raise serious privacy concerns. In order for digital evidence to be admitted into court, it must be kept private and authentic. However, if adequate guidelines and explanations aren't provided, electronic evidence may be rejected, which can complicate matters both legally and procedurally. Securing and safeguarding digital evidence is further complicated by the possibility of data breaches, cyberattacks, and tampering. Ensuring the integrity and admissibility of digital evidence in court proceedings requires the subtle detection and prevention of data breaches and tampering. The worldwide scope of cybercrime makes matters more difficult because cross-border investigations necessitate coordination and information exchange between several jurisdictions, each with unique procedural and legislative requirements. [12]In order to effectively conduct cross-border cybercrime investigations, stronger digital forensics skills, increased international collaboration, and the creation of standardised legislative frameworks are required to tackle the difficulty of data privacy concerns. In order to handle the complexity and privacy issues related to digital evidence in cybercrime investigations, these actions are important.

Another major challenge is the anonymity of the identities of cybercriminals. Investigating cybercrimes across international borders is made more difficult by the anonymity of hackers.

[11] Shiuh-Jeng Wang, *Measures of retaining digital evidence to prosecute computer-based cyber-crimes*, 29(2) COMPUT. STANDARDS & INTERFACES (2007)

[12] Mohammed Alghamdi & Mohammed Almushilah, *Digital forensics in cyber security -recent trends, threats, and opportunities*, 8(3) PERIODICALS ENG'G & NAT. SCI. (2020)

Cybercriminals frequently hide their genuine identities and locations using a variety of online anonymity tools and strategies, which makes it challenging for law enforcement to link criminal activity to particular people or organisations. Cybercriminals can encrypt traffic, conceal their IP addresses, and carry out illegal operations without disclosing who they are with the help of anonymization tools like proxy servers and anonymizing networks like Tor. Because of this anonymity, it is more difficult to identify the devices and people behind cybercrimes, which makes it difficult for investigators to find and capture the offenders. The worldwide scope of cybercrime makes matters more difficult because cross-border investigations necessitate coordination and information exchange between several jurisdictions, each with unique procedural and legislative requirements. Addressing cybercrimes committed by anonymous perpetrators is made more difficult by the absence of worldwide standardisation of evidentiary requirements and harmonised national cybercrime legislation. In order to effectively assist cross-border cybercrime investigations, stronger digital forensics capabilities, increased international collaboration, and the development of standardised legal frameworks are required to overcome the obstacle of cybercriminal anonymity.

8. CONCLUSION

Since cybercrime is an ongoing worldwide threat that crosses national borders, it is an organised criminal issue that affects the entire world. Cyberterrorism, theft, and online fraud are just a few of the many forms of cybercrime. It has been observed that the globalisation of technology and the remarkable growth of ITs that have affected criminal activity are among the most significant factors that assist the commission of this crime. Several obstacles to prosecuting cybercrime as an international crime have been discussed in this research article. In order to address the serious issue of cybercrime on a global scale, it is also necessary to build international law and specialised authorities. To address the situation peacefully, the nations must cooperate with one another.