INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 2 [2025] | Page 218 - 224

CRITICAL ANALYSIS OF ARTIFICIAL INTELLIGENCE: A WEAPON TO COMMIT AND AVERT CYBER CRIME

-Ishaan Choudhary[1]

ABSTRACT

The emergence of Artificial Intelligence in recent times has commenced a debate all around the world about its role in averting the cybercrime or becoming itself a menace for cybercrime. Artificial Intelligence (AI) is an advance technology that has a human intelligence, due to which it performs a variety of functions like ability to see, understand and translate spoken and written language, analyze data, making recommendations etc. Day by day AI is crossing all its boundaries and entering into all the fields like in business, education, law, marketing, finance and even in health care. That time is not so far when this AI will become an essential part in the human life. With the arrival of AI people have started relating it with the cybercrime. Cybercrime is a criminal activity in which the wrongdoer targets or uses the computer with malafide intention in order to satisfy his/her goal. Most of the cybercrimes is committed by cybercriminals or hackers who want to make money out of it. If AI can be held responsible for the increasing rate in the cyber-attack cases then with the help of it, security system can also be detected and respond to threats at current time, it can even analyze vast datasets in order to identify inconsistency and predict the future attacks. Thus this paper will explore different dimensions of AI which includes its pros and cons. This study will also examine existing legal framework to deal with cyber criminals in India and whether India's current legal system is adequate enough to combat cybercrime in the context of AI technology. Many cybersecurity experts predicted a year ago that artificial intelligence will be an important player for cyber-attacks in 2023 as well as it will also contribute in improvement in the defense against future attacks. This paper critically analyzes the role of Artificial Intelligence and its relation with cybercrime.

Keywords: Artificial Intelligence, Cybercrime, Cyber-attacks, Technology, Hacking

[1] Amity Law School, Amity University, Noida

INTRODUCTION

The advent of Artificial Intelligence has created a sensation around the globe regarding its functioning as well as how the human beings will deal with this advanced technology.[2] AI is a comprehensive range of computer science that can conduct any tasks with the help of human intellect which is installed in it. The technology which is installed in AI can understand, learn, write etc. on its own on the basis of information that is required and which is also derived from different sources and databases. The only trait that makes AI looks different from the computer i.e. in computer, in order to perform any task, the humans have to give instructions (program) to the machine but this is not in the case of AI, here the AI technology itself analyzes data, patterns and make decisions out of it. Thus it adapts itself over the time.

In this revolutionary era of digitalization and advance technology, the sectors like education, finance, healthcare, business etc. are being easily influenced by Artificial Intelligence. It is slowly replacing the human labour from various fields. On one side the innovations in AI has created several benefits for the humans who are working in multiple industries, right from automation to solving critical problems, AI has performed all those functions which are quite troublesome for human beings. But on the other hand the same AI is becoming a menace for the cybercrimes.

Cybercrime is an illegal criminal activity which is carried out by internet or computers.[3] Cyber offences like hacking, phishing, cyber theft, spying etc. are some of the offences which get accumulated under cybercrime. In this tech – savvy world where the cybercrimes are of great concern, the influence of AI has made the matter worst constituting technologies like deep fakes, AI algorithms, chatgpt etc. In India's perspective, cybercrime has always evolved over the period of time. Information Technology Act 2000 was introduced in order to provide legal recognition for transactions which is carried out by electronic means. But the hackers also started attacking on e – commerce platforms, thus this IT act failed in dealing with evolving cases of cybercrime like cryptocurrency. In the later year government introduced Implementation of Digital Personal Data Protection Act 2023, with the help of which they conducted several awareness programs for the public. In the recent times AI has played a major role in averting cybercrime, some of the tools they adopted are anomaly detection, through which the police can analyze vast amount of data in

[2] Sentient Digital, Inc, *Artificial and Cyber Crime: Facing New Threats and Embracing New Potential,* SDI (Jan.22, 2025) https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/?amp=1.
[3] Richard De La Torre, *How AI Is Shaping the Future of Cybercrime,* DarkReading (Dec.21, 2023) https://www.darkreading.com/vulnerabilities-threats/how-ai-shaping-future-cybercrime.

order to identify the upcoming cyberattacks, then there is phishing detention which analyzes emails and websites of the cybercriminals. There is also The Indian Cyber Coordination Centre which plays a major role in combating cybercrime, they usually collaborate with stakeholders like industry, international partners in order to enhance their power and to prevent cybercrimes. This study aims in determining the role of AI in alleviating the rates of cybercrimes and simultaneously it can also become the tool for deterring cyber threats.

RESEARCH METHODOLOGY

This study adopts the empirical research methodology which focusses on collecting and analyzing of data in order to get information regarding Artificial Intelligence and its relation with cybercrime. The spectrum of other sources like articles, documents has accessed through the official website of AI and cybercrime.

REVIEW OF LITERATURE

Shubhangi Srivastava's article on AI in Cybersecurity – Uses, Threats & Prevention critically analyze what role does AI play in cybersecurity and why AI in cybersecurity is important? This article also highlights the uses of artificial intelligence in preventing cybercrime. Further the article mentions some of the applications of AI in cybersecurity as well as the potential of the AI, which makes it smarter tool in preventing cybercrime.

The article on Malwarebytes focuses on how AI is helping the cyber criminals to escalate cybercrimes. By manipulating data through AI, creating deep fakes, misusing of chatgpt are the evidences which highlights the dangerous side of AI. In other article written by Richard De La Torre, he also talks about different ways through which cybercriminals are leveraging AI. Automated phishing attack, fake customer support chatbots, social engineering attacks etc. are some of the examples mentioned by him.

ARTIFICIAL INTELLIGENCE: A WEAPON FOR CYBERCRIME.

Artificial Intelligence means the development of computer system in such a way that it can perform any task and make decision with human intelligence.[4] It creates algorithms that enable machines to learn from the data and recognize different patterns in order to adapt to the given situations.

[4] Ansari Zartab Jabeen, *Camouflage of AI in Cyber Crimes Vis-a Vis legal issues and Challenges*, WOU (Jan.22, 2025) https://woxsen.edu.in/woxsen-law-review/wlr-papers/camouflage-of-AI-in-cyber-crimes-vis-a-vis-legal-issues-and-challenges/.

AI has been in the limelight in the past few years, and with the advent of it there has been a division of thought process among the people regarding it.

On one side AI is considered as the upcoming technology that will enhance the present digitalized world and will build a strong relation between humans and advance AI technology like robots. But on the other side people think that the emergence of AI has led to the increase in cybercrime. Experts say that the cyber attackers use generative AI to find out various ways to undermine different complexities for advance attack. If we look AI as a weapon for cybercrime in respect to India, then we will get to know that in present times India has become a victim of AI.

In the last few years there were lots of news which were being covered regarding bomb threats in schools, airports and hospitals but after the investigation done by police and different security agencies it was found that it all were fake.[5]Also during the Lok Sabha election 2024, FIR was being lodged against the Aam Aadmi Party and various allegations were being put up by BJP party for creating AI generated photos and videos of Prime Minister Narendra Modi and Union Minister Amit Shah on the party's official handle. The other criticism which is done against AI is regarding physical safety, means if there is an AI based self-driving car which suffers a security breach, it would result in risking the lives of the passengers. One of the biggest example of misusing of AI and promoting cybercrime is spyware.

A spyware is defined as the software which enters into any user's computer, gathers all data from that device and then sends it to the third party without taking the consent of the user.[6] The cyber attackers use spyware in order to trick, steal and sell the user data like internet usage, bank details, credit card, etc. Due to all these cyber-attacks, the cybercrime cases are also rising. The Pegasus spy controversy is one of the notable cases under which India also got trapped into. Pegasus spyware was developed by Israeli cyber – intelligence firm NSO Group for monitoring mobile phones and gathering all the data from it, it used to track politicians, government leaders, human right activists and journalists.[7] The opposition parties in India also put allegations on the central government for using Pegasus spyware in order to target the opposition parties, journalists, social activists as well as Supreme Court judges. This controversy led to the debate regarding privacy and

[5] Anirban Chowdhury & Rashmi Rajput, *Hoax bomb threats loom over aviation industry* ET Times Nov.16,2024, https://m.economictimes.com/industry/transportation/airlines-/-aviation/threat-is-in-the-air/amp_articleshow/115367342.cms.
[6] *What is Spyware,* FORTINET (Jan.21,2025), https://www.fortinet.com/resources/cyberglossary/spyware.
[7] RSI Security, *How To Detect Pegasus Spyware,* RSI Security (Apr.1,2024), https://blog.rsisecurity.com/how-to-detect-pegasus-spyware/.

freedom of speech and expression. The opposition also raised the question on preservation of democracy in India, but Indian government denied all these allegations.

AI becoming weapon for cybercrime can goes do this level that the wrongdoer with the help of AI tools can generate voice of any person. In India it has become quite common to generate AI voices of Bollywood artists and committing any cybercrime. In 2023 actor Anil Kapoor filed a case in the Delhi High Court, seeking protection of his own name, image, voice, persona and all those attributes of his personality against those who are misusing it over internet.[8] Thus the above examples show us that how India has become a hub of cybercrime due to this AI.

RELEVANCE OF ARTIFICIAL INTELLIGENCE IN COMBATING CYBERCRIME

Artificial Intelligence not only contributes to cybercrime but also plays a major role in combating cybercrime. With the help of AI, we can easily identify the unknown threats which can cause severe damage to any person, company, organization and country. AI can also handle large amount of data in order to detect, identify and to scan the threats. Since bots are growing in this digitalized era thus it has become a major threat for cybersecurity, to overcome with this problem AI helps in recognizing and blocking the bots by identifying their patterns and deploy honeypots to trap them.[9] If we look AI's role in combating cybercrime with India's perspective, then we will get to know that nowadays our Indian Police is also using AI to prevent cybercrime.

Some of the measures taken by them are, using AI algorithms which can analyze past crime data for predicting future crime. Recently the Nagpur Police launched AI powered technology called as SIMBA (System Integrated for Monitoring and Big – data Analysis) for enhancing the law enforcement in the entire city. SIMBA is an advance generative AI tool that provides various information from data like CCTV, images and audio of crime and criminals. The Surat Police has also launched "Cyber Mitra" which is an AI powered WhatsApp chatbox for averting the cybercrime. This chatbox provides 24/7 accessibility to the citizens, it spreads awareness among the people for protecting themselves from online fraud.[10] And if in the case of encountering the cyber fraud, the chatbox guides users through the complaint registration process, making quite

---

[8] Malwarebytes, *AI in Cyber Security: Risks of AI,* Malwarebytes (Jan.22,2025), https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security.

[9] Shubhangi Srivastava, *AI in Cybersecurity – Uses, Threats &Prevention,* engati (Nov.29,2024), https://www.engati.com/blog/ai-in-cybersecurity#:~:text=make%20sense%20of.-,How%20does%20AI%20in%20cybersecurity%20help%20prevent%20cyber%20threats%20%3F,malware%20code%20to%20evade%20detection

[10] *AI – Assisted Cyberattacks and Scams,* NYU (Jan.22,2025), https://www.nyu.edu/life/information-technology/safe-computing/protect-against-cybercrime/ai-assisted-cyberattacks-and-scams.html.

easy for the users to report the incidents. The U.P Police came up with another AI tool known as Crime GPT. The Crime GPT holds vast database of criminal records to analyze information and provide details to the police. This tool helps in identifying the patterns and connection between crime and criminal during the time of investigation.

In India AI is not only used by the Police or other agencies in order to avert cybercrime but also AI contributes to different sectors of industries. Like in education sector, the demand for AI has increased over the period of time. The AI technology helps in the development and setups of many learning programs. Different schools and colleges are organizing various seminars on AI which is ultimately attracting the youth towards it in order to know it as well to use it. And there can be chance in future that with the help of AI we can also reform our education system. In the business line also, AI is in great demand; by using AI tools the entrepreneurs can make smarter decisions.[11] According to CBIInsights 86% of health organizations will going to use AI in the upcoming years.

AI has also started significant contributions to healthcare in India, AI algorithms analyze patient's data which includes lifestyle, genetic information etc. in order to predict the developing disease. AI has also done discovery of drug which means identify potential drug candidates and predict their safety, this would also lead to faster development of new treatments for various diseases.

SUGGESTIONS AND CONCLUSION

Artificial Intelligence plays a major role in committing cybercrime as well as helps in averting the cybercrime also. In today's time where the whole world has become digitalized and day by day new science inventions are taking place. Thus the demand for AI whether in malafide or bonafide intention becomes quite common. Like if we see AI from India's perspective then we can notice that how AI is being used by the cyber attackers in order to commit cybercrime. With the help of AI tools, they create deep fakes, misuses any user's data, spread wrongful information regarding any person etc. But on the other side there are some sections in the Indian society who take help of AI in order to prevent cybercrime.

Various state police have developed their own AI generated tools in order to catch the cyber criminals and to combat cybercrime. AI not only used in stopping cybercrime but it also used in other sectors like education, healthcare, business etc. in order to introduce new innovation in these sectors so that their pace of development also increases. Thus we can say that Artificial Intelligence

[11] Avijeet Biswal, *Top 24 Artificial Intelligence Applications and Uses,* simplilearn (Jan.8,2025), https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/artificial-intelligence-applications.

presents both sides of coin in the context of crime. In order to reduce its misuse and to enhance its uses in India, the government should take some initiatives. Firstly, the government should add specific provisions which addresses AI under Bharatiya Nyaya Sanhita (BNS). Along with it for misusing of AI, government should add strict punishment under Bharatiya Nagarik Suraksha Sanhita (BNSS). By doing this the cases of cybercrime will definitely be going to get decline. Organizing of various workshops and seminars in schools and colleges will going to educate the students and make them aware about AI advantages as well as disadvantages.

We can also add AI in the curriculum of the students in order to educate them. Government should also come up with Data Protection Bill in order to protect the data from the cybercriminals. We can also educate our society regarding ethical use of AI. Thus the whole research paper highlights how AI can be good or bad for humans, also we can't only blame AI for committing cybercrime because the same AI provides us with lots of knowledge, protect the user from unwanted sites, but it all depends upon how we humans how with deal it. The malafide intention of humans will use AI for committing wrongful acts while the bonafide intention of humans will use AI for averting wrongful act.