International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 26-10-2023, Accepted: 11-11-2023, Published: 27-11-2023
Volume 5, Issue 4, 2023, Page No. 111-114

Cyber crimes: Emerging issue and challenge

Maria Binte Belal[1], Akhilesh Ranaut[2]
[1] Department of Law, Chandigarh University, Punjab, India
[2] Professor, Department Law, Chandigarh University, Punjab, India

Abstract
The internet's rapid expansion has had enormous positive effects on society. The internet is used daily by millions of people for a wide range of activities, including leisure, communication, education, commerce, and more. However, a small but significant minority of internet users engage in criminal conduct online. As a result, several countries have passed cybercrime legislation to try to stop criminal conduct on the internet. Unfortunately, cybercrime has persisted despite these laws designed to combat it. Cybercriminals are able to hide their identities behind a mask of anonymity because to the design of the internet. Criminals take use of the anonymity afforded by the Internet to perform a broad range of illegal activities, including fraud, the dissemination or marketing of child pornography, the selling of jewels and drugs, and many more. The Space Transition Theory is only one of several that posit anonymity as a major contributor to the exponential growth of cybercrime. In terrestrial space, people do not commit crimes because of their social standing. However, the anonymity provided by the Internet allows them to break these rules and engage in crimes. In this research, the author will look at some of the most important causes behind criminal law's diminished effectiveness in fighting cybercrime.

Keywords: Cybercrime, cyber law, cyber challenges, cyberspace, cyber criminals

Introduction

The fast development of technology and the broad adoption of the internet have revolutionised our society by bringing together previously unconnected individuals, organisations, and governments. Despite the many advantages, cybercrime has emerged as a new kind of criminality in the digital era. Cybercrimes are any illegal activity committed over the internet that may affect anybody from a person to an entire country. Thefts of personal information and financial resources as well as other forms of internet fraud have arisen as major dangers in recent years. There are a number of causes behind the increase in cybercrime [1]. First, the availability and declining cost of internet-connected gadgets have greatly increased the number of possible victims, making everyone with an online presence a target. In addition, criminals may commit their acts from any location in the globe because to the anonymity the Internet provides, making it exceedingly difficult to track them down and bring them to justice. Cybercrimes have a significant and far-reaching effect. There is always a chance that a financial institution, organisation, or individual will suffer a loss of funds, a data breach, or damage to their reputation online. Critical infrastructure can be disrupted, national security might be compromised, and public safety can be at risk if there is a large-scale cyberattack. Victims of cybercrime typically feel violated and lose trust in others, which can have a significant impact on their mental health. Law enforcement agencies and judicial systems face new obstacles in the fight against cybercrime as a result of the dynamic nature of technology [2]. The speed and complexities of digital crimes make it difficult for conventional investigation techniques and legal systems to keep up. Due to the transnational scope of cybercrime, international collaboration and coordination are essential for successful prosecution. Knowing the legal framework and the difficulties in investigating cybercrimes is essential in light of the evolving threat scenario. It is clear that strong legal measures and a thorough grasp of the difficulties are necessary to tackle cybercriminal activities in order to uncover the intricacy of these crimes and their effects on individuals, corporations, and society at large.

Literature Review

Jurisdictional Challenges

Currently, the international system is based on the idea that each nation has complete autonomy inside its own borders. This means that every nation has the power to legislate, prescribe, and enforce its own laws, as well as to settle any conflicts that may arise from doing so. Therefore, each nation-state's criminal justice system is only effective within its own borders. However, the boundaries of countries have little bearing on what is possible in cyberspace. Online criminal activity is not limited by borders or national jurisdictions. It is possible for a cybercriminal to perform an act of cybercrime from the safety of his own home in one nation, with repercussions felt in another [3]. Many difficult jurisdictional concerns may up when a cybercrime victim is in another nation. Enforcement of the criminal laws of the victim's nation against the perpetrator of the cybercrime would be hampered by a variety of legal and practical obstacles.

Challenges Relating to Extradition of Criminals

When a person is suspected of committing a crime in one country, they may be extradited to face charges in another country. Due to the inherent close proximity of the offender to the victim in every traditional crime, extradition is rarely necessary. As far as online crimes involve, however, such is not the case. A criminal can use internet technology to commit crimes hundreds of miles abroad in completely different legal jurisdictions. As a result, a significant amount of cybercrime occurs across international boundaries. As a

result, extradition is a serious obstacle to the prosecution of cybercriminals. No treaty, convention, or other body of international law imposes upon a state the responsibility to extradite suspected criminals or cybercriminals to another state for prosecution [4]. Treaties between countries, both bilateral and multilateral, allow for extradition to occur. If no such accords exist, extradition must be pursued in accordance with the national regulations of the jurisdiction from which the extradition is requested. Such international laws typically necessitate that the seeking state go to a special court or tribunal. In either case, extradition is a time-consuming and complicated procedure.

Challenges in Existing Law Enforcement Mechanism

The existing criminal investigation/law enforcement system, including operational processes, has evolved to handle conventional offences. Cybercrimes and cybercriminals are now being handled using the same method. However, the current system is unable to cope with cybercrime since it lacks many of the characteristics of traditional crime in the physical world. The physical nature of the actual world means that most crimes occur between two people. In the context of cybercrime, however, no such assumption can be made [5]. Through the use of automated tools, hackers may significantly increase the rate at which their crimes are done. The standard system of investigation and prosecution is readily overwhelmed by crimes of this magnitude. It might be difficult for law enforcement to successfully investigate and punish cybercrimes due to limited resources. Limitations in funding, availability of trained staff, and ease of access to cutting-edge technology and techniques are all examples of resource restrictions that prevent complete investigations of cybercrime from being carried out. Investigations of cybercrime call for specialised training and information. Experts such as digital forensic analysers, cybersecurity specialists, and lawyers are in limited supply, however. Investigations and prosecutions of cybercrimes may be hampered by a insufficiency of specialised people [6]. The ability of law enforcement to keep up with the ever-evolving methods used by cybercriminals is frequently outpaced by these developments. Countering sophisticated cyberattacks requires access to cutting-edge techniques and technology, such as comprehensive analytics programmes, network assessment equipment, and intelligence-based threat systems.

Challenges Relating to Attribution of Criminals

Officers on the field know from experience that capturing a cybercriminal is difficult. Cybercriminals are able to protect their anonymity and location because to the special technical characteristics of the internet. Because of this, it is incredibly challenging for law enforcement to identify and track down the perpetrator. The criminal may also employ technological means to assume the identity of a non-criminal in order to throw off law enforcement. In addition, the perpetrator and victim of a cybercrime need not be in the same place at the same time [7]. A criminal in one part of the world can perform cybercrimes that affect people thousands of kilometres distant from where the crime was committed, because to the decentralised structure of the internet. Extreme difficulty has been encountered by law enforcement in apprehending cybercriminals because of the great distance between the site of the police inquiry and the place of operations of the cybercriminal. Crimes may be committed in mass quantities using cyberspace technologies in a very short amount of time. Cybercriminals may conduct many more offences in a short amount of time by automating the process of committing crimes like online fraud. With the use of automated technologies, offenders may begin the victimisation process and then step back, allowing the automated systems to do the job [8]. By taking advantage of technological advancements, cybercriminals can dramatically accelerate the rate at which they can conduct crimes. The current criminal justice system is unprepared to deal with these kinds of cases.

Inadequacy of Professionals in Prosecution

There are currently no dedicated cybercrime courts in most countries of the world. Circumstances involving cybercrime are tried in the same criminal courts that hear instances involving physical crime. Therefore, the same public prosecutor handles both traditional and online criminal cases. To become a public prosecutor, one must have worked as an attorney for at least the minimum amount of time required by law. In India, for instance, a public prosecutor must have at least seven years of experience as an attorney. There are no required technical skillsets. However, a high level of expertise is necessary when prosecuting cybercrimes [9]. Therefore, regular prosecutors would struggle to handle cybercrime cases because they lack awareness of the technical aspects of the internet and ICT. This is a significant disadvantage that is likely to have an impact on the conviction rate. Technology is essential to the investigation of cybercrimes. The investigative organisations utilise expensive technology and devices to track out cybercriminals. To achieve this goal, law enforcement personnel must get adequate instruction in the use of technological resources. In the United States, for example, only the Federal Bureau of Investigation (FBI) has the means to buy expensive devices and adequately train its workers on the use of technology [10]. However, most other nations' law enforcement agents lack the necessary training to investigate cybercrimes due to a lack of resources.

Availability of Tools to Commit Cybercrime

The widespread availability of the computers, mobile phones, etc., needed to perpetrate cybercrime is a major factor in the ineffectiveness of cybercrime laws un curbing criminal activity online. Cybercrime used to need a high level of technical expertise in the early days of the internet. However, it is now easy to obtain specialised software that aids in the commission of cybercrimes. As a result, the importance of a cybercriminal's technological expertise has diminished significantly [11]. The majority of these specialised pieces of software do double duty, aiding the cybercriminal in both his criminal activities and his attempts to conceal his true identity. The vast majority of countries have not yet passed legislation outlawing the usage of such specialised software. There will always be a constant increase in cybercrime as long as technology is allowed to help cybercriminals conduct cybercrimes. As the internet, digital gadgets, and communication networks continue to develop at a rapid pace, new security holes and attack routes become available to hackers. Constant revision of legal structures is required to accommodate new technology. Legislation must be kept current in order to deal with the ever-evolving concerns posed by cybercrimes. The evolving nature of cyber threats necessitates the creation of new

crimes, stricter punishments, and legal frameworks [12]. Staying ahead of new cyber dangers requires close cooperation between law enforcement, policymakers, and cybersecurity specialists. The creation of successful solutions to fight these dangers is made possible by ongoing study and analysis of developing trends, tactics, and technology.

Challenges Posed by Introduction of AI

Cybercriminals are rapidly automating assaults, exploiting weaknesses, and evading protection with the help of AI technology. Cybercrimes like systematic phishing attempts and AI-driven viruses are brought up in light of how AI might increase their technical ability and pace. Cybercriminals have used AI technology to scale up their operations and improve the efficacy of their assaults. Phishing tactics may be automated and personalised with the help of AI, making them more effective and harder to spot [13]. With the help of AI algorithms, social engineers can sift through mountains of data to craft convincingly authentic-looking phishing emails. AI is being used by cybercriminals to create and release malware that can change and improve in real time, allowing it to evade conventional defences. Malware powered by AI may use evasion strategies, adapt its behaviour to the context in which it is running, and even acquire information from how it communicates with its intended targets. Artificial intelligence (AI) is a potential weapon in and of itself. For the purposes of fraud or extortion, for instance, AI systems may be taught to make convincing deep fake films or voice recordings [14]. Attacks may be automated with little human interaction by using AI algorithms deployed by malicious actors to assess and exploit software or system weaknesses. The use of artificial intelligence (AI) in cybercrime poses serious issues for cybersecurity experts and law enforcement. A proactive and adaptable strategy is required to detect and fight AI-driven cybercrimes in light of the rapidly developing and more available AI technology. To counter the ever-evolving risks posed by AI-enhanced assaults, it is essential to build AI-based defensive mechanisms such as recognising anomalies and behavior-based analysis [15]. Cybersecurity professionals and organisations throughout the world must work together and share data if they are to remain ahead of fraudsters who exploit AI for harmful ends.

Objective

a. To analyse how cybercrime has changed the landscape of criminology in the digital era.
b. To investigate the difficulties experienced by law enforcement in successfully responding to cybercrime.
c. To examine how technical developments, international collaboration, and jurisdictional questions have influenced law enforcement's response to cybercrime.
d. To assess how well these strategies prevent cybercrime and safeguard citizens, companies, and governments.

Hypothesis

This research hypothesises that societies can effectively lessen the impact of cybercrime if they gain a thorough familiarity with the many facets of these offences.

Research Methodology

Doctrinal research methodology is the major approach taken in this research [16]. Also, this research relies entirely on secondary sources because no primary research was conducted. These secondary sources are expected to provide with in-depth understanding of the issues in hand to settle future research directions.

Discussion

When prosecuting cybercrime, visible or material proof, which is widespread in cases of real-world crime, is relatively uncommon. Since cybercrimes are performed in cyberspace, which is a virtual world, intangible digital evidence is typically offered in court to achieve a conviction. Investigative organisations, used to collecting physical evidence, have a new issue with the acquisition of this type of evidence [17]. The handling of digital evidence is problematic since it can be readily manipulated or deleted. As a result, investigators often need to spend a significant amount of time examining digital data in order to uncover pertinent evidence. A significant proportion of police officers today lack the skills necessary to process digital evidence. Most international laws created in response to cybercrime do not mandate a unique process for the search and seizure of information on the internet. Thus, while gathering digital evidence, law enforcement officials depend on the established procedure of search and seizure. However, many problems arise when law that was developed to handle activities in the real world is applied to behaviour in cyberspace. For instance, digital evidence is much more difficult to manage and readily corrupted than physical evidence [18]. Therefore, digital evidence needs to be acquired and stored securely. This necessitates spending a lot of money on things like new gear and training for police officers. The majority of nations cannot afford to invest so much money right now.

A major obstacle to effectively implementing cybercrime laws is the underreporting of cybercrimes by victims, especially enterprises and corporations. It has been stated that just 2% of internet crime occurrences were reported by companies to law enforcement authorities in the United Kingdom in 2019, according to the CVS. Compared to other crimes, such as auto theft (100%), burglary (80%), etc., this was far lower than the reported rates. This pattern is also observed in the population at large. Only 3% of adult internet users in England and Wales acknowledged hacking/unauthorized utilisation of data in the Crime Survey for those two countries in 2020 [19]. Due to insufficient reporting, not enough information or statistics are available on cybercrime. As a result, the public and companies are misinformed about the scope of cybercrime. Furthermore, policymakers tasked with combating cybercrime have struggled to develop effective long-term strategies due to a lack of relevant data. The inability of criminal law to combat cybercrime is partially attributable to the lack of sufficient cybercrime legislations enacted by nation-states. Only 79 of the 201 nations surveyed in 2015 have any sort of cybercrime legislation in place. In other words, just approximately 40% of the world's countries have legislated against cybercrime. In addition, 47 of the 79 countries with cybercrime legislation are located in Europe [20]. This worrying trend has allowed crooks to avoid punishment by moving their operations to a nation that has not yet passed cybercrime legislation. Also, the concept of double

criminality precludes the extradition of such an offender since extradition is only allowed if the claimed deviant behaviour constitutes a crime in both the asking state and the sought state.

Conclusion

Current international law is founded on the idea of state sovereignty. Since there is no central body to implement international law, it falls on individual governments to do so. Due in large part to the ineffectiveness of international law, transnational cybercrimes are increasing at an alarming rate. The Convention on Cybercrime, drafted by the Council of Europe, entered into force in 2004. The Council of Europe may only recommend that member states implement the measures it recommends; it cannot mandate that they do so [21]. Even while the Convention calls for international cooperation in investigating cybercrimes, the Council of Europe has no authority to compel any state member to do so. As a result, cybercrime rules have not been effectively enforced due to the non-binding character of international law and the absence of an effective enforcement mechanism. Together, the aforementioned and other elements have made it exceedingly challenging for criminal law to work efficiently to restrict cybercrimes. All of this highlights the necessity for the creation of an international court or tribunal dedicated to investigating and prosecuting serious transnational cybercrimes. There is now insufficient support on a global scale to establish a universal court or tribunal. There is a need to deploy cybercrime prevention techniques even as this international framework is being considered. Cybercrime prevention strategies that use a combination of technological and non-technical measures should also be supported. Important cybercrime prevention tactics include public education about the issue, the implementation of strong cybersecurity practises, the use of private online police forces, and many others.

References

1. Nicholas Tsagourias and Michael Farrell, Cyber Attribution: Technical and Legal Approaches and Challenges," 31 *European Journal of International Law* (2020).
2. Nori Katagiri, Why international law and norms do little in preventing non-state cyber-attacks, 7 *Journal of Cybersecurity* (2021).
3. Duncan B. Hollis and Martha Finnemore, Constructing Norms for Global Cybersecurity," 110 *American Journal of International Law*, 2016, 425–79.
4. Josephine Helen Dwan, Tamsin Phillipa Paige and Rob McLaughlin, Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers?," 3 *Law, Technology and Humans*, 2022, 52.
5. Paul Cornish. *The Oxford Handbook of Cyber Security* 256 (Oxford University Press, Oxford, 2021), at p. 256.
6. Ben Buchanan, *The Cybersecurity Dilemma Oxford Scholarship Online* 88 (Oxford University Press, 2017, 88.
7. Majid Yar and Kevin F Steinmetz, *Cybercrime and Society* (SAGE, 2019).
8. David Wall, *Crime and Deviance in Cyberspace* (Routledge, London, 2016).
9. Jahankhani H. *Cyber Criminology* (Springer, Cham, Switzerland, 2018).
10. Leukfeldt R, Thomas J Holt. *The Human Factor of Cybercrime* (Routledge, 2019).
11. Prerna Agarwal *et al*. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms* (De Gruyter, Berlin, 2021).
12. Matthew Richardson, *Cyber Crime: Law and Practice* (Wildy, Simmonds & Hill Publishing, London, 2019).
13. Raul AC. *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, London, UK, 2021).
14. Sunil. C. Pawar and R. S. Mente, Cyber Crime, Cyber Space and Effects of Cyber Crime" *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 210–4 (2021).
15. Andrew Murray, *INFORMATION TECHNOLOGY LAW: The Law and Society*. (Oxford Univ Press, S.L., 2019).
16. Mark Van Hoecke, *Methodologies of Legal Research* 32 (Bloomsbury Publishing, 2011), at p. 32.
17. Kevin F Steinmetz and Matt R Nobles, *Technocrime and Criminological Theory* (New York ; London Routledge, 2018).
18. Han-ho Park, A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime," 16 *Korean Association of Criminal Psychology* 85–98 (2020).
19. Michael Schmitt, The United Kingdom on International Law in Cyberspace" *EJIL: Talk!*, 2022*available at*: https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace/ (last visited July 26, 2023).
20. Richard A Clarke, *FIFTH DOMAIN: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* (Penguin Books, S.L., 2020).
21. A Mihr, Cyber Justice: Cyber Governance Through Human Rights And A Rule Of Law In The Internet," 13 *US-China Law Review*, 2016.