International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploring the Intersection of Technology and Criminal Justice: Cybercrime, Cybersecurity, and AI

K. Hemali

Student, Anantha Law College

Abstract

The influence of technological development on criminal justice system has become more evident in modern world. This is because the upgraded and refined technological metamorphosis has helped not only in the prevention of crime but also come to the aid of expeditious legal proceedings.

Traditional crime differs from cybercrime in the sense that in traditional crimes physical tools are used and the material distance is wide between the offender and the victim. While cybercrime occurs in the realm of digital space with intention of financial harm or theft. The role of Artificial Intelligence (AI) has become very important in cyber forensics and also to make better the opportunities to successfully solve cybercrimes. Since the technology of AI is so advanced that it can impersonate the human characteristics, it is necessary that cybersecurity measures must be implemented by organizations to counter the strategy of AI-enabled cybercriminals. One can see that cybercrimes are not limited but encompass the whole world. Keeping this in view when India hosted BRICS Summit, cybersecurity was an important area of concern and was a beginning to and adoption of many related regulatory and legislative measures. Since technology can very effectively reduce the gap between law enforcement and the public, its incorporation in investigation methods helps police to solve crimes effectively and maintain law and order.

1. Introduction

India has allocated large amount of resources for technological advancement in its various processes and spheres of life. The prevention of crime, a vital role of the State and the Legal industry is not immune to this change. The intersection of technology and criminal law making its presence everywhere and the new technological developments present both benefits and challenges for law enforcement and the legal framework in the country. The advancements in technological developments are meaningfully influencing the modern-day criminal justice system by transforming the methods employed by professionals in the field. The core functions which include crime prevention, legal proceedings and the rehabilitation of offenders are augmented by improved technological innovations. In the criminal justice system, Legal technology encompasses GPS systems, powerful computer system along with internet technologies, advanced cameras, and robots. This transformation is driven by the need to enhance efficiency, accountability, and effectiveness in crime prevention, legal proceedings, and rehabilitation of offenders.

2. Criminal justice technology

Crime-solving techniques and procedures have advanced significantly over time. Experts in the field now acknowledge the importance of integrating crime scene analysis, physical evidence, witness statements,

and documentation for successful investigations. Today, teamwork is essential in solving crimes. Effectively processing crime scenes by identifying, collecting, and preserving all relevant evidence and information improves investigative skills[i]. Criminal justice technology refers to the advanced tools and resources that have become increasingly ubiquitous across law enforcement agencies nationwide. Although the commission of crimes have been there from times immemorial, the solving of crimes has advanced in years with access to new and progressive technology. Different revolutionary technological changes have widened the scope of enforcement of law and criminal justice in important ways. Thus from fingerprint scanners to robotics to smart devices these have played an important role in empowering police personnel and the law enforcement agencies. From the limited or practically non existent technology usage in the 1700's to the present day Information technology where mobile computer terminals (MCTs) are used the police have used these innovations effectively to control crime

3. Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device and may be carried out by individuals or organizations. These can be novice hackers or may be highly technically in their skill of using advance techniques of cybercrime. It is frequently observed that cybercrimes are mostly committed by cybercriminals or hackers with intention of making money. However, it is also seen there coulda political or personal purpose or agenda to damage computers or their respective networks for reasons other than profit.

Cybercriminals use various illegal ways to continue with their criminal activities. It is seen that when computers are targeted by the cybercriminals it results in damage to them or may even stop these devices from working. One of the ways in which these illegal activities result in is a Denial-of-Service (DoS) attack wherein preventing a business providing software service to its customers or users may be stopped from using a network or a website. Of course these different criminal activities which are done online may be done in isolation or together like firstly targeting computers with viruses and later using them to spread the malware to other machines or over a network. The computers are also used as an accessory to commit cybercrime by storing stolen data. Thus we can say that Cybercrime is a criminal activity where computers are used to commit different crimes and also this type of activity which is criminal in nature targets computers by using viruses and other kinds of malware.

One of the ways in which Cybercrime is committed is by means of using computers or networks to spread illegal information, illegal images or malware. Theft of financial or card payment data, Cyberextortion where there is a demand for money to prevent a susceptible or threatened attack, Illegal gambling, Soliciting, producing, or possessing child pornography, Illegal gambling, Selling illegal items online, Infringing copyright, Email and internet fraud, etc. are some of the types of cybercrime.

3.1 Types of cybercrimes

- Identity Theft: A crime where an attacker employs fraud or deception to acquire personal or sensitive information from a victim and then misuses that information to impersonate the victim. Victims' personal information is stolen and used to carry out online transactions without their consent.
- Online Trolling: It comprises of sharing especially through social media different characters, marks, badgering symbols etc. Thus in an online trolling defamatory content is posted by persons on online forum or persons may be attacked directly by way of online trolling.
- Illegal Downloads: There are some apps made by hackers either for hacking data or with a special purpose gaining profit. The popular games like PUBG and Blue Whale Game are made in such a way

so the players need to purchase cards with money, giving opportunity to the hackers to make profit.

- Hacking: The deletion of personal and or private data can be described as Hacking. This stealing of personal information on a on a social networking site and is done through a computer system comes under the meaning of Hacking and in this it is found that many social website users receive false electronic mail with fake operator directions. Thus with these hundreds of phishing emails sent to hundreds of people are results in shutting down of business communication.
- Virus Attacks: Here criminals produce harmful viruses which are released into the computers, which then harm and delete personal information. Thus, hackers would strike other people's accounts in different ways including different kinds of photos or video etc.

4. Artificial Intelligence

Artificial Intelligence (AI) has become a game changer in many fields, especially in cyber forensics. This area, focused on the collection, preservation, and analysis of digital evidence for criminal investigations, has greatly advanced with the integration of AI. Technologies such as machine learning, natural language processing, and deep learning enhance forensic experts' capabilities by automating complex tasks, increasing precision, and accelerating the analysis of large data sets. AI tools can swiftly process massive volumes of data to identify patterns, anomalies, and connections that would be difficult and time-consuming for human investigators to find. For instance, AI algorithms can analyze network traffic to detect suspicious activities, evaluate images and videos to identify key evidence, and even recreate digital crime scenes. These innovations not only streamline investigative workflows but also enhance the accuracy of results, significantly improving the chances of effectively solving cybercrimes.

4.1 Potential Threats Posed by AI to Organizations

AI presents significant threats to organizations by enhancing the capabilities of cyberattacks, automating the process of identifying vulnerabilities and launching sophisticated attacks with minimal human intervention. AI-driven security systems, while improving surveillance, create vulnerabilities that cybercriminals can exploit to access sensitive data, leading to privacy breaches and reputational damage. Furthermore, hackers can use AI to autonomously manipulate or destroy information systems, resulting in catastrophic data loss and service disruptions. The technology's ability to convincingly mimic human characteristics raises additional risks of impersonation and fraud, complicating the detection of legitimate communications. To counter these threats, organizations must implement proactive cybersecurity measures and robust security frameworks, ensuring vigilance against the evolving tactics of AI-enabled cybercriminals.

5. Cyber Crime and Cyber Security

Loss of information through online services is called a "footprint of cybercrime".[ii]

The footprints of cybercrimes is such that it poses a threat to human life, particularly affecting children and adults. There is the evolution of digital crimes like cyber bullying, stalking, identity theft etc and which present a security hazard to the human lives. It is not unknown to anyone that use of use of cyber work can be seen extensively among teenagers and which may create problems for many.

Cybercrime is one of the fastest-growing areas[iii]

5.1 ICT tools (Information Communication Tools) are one of the many ways in which cyber crimes are done. Modern gadgets like laptops, mobiles phones, computers are used to work, mimic robots. In modern times the internet is used extensively and has become an integral part of human life. This comes with its

own downsides like social hacking which can damage and cause turmoil in a person's life. And while these devices do lessen the pressure on the human minds, yet they come with the price of drawbacks of cybercrimes and insecurity.

In today's world Cybercrime is the singular reason of both prosperity and poverty. If users unknowingly and innocently give their user id, passwords etc., then the hackers can use these with the consequence of the user losing all their money. Today women and children are using chat rooms more than before as they have become comfortable with them. There is an increase in cybercrimes in India through social media and the rise has been found from 155 in 2016 to 328 in 2016. Positive and constructive safeguards are wanted by people to make both their lives and data safe.

Privacy and security is covered by Data security measures and in todays world it is the Digital forms which maintain data. The fight against cybercrimes needs an enlargement of security[iv]

6. India Internationally

The state of affairs of Cyber Threat in BRICS

The leading positions in global economy in the consumer marketers has been taken over unofficially by BRICS, Brazil, Russia, India, China and South Africa and countries around the world and those belonging to BRICS use the social media extensively.When India hosted the 13th BRICS Summit on 9 September 2021, it highlighted cybersecurity as one of the important concerns in the Summit's concluding New Delhi Declaration (BRICS, 2021). A number of legislative and regulatory initiatives have been adopted by the BRICS governments which relate to cyber security and may have bearing at the international level[v]

Importantly, the five countries' national approaches present several points of overlap and tend towards convergence, but at the same time we can identify significant points of divergence. India has the largest chunk of global poor because of cybercrime. The intense interest with which internet is being used coupled with the data revolution, does not come alone but brings along with it the menace of cybercrime. And these types of cybercrimes are not restricted to a single area but the entire world is facing its consequences and increasing in a linear manner.

7. The Path Forward

Thus whenever crimes are organized through the web they are known as cybercrimes and the method by which it is prevented or protected is known as cyber security. This action of protecting any information or data from hackers is called cyber security. Just as and when any problem is faced or seen, a solution is also worked in its direction and looking for solutions for cybercrimes is no exception. The efforts to have and improvise the many technological solutions to deal with cyber security is expanding and refining with each passing day.

7.1 Effective ways to protect data

- Since there is acceptance that cyber terrorism is spreading its tentacles, there is also the initiative to curb its menace.
- Stringent measures should be taken by the government regarding all these crimes.
- Provisions should be made to make an upsurge in the punishments for cyber-crime.
- The need of increase in manpower for the administration and management of the increase in cybercrimes.
- Online arrangements are currently secured through private activities, laws, enforcement and other forms of international cooperation[vi]

International and National procedures

Domestic governments make their own laws to penalize cyber criminals.

Social Media Applications: At the same time of creating social networking sites, simultaneously the aspect of cyber security and saving data from threats is also created anticipating a cyberattack.

"Communication Security" means COMSEC and is utilized to secure and protect data from telephonic communication. The transfer after information is written, decoding of data on the site of the sender so as to make it unreachable or unreadable to the receiver until the data is inscribed on the receivers side.

7.2 AI-New Threats and New Potential

Modern situations have bought the relationship between artificial intelligence and cyber crime more into attention and notice in our lives. The 2023 AI based phishing attack and hacking of Facebook's user data in 2018 has made people even more apprehensive to this nexus. It is undeniable that in our ordinary discussions, our chats and in our everyday routine artificial intelligence has forayed deeply.

It has therefore become even more important that an organizations capability to supervise the working and proper management of its AI systems should be of the highest quality and satisfactory for the general public to trust it completely and fully. This is especially in the light of protection of consumer data against advanced criminal activity.

The usage and role of AI in modern time's businesses and organizations are undisputable although the opinions on use of AI in business is divisive. Since along with the benefits, there are problems that accompany the use of AI. This means criminals, cyber criminals would have different ways to hack into a company's AI systems by creating their own AI systems and upset an organization or hack the system with malice intentions. Therefore the need of the hour is to capitalize in newer updated technologies of AI even while protecting one's organization and enterprise from newer digital threats.

Thus to counteract the intimidations and threats presented by misuse of AI, an AI-based cyber security solutions is indispensable and critic

The paradox is while there is a threat of cybercrime in AI, there are advantages also of AI in cyber security and AI itself can be used to manage the threat of cyber security. For example when AI is trained to identify malware and viruses its ability to do so becomes faster than humans over a period of time through automated threat. On average, AI implementations have been found to reduce the average cost of an organization's data breach scenario by $230,000[vii]

The proficiency of a data system is increased by using AI which has the ability to spot any potential threats. By this recognition of a possible threat the incoming cyber attacks are squashed at a speed beyond which the human mind can comprehend. Yet because of the benefits associated with the integration of AI into different operational systems various business owners

7.3 Need for Cyber Security Measures

By remaining focused on the benefits of AI and its integration into various operational systems, many business owners are oblivious of the vulnerabilities that external AI systems may create not only to their businesses but to their own AI systems.

Technology has progressed immensely, so much so that with the aid of artificial intelligence, ransomware processes and automated phishing can be completed. In modern times lower-level cyberattacks have become possible due to the advancement in AI systems.

Today there is a likelihood to carry out a cyber attack which is well coordinated without the presence of a vocal, active human cyber criminal. This has become possible because human thought patterns are being mimicked with new AI knowledge. This means that cyber criminals have more time now to conduct a cy-

ber attack with minimal or no human participation.

Since it is now possible to have innumerable password combinations with the help of AI the threat of illegal access to systems is more probable. Apart from the unauthorized access, with assistance of adaptive learning algorithms, these systems can continually improve their efforts to hack into systems. It is unfortunate that establishments have little or no time to look for corrective measures of these weaknesses which AI recognize' s and attacks in a short time.

In order to protect themselves against cyber crime by way of AI, organisations must incorporate cyber security technology which is supported by AI and responds with the same speed. This means that establishments require to continually and regularly keep themselves updated with the latest developments in AI and thereby being ahead of the methods of cyber criminals.

Facial and object recognition technologies help cyber criminals to hack systems. There would be no protection for both data stored in the security footage and physical security footage if a hacker gets access to the AI-based surveillance footage.

Thieves used voice-mimicking software to imitate a company executive's speech and dupe his subordinate into sending hundreds of thousands of dollars to a secret account, the company's insurer said, in a remarkable case that some researchers are calling one of the world's first publicly reported artificial-intelligence heists[viii]

So while the utility of AI is obvious and visible there is very less knowledge as to how establishments can safeguard their interests from cyber threats. Because of the ability of AI to generate and create a human appearance in a persuasive manner, the likelihood of detection of crimes by way of AI will become even more difficult[ix]

Since advanced AI technologies have learned to duplicate so accurately both human behaviour and language, even lower-level cyber attacks would be difficult to identify.

7.4 Technology in Law Enforcement

The new emergence of technologies has brought a sea change in the methods of law enforcement and investigation methods. It is therefore necessary that law enforcement technologies keep in touch with modern technology thus empowering organisations to fight crime more effectively and speedily.

In India there is an enormous workload on the police department as the police strength is much lower than recommended by the UN. While the UN mentions that for every lakh people there should be 222 police officers, India has only 150 police officers for a lakh people[x] This means that the workload on the working average police officer is enormous and undoubtedly it affects his performance and efficiency.

By utilising technology, the effectiveness and efficiency of Law Enforcement Agencies (LEAs) can be improved thereby serve the public better and fight crime more effectively.

7.5 Law enforcement, investigation and role of technology

While progress in technology, the commission of crime has altered over time and has become more sophisticated, making it tough to solve, technology will also play a substantial role in helping law enforcement agencies to resolve the issues.

Technology for law enforcement agencies can be seen in the different ways like Detection and Prevention of crime, CDR Analysis, Thermal Imaging, Surveillance and Monitoring wherein India has many legislative measures to undertake surveillance. The Indian Telegraph Act of 1885, which talks about call interception, and data interception is covered under the Information Technology (IT) Act of 2000.

Conclusion

The Indian legal system has established procedures for electronic surveillance; however, these measures frequently fall short in their effectiveness. In an effort to address this issue, the Ministry has proposed amendments to the Central Motor Vehicle Rules of 1989 through a draft notification titled "Electronic Monitoring and Enforcement of Road Safety." This amendment suggests the use of body-worn cameras by law enforcement officers to document events and serve as evidence in court against individuals who violate traffic safety regulations. The intention is to ensure that offenders are held accountable in accordance with legal provisions. Technology plays a crucial role in bridging the gap between the public and law enforcement. The five key pillars of the criminal justice system—police, courts, prosecution, correctional facilities, and forensic science—can greatly benefit from technological advancements. By providing cohesive data and enhancing investigative processes, technology can support police efforts in solving crimes more efficiently. A strong and collaborative partnership between law enforcement and technology can facilitate quicker criminal investigations, reduce the incidence of crime, and contribute to the maintenance of law and order.

1. https://www.waketech.edu/programs-courses/credit/criminal-justice-technology
2. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
3. file:///C:/Users/hemal/OneDrive/Desktop/Tech&crmn%20jus/An_Overview_on_Cyber_Crime_and_Cyber_Security.pdf
   An Overview on Cyber Crime and Cyber Security Asian Journal of Engineering and Applied Technology
4. file:///C:/Users/hemal/OneDrive/Desktop/Tech&crmn%20jus/An_Overview_on_Cyber_Crime_and_Cyber_Security.pdf
   An Overview on Cyber Crime and Cyber Security Asian Journal of Engineering and Applied Technology
5. https://www.scielo.org.za/scielo.php?script=sci_serial&pid=2077-7213&lng=en&nrm=iso
   The African Journal of Information and Communication (AJIC)
6. file:///C:/Users/hemal/OneDrive/Desktop/Tech&crmn%20jus/An_Overview_on_Cyber_Crime_and_Cyber_Security%20(1).pdf
   An Overview on Cyber Crime and Cyber Security Asian Journal of Engineering and Applied Technology
7. https://securityintelligence.com/articles/why-2020-will-be-the-year-artificial-intelligence-stops-being-optional-for-security/
   Why 2020 Will Be the Year Artificial Intelligence Stops Being Optional for Security
8. https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/
   An artificial-intelligence first: Voice-mimicking software reportedly used in a major theft
9. https://link.springer.com/article/10.1007/s11948-018-00081-0 Artificial intelligence Crime: An interdisciplinary analysis of foreseeable threats and solutions volume 26
   file:///C:/Users/hemal/OneDrive/Desktop/Tech&crmn%20jus/clearias.com-Technology%20in%20Law%20Enforcement%20How%20can%20it%20be%20used.pdf
   Technology in Law Enforcement: How can it be used?