AI & CYBER FORUM
AN INTERNATIONAL JOURNAL
OPEN ACCESS
ISSN 3117-6399
Review Article
Check for updates

AI and Cyber Crime

Rashmi Shenoy[1], **Pallavi G.P.**[1,2], **and V. Basil Hans***[1]

[1]*Srinivas University, Mangalore, India*
[2]*Sri Siddhartha Institute of Management, Tumkuru, India*

Corresponding author: **V. Basil Hans** | E-mail: **vhans2011@gmail.com**

Citation: Rashmi Shenoy, Pallavi G.P., and V. Basil Hans (2026). AI and Cyber Crime. *AI & Cyber Forum: An International Journal.*
DOI: https://doi.org/10.51470/AI.2026.5.1.30

Received 10 January 2026 | Revised 13 February 2026 | Accepted 08 March 2026 | Available Online April 15, 2026

Abstract

Artificial Intelligence (AI) has changed the digital world, allowing for automation, predictive analysis, and intelligent decision-making across several industries. But the rapid evolution of AI technologies has also added new aspects to cybercrime. Cybercriminals are increasingly using AI to carry out complex assaults, such as phishing, malware development, identity theft, ransomware, deepfake manipulation and automated hacking. Meanwhile, AI is being used as a potent defensive tool for threat identification, intrusion prevention and cybersecurity monitoring. This paper addresses the dual role of AI in cybercrime, exploring its possible benefits and the hazards it poses. It examines how machine learning algorithms, natural language processing and generative AI are driving the evolution of cyber threats, but also of the strengthening of cyber defence measures. It also covers the legal, ethical and security problems posed by AI-enabled cyber operations and emphasises the necessity for international collaboration, effective legislation and responsible AI governance. The study suggests that the key to minimising the misuse of AI in the digital world is to strike a balance between innovation and cybersecurity readiness.

Keywords: *Artificial Intelligence (AI), Computer crime, Machine Learning, Cyber Security, Malware, Deep Fakes, Phishing attacks, Data Protection.*

1. Introduction

Artificial intelligence, or AI, is defined as robots that mimic the intellectual behaviour of humans, such as thinking, learning, reasoning and planning. A typical AI system is made up of models that have been trained on large amounts of data. The user offers a prompt, and the AI tool generates a continuous response based on its training.

The increasing use of AI algorithms has enhanced the danger of cybercrime to a considerable extent. Attackers are now using AI for malware development, spam, phishing scams, information theft, identity fraud and insider attacks. The emergence of automated systems means that perpetration can happen at a larger scale and at faster speed than previous harmful software. Artificial Intelligence-based malware and harmful programs are software capable of conducting cyber-attacks that mimic intelligent behaviour. The application of AI methods to create customised malware has been called AIE, or Attacks with Intelligent Envelopes. Bots are cyber crime automation technology that helps cybercriminals to carry out large-scale cyber-attacks in a short time [1]. AI also allows for new malware and exploits to be created to circumvent security, automation of social engineering and phishing malware and an up-tick in identity fraud.

AI can also act as a cybersecurity digital assistant to protect organisations from cyber-attacks. Many organisations that are more likely to be targeted by cyberattacks are investing in AI technology.

AI can help to accurately detect new and fatal viruses that can massively infect connected devices in little time. At now, companies are exploring AI methods for cyber security systematically [2].

AI security systems use machine learning and AI in many cybersecurity operations such as anomaly detection, fraud protection, digital forensic analytics, threat intelligence, and security incident response. Every day a huge amount of spam emails are sent out by cybercriminals and no system can provide 100% protection against spam. The statistical and text-matching approaches used against spam email have become ineffective due to the changing nature of attacks and defences used. The combination of deep learning and statistical approaches is challenged by all four tasks, spam detection, spam filter evasion, malware detection and malicious code development. The increasing development of AI, specifically letting the computers learn and anticipate profoundly from the data becomes a necessity.

Cybercrime can be defined as “any illegal activity that uses a computer as its primary means of commission” and the illegal acts must be penalised by the current criminal laws. Cybercrime is also defined as, “any activity or act performed using a computer, computer system and computer network, which harms the individual or society, such as Data Theft, Identity Theft, Fraud, Harassment, Phishing, Cyber pornography, spreading wrong information, etc.” Cybercrime can be depicted as a crime done with using computer in any of the means of traditional

crime, like Hacking, Password theft, Money Laundering, Online Gambling, Cyber terrorism, etc. Cyber-crime has also been referred to as: "Criminal activities performed by means of computers or the internet" in international treaties and many study papers.

2. What is AI?

Artificial Intelligence (AI) is a collection of techniques that use data, computing and automation to improve decision-making and problem-solving abilities [1]. Three basic principles that make up AI: data, models and automation. Data is any information that can be collected or kept that is measurable. Data can include text, audio, video, and logs. Models are mathematical representations of real-world things, events, or processes that allow us to make reasoned inferences from a certain set of observable inputs. Automation allows a computer to do things for itself that were once done by a human operator. AI systems learn and get better at models from data, then use those models to automate choices, perhaps at a scale or speed beyond human ability.

The phrase "Artificial Intelligence" was coined in 1955 and is about machines that can replicate intelligent human behaviour, like learning, thinking and planning [3]. The AI area is full with approaches and models, configured in many different ways to solve many different issues. Specific methods may be used. Often , these are used for the purpose of enhancing model performance via data analysis. Machine Learning is a subset of methodologies . AI approaches have been effectively implemented in many areas as automated communication, personal assistance, speech recognition, translation, search, medical, fraud detection, credit scoring and machine vision. AI models often form the basis for human-transparent automated decision-making, where humans interact with the computer by means of simple requests.

3. How AI is helping crime

Cybercriminals can employ artificial intelligence in a variety of ways to assist them in their unlawful actions. Other AI platforms like ChatGPT can impersonate trusted people and provide other functionality not easily available in traditional applications. Generative artificial intelligence fuels deception, making it easy to personalise mass communications to look like believable fake messaging. Cybercriminals scam people in all kinds of ways to make money . Invoice fraud , impersonation fraud , advance-fee fraud , and lottery fraud . The automated theft of identities of bank clients or social security numbers from public profiles, especially on the dark web, still requires a significant investment of human resources. Detection and traceability reduce by automation of services (e.g. auto-dialing, creation of false voices, transfer of funds without direct interaction) and scale and speed of operations rise. When paired with code creation, botnets and other infrastructure, this automation of malware creation within controlled settings helps customise attacks to particular targets.

Similarly, the development of dangerous code that extends existing code represents a new service to malware creators, increasing the pool of possible offenders. They can get pre-written scripts that can steal sensitive information, can be used on certain operating systems or devices, and can be quickly adapted to new weaknesses or situations.

The essence of cybercriminal actions is not changing, but the risk is becoming higher in case of involvement of AI. This improved capacity to impersonate can be leveraged to conduct social engineering assaults. The development of information speeds up the opening of new online services and accounts that can be used for further attacks like fraud. Automation services magnify the impact of crimes such as ransomware theft, selling unlawful data or spreading undesirable information. These tactics are available to anyone who does not have any specific ability or understanding.

The combination of impersonation and the flexibility to customise a hostile social engineering attack is a huge enabler for growing such operations. Trusted platforms can host deceptive services outside the attacker's control, enabling the use of attributes such as existing followers and established trust that would be much harder to use on untrusted venues. At the generation stage it is at all conceivable to abstract away language. And even there language is fairly significant at other levels of detail in the process. Social engineering attacks no longer require a great deal of customising of each individual message in a detectable way. Such approaches produce findings that look convincing yet are false.

4. How AI is combating crime

Artificial intelligence (AI) is the capability of a computer or a computer-controlled robot to do things that are normally done by intelligent beings. It is based on the imitation of cognitive functions such as learning and thinking. AI is usually divided into strong and weak AI. Strong AI, often known as artificial general intelligence (AGI), is a system that can make judgements independently. Weak AI , or narrow AI , is AI that is programmed and trained to do a specific task . AI requires data input, often in massive quantities, to develop models that include statistical inference and permit the automation of future tasks. It works through the pairing of algorithms that tell it specific actions based on the input and data model and models. Models are algorithms of sorts that have been altered through training data. Although it is widely believed that AI removes the need for human involvement, in reality human oversight continues to be an important part of both training, and deployment, e.g., through monitoring, auditing, and quality assurance [4]. Artificial intelligence technology are capable of analysing vast amounts of data or monitoring Internet activity in real-time to detect aberrant events suggestive of crimes such as fraud, phishing, hacking, viruses and spreaders, information theft, and money laundering.

5. Practical illustrations

Artificial intelligence is ubiquitous in numerous industries and involved in a range of enterprises, on the frontiers of research and engineering, or drug

discovery and development. Up until now, amazing breakthroughs in knowledge and technology have been achieved. But the dark side of the development has developed together with the upswing. Parallel development A mission-oriented development. AI has been utilised to power a range of cybercrimes. There are very few technical developments that are totally benefiting the society and lack of balance has proven quite detrimental. Cybercrime has been the topic of discussion for decades but not comprehensive discussions have been put under the relevant idea of AI in Cybercrime, and not well-structured position and argument has been presented. Cybercrime is often referred to as Digital Crimes, Computer Crimes, Internet Crimes attacking information technology systems. Cyber Crimes are computer intrusion, misuse of intellectual property, economic espionage, online extortion, worldwide money laundering. Cyberthreats map is established by Cyber Administrate Bureau under National Police Agency of Taiwan. Cyber Crime occurrences trend is regularly tracked and built by many government or private companies. Dark and deep web's malicious and illegal activities are spidered and collected as per templates by web crawlers. Cyber Security Operation Center of Taiwan National Security Committee investigates and analyses the cyber incident event. There are different methods and techniques to get the optimum answer for protection [1].

6. Risks and challenges

The use of Artificial Intelligence (AI) presents a variety of hazards to the security of individuals, organisations and infrastructure. Those dangers include bias, privacy, abuse, errors, over-reliance and governance weaknesses. They must be countered by transparency, controls, audits and accountability. A multitude of AI applications is available every day to help with business and assure safety, but those very same systems can just as easily be abused by persons with bad intent [2].

The need to put in place a legal framework to set what is permissible usage and the responsibilities of the AI systems adopted is widely recognised. As AI keeps expanding its role in augmenting and automating increasingly bigger portions of business processes, it is essential to keep transparent systems with interpretable decision frames in place and with sufficient human supervision. AI in the form of automated decision support systems can be in the form of chatbots and robotic process automation (RPA) and is a great example of useful implementations. However, it is important to pay equal attention to the decisions made by the system, the input data, potential derivations and potential errors that may occur during operation [5].

7. Safe use and prevention

"Safety is a function of safe use and adequate preparation against threats." Best practices for responsible use include limiting access to trusted staff, monitoring AI activity, upgrading software and models to repair problems and guard against new vulnerabilities, and ensuring users understand AI constraints.

A risk assessment should be done and dedicated defences should follow to defend the regions of high priority. An incident response plan minimises the harm and gets things back to normal fast. Minimum security measures are required for compliance with relevant legislation and to decrease the risk of abuse.

"In recent years, the growth of mobile internet, online banking and digitalisation of public services have contributed to an accelerated growth of the use of digital technologies in Ecuador. With the advance of AI (Artificial Intelligence) that provides us a personal assistant on mobile devices and direct access via the Internet, and machine learning (a subset that uses algorithms and statistical models that allow systems to learn and adapt to data without the need for explicit programming), in addition to the use of natural language processing (NLP) that gives AI systems the ability to understand, interpret, generate and interact with human languages, exposure to cybercrimes has increased which are becoming increasingly sophisticated due to the malicious use of artificial intelligence (AI) in their processes. According to the Attorney General's Office, in 2021, 5237 cybercrime reports were filed, which represents a 129% rise in relation to 2020 [6]. The 2021 Cybercrime Reports in Ecuador.

8. Future trends

Artificial intelligence (AI) will revolutionise the face of cybercrime. A growing tool of criminals [3], its mechanisms for illicit activity differ fundamentally from traditional crime-enabling technologies—criminal exploitation of the Internet, for example, has commonly involved genuine or downloaded programs, whereas AI synthesises materials on demand. Already, fewer, less specialised models can reproduce a large range of components (e.g. code, text, graphics). Cybercrime employing AI is become faster, more anonymous and cheaper [1]. New criminal techniques are being developed for attack programming, phishing emails, malware generation, and fraudulent text production. Actors who are able to develop criminal strategy need only upload a few prompts to a free public-of-the-market language model and modify the output sufficiently to remain under detection thresholds. Even more widely circulated are huge, specialised models. Other disciplines such as art or journalism, have gone through similar upheavals; there are more disruptive AI developments to come. Still, many applications need domain expertise, which is a prerequisite that still need human competence [2]. The requirement for organisations to analyse and respond to AI-induced risk has increased dramatically, and risks left unaddressed invite more civil and criminal culpability.

Trends like edge computing and real-time analytics can improve system responsiveness and reduce latency, making AI-sensor systems more realistic for time-sensitive applications. Such advancements will lead to a growth in intelligent and autonomous settings and will be the future of smart technologies [7].

9. Conclusion

The conclusions of this debate are twofold: the general results and practical consequences, and, in particular, recommendations for safe and responsible use, particularly in the context of help. When considering whether AI enhances or lessens the threat of cybercrime, it is apparent that it provides new options for the criminal user and expands the toolkit for defenders at the same time. Instead of banning AI, which is probably impossible and will merely force misuse underground, the best thing to do is raise awareness of the hazards and adopt common-sense steps to minimise exposure. Any implementation, then, should be accompanied by a standard set of safeguards to prevent possible issues and remain within legal constraints. The first steps include limiting access to a small number of trusted users, monitoring for anomalous behaviour, keeping the system updated, and educating all users on safe practices and the possibility of AI misuse [2] [4] [1]

References

1. S. Dilek, H. Cakir, M. Aydin. (2015). **A Review on the Application of Artificial Intelligence Techniques to Combat Cyber Crimes** https://arxiv.org/abs/1502.03552
2. Velasco, C. (2022). Cybercrime and Artificial Intelligence. Summary of the activity of the international organisations on criminal justice and the international applicable instruments ncbi.nim.nih.gov
3. Mayer, M. ((2018). Cyber Power and Artificial Intelligence: A Strategic Perspective. IFS Perspectives 4/2018
4. Anwar Pasha, S., Ali, S., & Jeljeli, R. (2022). Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan. National Center for Biotechnology Information
5. Polemi, N., Praça, I., Kioskli, K., & Bécue, A. (2024). Challenges and efforts in managing AI trustworthiness risks: a state of knowledge. ncbi.nlm.nih.gov
6. Carlos Varela Enríquez, Renato Toasa and Maryory Urdaneta The Use of Artificial Intelligence in Cybercrime: Impact Analysis in Ecuador and Mitigation Strategies J. Cybersecur. Priv.2025, 5(4), 100;https://doi.org/10.3390/jcp5040100 Accessed from https://www.mdpi.com/on 13/05/26
7. V. Basil Hans. Looking into how modern technology combines sensors and Artificial Intelligence. Recent Trends in Sensor Research & Technology. 2026; 13(01):