

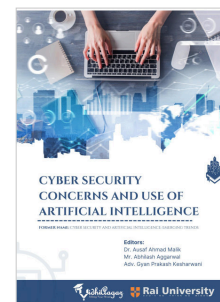
CHAPTER 6

A Dive into the World of AI in Moulding Cybercrimes

Smita Goswami

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 58–66

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Smita Goswami, *A Dive into the World of AI in Moulding Cybercrimes*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 58 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Smita Goswami, ‘A Dive into the World of AI in Moulding Cybercrimes’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 58.

CHICAGO (17TH ED.)

Goswami, Smita. “A Dive into the World of AI in Moulding Cybercrimes.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 58–66. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-6/>.

APA (7TH ED.)

Goswami, S. (2024). A dive into the world of AI in moulding cybercrimes. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 58–66). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-6/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-6/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

A DIVE INTO THE WORLD OF AI IN MOULDING CYBERCRIMES

Smita Goswami⁷

ABSTRACT

In the 21st century, internet and computers have become the part and parcel of everyone's lives. The rise of the digital era and our continuous dependence on internet have brought everything at our finger tips. In spite of the positive impacts, the advancement of information technology has opened new avenues for the tricksters. This is leading to a surge in cybercrimes across the world. Hence, it becomes necessary to protect the information shared online from being misused by any third-party and to penalize the cyber criminals in a just manner. Various laws have been enacted like the Information Technology Act, 2000 to combat the proliferation of such crimes and the existing penal law like the Bharatiya Nyaya Sanhita, 2023 has been amended to include 'cybercrimes' within the ambit of 'organised crimes' and includes punishments for the same. Cybercrime is very much different from the conventional crimes that we generally witness in our society. This paper throws light on the different cybercrimes committed by the miscreants along with the misuse of Artificial Intelligence (AI) for committing cyber offences and the way AI is fighting back, concluding with the future of cybersecurity in India.

Keywords: Cybercrime, cyber security, cyberattack, Artificial Intelligence (AI), data breach, robotics.

PRELUDE

With the evolution of human beings, men are always inclined towards making progress and bettering the existing technology. This sowed the seed for launching of the most commonly used innovation, that is, the Internet, without which we are technologically challenged these days. Starting from booking hotel rooms, online shopping, finding jobs to video conferencing among individuals staying at different corners of the world to ordering food online, internet has greatly influenced our day-to-day activities. We all know progress comes with a lot of shortcomings as well. The menace of cybercrimes is one of the dark sides of internet which instills a feeling of fear among the users.

CYBERCRIME AND ITS CLASSIFICATIONS

Though we are very much familiar with the term 'cybercrime', it is neither defined in the Information Technology Act, 2000 nor in any other legislations. Cybercrime refers to the criminal activity involving computer or computer networks. According to the dictionary meaning, it means a crime or an illegal activity that is done using the internet. Cybercrime is easy to commit (if one has the knowledge how to do it), hard to detect (if one knows how to erase one's tracks) and often hard to locate in jurisdictional terms, given the geographical indeterminacy of the net.

According to U.S. Department of Justice, cybercrime can be performed in the following ways: -

1. Crimes where the computing device is the target - for example, to gain network access.
2. Crimes where the computer is used as a weapon - for example, to launch a denial-of-service (DoS) attack.

⁷ Student at Department of Law, Calcutta University, Kolkata, India.

3. Crimes where the computer is used as a medium to a crime - for example, using a computer to store illegally obtained data.

Cybercriminals have a plenitude of avenues to dexterously commit crimes in the cyber space, of which a layman becomes an easy prey. Some of the common ways of cybercrimes are explained below in brief: -

- i. **Hacking-** It is an act to exploit the computer system, without any permission and gain unauthorised access to a particular data and make any changes for illicit purposes. It is a kind of trespass. Hackers have an advanced knowledge about the working of computer systems and use it for illegal usages such as to collect personal information, deface websites etc.
- ii. **Virus dissemination-** Viruses are computer programs which, just like biological microorganisms, show the trait of infecting a system or file and proliferate on other computers over a network as well. They invade the data stored either by completely modifying or deleting it. Commonly termed as Malware (MALicious softWARE), they replicate in the system until the available memory gets filled up. Trojans, worms and spyware are some of the common malwares which can steal personal data by tricking the users.
- iii. **Denial of Service (DoS) attacks-** It is a precise attempt by the attackers to prohibit users from accessing a particular service. It includes flooding of computer servers with surplus number of requests or links, greater than the server's capacity resulting in significant slowing down or crashing of the server.
- iv. **Phishing-** It refers to extraction of restricted information of the user like username, password details, credit card numbers by impersonating as a legitimate identity or enterprise. Phishing involves sending fake emails or messages containing links of virus infected websites which makes the user fill up his personal details under false pretences.
- v. **Carding-** Carding means using false ATM cards by the fraudsters to withdraw money from the victim's bank account and fulfil their pecuniary benefits.
- vi. **Cyber stalking-** We are very much familiar with the term stalking which refers to an act of following a person physically. Similarly, cyber stalking refers to pursuing or following a person online. The stalker infringes one's privacy and keeps an eye on the online activities of the victim. The internet provides them an open platform to harass, threaten and be vigilant over the victim's actions.
- vii. **Data diddling-** Data diddling is an unauthorized modification of data during entry into a computer system done with a malicious intention, and then changing it back after processing is done. Using this technique, the attacker may alter the expected output and is difficult to track. For example, an employee modifies his own salary details in the company payroll system to get higher pay check.
- viii. **Intellectual property crimes-** Intellectual property refers to intangible creations of human beings such as inventions, literary, artistic, cinematography and other works. Intellectual property rights

encompass trademarks, patents, copyright, industrial design rights, geographical indications etc. Any illicit act by which the owner is deprived of his rights completely or partially is said to be an offence.

- ix. **Email spoofing-** A spoofed email is said to be the one which is sent from a different location by camouflaging its original location. The location is normally traced from the email address and the phone number of the victim and the email is sent through internet.
- x. **Identity theft and credit card fraud-** Identity theft means stealing of identity and pretending to be someone else to access credit cards, bank accounts and other benefits. Credit card fraud is a common form of identity theft where the criminal gets hold of the credit card and has access to his transactions.
- xi. **Cyber trafficking-** Cyber trafficking is a term that defines human trafficking for sexual exploitation, drug abuse where the exploitation is recorded through electronic means. Internet bestows the online platform to target, control and exploit victims.
- xii. **Cyberextortion-** Cyberextortion refers to a crime where there is an attack or a threat of attack with a demand of a lumpsum amount of money to prevent the attack. In a ransomware attack, the attacker gains an access to a system's documents and files in unauthorised manner and makes the data inaccessible by the victim unless the money is paid. Usually, the payment is made in form of cryptocurrency like bitcoin.

CONCEPT OF ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence is a branch of computer science which recreates the intelligence of human beings in a computer to perform the tasks with less human intervention. The groundbreaking innovation of AI represents a paradigm shift in the realm of cybersecurity, offering multitude of opportunities to strengthen defenses and combat cyber threats in the digital age. The term 'Artificial Intelligence' was first coined in a summer research project organised by John McCarthy at Dartmouth, 1956 where he explored various ways by which a machine makes use of intelligence to carry out specific tasks. In 1997, Deep Blue became the first AI-powered computer program to defeat the world class chess champion Garry Kasparov. AI is also known as Machine Intelligence. The core principle of AI is to associate programs and computers capable of performing tasks that require intellect like problem solving, perception, decision making, human communication.

Types of Artificial Intelligence-

AI is categorised into four types which are as follows: -

- **Reactive Artificial Intelligence-** From the very name, we can easily figure out that these AI machines can react to situations, analyse the process and takes the best decision. The best example is the IBM Chess program, Deep Blue which defeated Garry Kasparov.
- **Limited Memory Artificial Intelligence-** These systems are capable of storing memory temporarily for decision making purposes. Suppose in a self-driving car, it uses past experiences as reference to use in future but cannot be used permanently.

- Theory of Mind Artificial Intelligence- This type of AI systems has not been invented yet, but it is not far from being introduced in this digital age. Such system is believed to communicate its intents and decisions in human languages, making interaction between the user and the computer a cake walk.
- Self-Awareness Artificial Intelligence- Such system is also not available in cyber sector yet. This kind of system is believed to have sense of awareness and emotions. This type of technological invention will make the computer systems at par with human beings.

INTERSECTION OF ROBOTICS AND AI

The sphere of AI and robotics have been smoothly advancing in the recent years, skyrocketing the pace of technological development. So far, we have read about robots and its functions only in stories or cinematographic films, but now, it has become a reality. Counting from self-driving cars to virtual assistants like Siri and Alexa, AI is making our lives easier, faster and more convenient.

A robot is a machine designed and programmed to perform tasks autonomously or with minimal human intervention. These tasks can range from simple actions like cleaning to more complex tasks like performing surgery. Artificial intelligence, on the other hand, is the ability of a computer or robot to think and learn like a human. This includes learning from past experiences, recognizing patterns, and making decisions based on data rather than being programmed to do a specific task. Robots and AI work together when the robots are equipped with sensors and cameras to receive information from the surrounding which is then sent to the AI systems fixed in them. They carry out complex algorithms to interpret the information and produce the desired result.

The AI-robotics duo has excelled in quite a few areas like the healthcare sector, space exploration, defense etc. With the sheer advancement in technology, it is feared that these may replace human workers leading to robots becoming the masters and we, their slaves. It is necessary to deal AI cautiously keeping in mind all the probable pros and cons.

IMPORTANCE OF AI IN CYBER SECURITY

Living in the 21st century, we are witnessing the proliferation of digital development which have transformed or rather, is revolutionising the ways of interaction among individuals and other entities. On one hand the whole world is getting modernised which in turn, is catalysing the attackers to plot loopholes in cyberspace resulting in cyber security breaches. This is where AI plays a pivotal role in dealing with treacherous challenges posed by cyber threats. It uses machine learning, neural networks, and other various techniques to detect, prevent, and respond to cyber-attacks immediately, efficiently and effectively. The primary function of AI in cybersecurity is to foresee potential vulnerabilities and future attacks through predictive analytics, while automated threat hunting reduces the workload on cybersecurity professionals by identifying threats within a network. AI lends its hands in incident response by swiftly analysing attacks, suggesting remediation steps, and automating responses to mitigate damage.

AI and machine learning are the absolute need of the hour for preventing cybersecurity threats. They can analyse large amounts of data and detect risks like phishing and malware. However, cyber criminals are experts in modifying malware code to evade detection. Machine Learning or ML is ideal for anti-malware protection since it can perceive data from previously detected malware to detect new variants. This works even when dangerous code is latent within a basic code. AI-powered network monitoring tools can track the behaviour of the user, locate anomalies, and react accordingly. These technologies can alleviate threats in real-time without interfering with business processes and can track data that gets overlooked by human sight, such as videos, chats, emails, and other communications. AI-enhanced cybersecurity systems leverage machine learning algorithms to learn behavioural patterns of users, assets and networks and permit them to detect anomalies and probable risks in real-time. By setting up norms and recognizing deviations from normal behaviour, AI elevates the ability to proactively identify and alleviate cyber threats, ultimately strengthening the security posture of organizations.

There are a few reasons why AI is extremely important in cybersecurity. Some are discussed below: -

1. Intensified Threat Detection- AI systems can analyse large amount of data and identify even minute anomalies and potential threats that might be missed by traditional methods. This detection helps in preparing and preventing future attacks.
2. Capability to handle Complexity- AI is capable of tackling complex data. It provides a bigger picture of the data sources and threat landscape and enables efficient defence strategies.
3. Improved Response Time- AI is too efficient to take longer periods of time to respond. The time duration between detection and preclusion of malware is sufficiently reduced and hence, the damage by cyberattacks can be prevented swiftly.
4. Adaptive Learning- AI systems can learn from new data and past experiences, improving their ability to locate and respond to threats over time. This adaptive capability ensures that efficient mitigation of damages.
5. Proactive Defence- AI has the feature of predicting future threats allowing the organisation or entities to take precautions even before they occur. As a result, the security measures get scaled up.
6. Secures Authentication- AI provides a layer of security by using tools like facial recognition, CAPTCHA, strong passwords and fingerprint scanners to secure authentication during login attempts. This helps to detect fraudulent login attempts by the tricksters and prevents a potential security breach on our network.
7. Battle Bots- Bots are a part of artificial intelligence and a growing threat in cybersecurity, used for nefarious activities like spreading malware and stealing data. AI can recognize and block bots by detecting their patterns, creating more secure captchas, and deploying honeypots to trap them.

LEVERAGING OF AI BY CYBER CRIMINALS

Artificial intelligence has been a leading player on the cybercrime landscape, escalating attacks while also contributing to improvements in the defence against future offences. Now experts across the industry expect AI to exert even more influence in cybersecurity. There is a close association between increased AI usage and snowballing of cybercrime incidents in recent times. Some of the common ways of using AI by cyber criminals include: -

- Multiplying existing attacks making it difficult for antivirus software to detect threats.
- Creating new attacks by making fake data to create confusion or impersonate officials.
- Automating and increasing attacks within less time and putting negligible efforts.

AI-POWERED CYBER ATTACKS

AI has been discovered to improve the lifestyle of people across the world but the digital attackers are leaving no stones unturned to use AI for malicious purposes. Cybercriminals are using AI- generated tools like ChatGPT and other chatbots to carry out social engineering attacks that arouse chaos. Several AI-powered cyberattacks are discussed below: -

1. **Deepfake attacks-** Deepfake is a blending of two words ‘deep learning’ and ‘fake media’. Here, the miscreants use AI techniques to impersonate someone and create audio/visual media depicting any particular person in such a flawless manner that it seems authentic. It is hardly distinguishable from the original person’s facial expressions. These types of attacks are used to collect information or trick people into performing harmful actions.
2. **Phishing attacks-** Cybercriminals are experts in using AI to create more sophisticated and difficult ways to determine phishing attacks. For example, AI can be leveraged to generate convincing deceitful emails or websites that look legitimate apparently. AI can clone any website in no time and customize it, based on the original one and give the impression of real access to an internal resource. These emails or websites seem to be so authentic that many innocent people fall into the traps of such tricks.
3. **AI- driven Password Cracking-** We all are very much familiar with the fact that hackers can proficiently gain unauthorised access into one’s personal information like passwords, credit card credentials etc. The usage of AI has cleared their path in committing such crimes in a flawless manner than before, yielding a higher success rate and also withing lesser time. They use password-cracking algorithms to analyze large password datasets and generate different password variations.
4. **AI-powered ransomware-** Ransomware has evolved throughout this 21st century. The pandemic has kindled the attacks of ransomware much more. By using artificial intelligence and machine learning capabilities, cybercriminals can develop increasingly damaging ransomware that can evade detection and spread more effectively. The cyber crooks blackmail organisations to pay a lumpsum amount of money otherwise they would delete or leak confidential data to the public.

5. **Payment Gateway Fraud-** AI has gone to wrong hands in creating various paths of payment gateway fraud which can be hardly detected and eliminated. Fraudsters may induce techniques like generating realistic identities, analyzing patterns to dodge detection systems or conducting targeted phishing attacks using AI-generated content.
6. **Business Email Compromise (BEC)-** This is similar to a phishing attack where the tricksters impersonate any business organisation and send convincing emails to the respective employees abetting them to perform unauthorized actions like initiating fraudulent transactions or disclosing sensitive information.
7. **Fake customer support chatbots-** Though these fake chatbots make take time to gain popularity, it can be another technique to fool people by AI's grace. The victims may not have an idea that while resolving their doubts in a particular site, be it regarding opening bank account or enrolling in a course, these fake chatbots may tactfully ask for their personal information and instigate them to perform unlawful activities without their knowledge leading to their monetary loss.
8. **Data breaches-** Almost all websites and applications collect user data, like ours, for storing data like our name, email address, address and interests. The most commonly used applications like the Instagram and Facebook store data based on the contents we like. Although these are secured to some extent, less secure websites and applications that store data about its users are very susceptible to data breaches. In this way, AI- assisted methods are scamming people across the world and infringing their right to privacy which makes it difficult to store or save anything online.

SECURITY MEASURES TAKEN BY CYBERSPACE

AI is not only being used by the cyber attackers to catalyse the invasion of data or intrusion into one's digital privacy but also to combat cyber threats. There are mainly three ways harnessed for cybersecurity: -

1. **Developing antagonistic AI-** This is basically 'good AI' combating 'bad AI'. Generative Adversarial Networks (GANs) are developed which create new patterns of the attack. Being familiar with such attacks, it can predict the possibilities of attacks in the future.
2. **Detection of abnormality-** Use of AI can detect any kind of anomaly in the server as well as the system. Any kind of potential threats can be located and prevented from capturing and destroying the whole system.
3. **Detection of response-** AI helps security teams to identify and address legitimate threats by receiving information and less amount of time is spent on chasing false positives and attempting to decipher security logs helps teams to launch more immediate and effective responses.

In India, several legislations have been passed to look into the matters of cyber related crimes which are as follows: -

- The Information and Technology Act, 2000- This Act encompasses different offences related to information technology, i.e., computers and other devices, and respective punishments for them.
- Digital Personal Data Protection Act, 2023- This Act was passed for the processing of digital personal data within and outside the territory of India. It mainly focusses towards regulating the accumulation, storage, processing, and transfer of personal data in the digital landscape.
- The Copyright Act, 1957- This Act deals with a collection of exclusive rights given to the authors/creators of different works which can be claimed by them only. AI can be misused at times to claim copyright but there are not any laws to sue AI for compensation or damages.

THE FUTURE OF CYBERSECURITY IN INDIA

As far as the future of cybersecurity is concerned, the following points are to be kept in mind:

1. Improvement in International cooperation- Cyber threats happen irrespective of state boundaries. It is important for the country to work together with other nations in order to strengthen cyber security standards.
2. Adoption of latest technologies- Since, AI is the latest discovery and almost everything revolves around it in today's time, India must invest towards using latest technologies in order to bolster cyber defences.
3. Training towards cyber security education- With the growth in technological advancement throughout the country, India needs to raise awareness regarding cyber laws and train employers with adequate knowledge of cybercrimes in order to fight against this menace.
4. Cooperation between public and private sectors- Both public and private sectors should work together to fight cyberattacks in the country. There must be equal sharing of threat intelligence and other innovative measures between government agencies and private entities.
5. Strengthening legislative mechanisms- There are several laws enacted to protect individual's personal data online and to prevent infringement of right to privacy. India needs to bring more stringent laws in data management and cyber security to safeguard sensitive information from the claws of cyber tricksters.

POSTLUDE

The intriguing invention of AI has become an indispensable part of our lives. Its potential for increasing efficiency and making groundbreaking applications in the future is immense. It is not an elixir rather a proportionate blend of risks and benefits. The advent of AI has been a boon as well as bane depending upon the hands of the person with whom the steering wheel of AI is. The amalgamation of AI and cybersecurity has given birth to an advanced digital era shielding from various threats. It is our responsibility to ensure that it is used for the betterment of the society rather than its misuse. In the budding sphere of technologies, it is highly probable that it will usher in legal implications. Though there are legal instruments to deal with different cybercrimes in the country, it is not enough to deal with upcoming crimes done with the aid of AI. There is a need for legal definition of artificial

intelligence Specific enactment of legislations with necessary safeguards tackling AI-assisted technological developments is the need of the hour. Moreover, it is the duty of the government to spread awareness and educate people regarding its negative impacts and the measures on how to immediately respond to such unprecedented threats.
