Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Role of AI in Tackling Cybercrime

Ivan Johns[a]

[a]Symbiosis International University, Pune, India

Received 25 July 2022; *Accepted* 23 August 2022; *Published* 25 August 2022

Criminals are increasingly leveraging cyberspace to perform a variety of cybercrimes as information technology (IT) improves. Intrusions and other threats pose a significant risk to cyber infrastructures. With recent advances in artificial intelligence, the danger of cyberattacks and crimes has increased rapidly. It has been used in nearly every branch of science and engineering. Artificial intelligence (AI)-based cybersecurity products have evolved to assist information security teams in swiftly and effectively reducing breach risk and improving their security posture. This article analyzes the use of artificial intelligence technology in tackling cybercrime and its disadvantages of the same.

Keywords: *artificial intelligence, cybercrime, information technology, cyber-attacks.*

INTRODUCTION

Criminals are becoming more adept at catching up with current societal and technological advancements. As per a McAfee-led analysis, cybercrime is responsible for about $600 billion in global damages, or nearly 1% of global GDP. According to a recent Verizon Data Breach Investigation Report, upwards of half of all security infringements go undiscovered for several months. Most conventional methods concentrate on simply accumulating information about malware, hacking attempts, identity fraud, data leaks, phishing campaigns, and so on, converting these into threat signatures (digital fingerprints of the threat), and afterward analyzing streams of statistical information for similar trends. The term "artificial intelligence" refers to a group of technological advancements whose shared characteristic is the capacity to simulate human cognition, particularly the human brain's ability to reason, learn, and act appropriately when faced with a particular environment. AI spans a vast terrain of technologies and fields of scientific research, from computer science to mathematics and neurology, in an even larger sense than is the case with all matters cyber.

The technologies of AI can generally be viewed as existing across three broad categories: (1) sensing and perception, (2) movement, and (3) machine thinking and learning; however, there is considerable crossover and significant within-category diversity. Machine learning, scientific study, and the development of methods for pattern recognition and knowledge generation without preprogrammed instructions about interpreting information is perhaps the most critical element in this field. Machine learning entails the input of data and an expected outcome to an algorithm that infers, learns about such a specific issue reflected in the data, and produces another algorithm created to enable intelligent engagement. This algorithm is frequently referred to as a "learner." In other words, more advanced AI algorithms more effectively analyze data to create better processes rather than using processing capacity to overpower computational constraints.

Cybercrime also develops along with technology. Cybercriminals have proven themselves to be nothing if not resourceful and opportunistic in the wake of the latest increase in remote labour and the expansion of the attack surface that went along with it. AI-powered security technologies can foresee assaults and immediately respond to them. Future cyberattacks are predicted to happen in milliseconds; therefore, being able to react quickly is essential. To successfully guard against threats, humans' current jobs will change to guaranteeing that security systems are given enough intelligence.

CYBERSECURITY

According to prevailing trends and statistics, cybercriminals are mainly depending on IoT to write and disseminate malware and target ransomware attacks that are greatly enhanced by

AI technologies. This growth is expected to continue as more than 2.5 million devices, which include industrial devices and critical infrastructure contractors, are expected to be fully connected digitally over the next five years, making businesses and consumers more susceptible to cyberattacks.

Cybersecurity refers to the numerous measures/techniques used to secure interconnected networks, programs, technology, and data against cyber-attacks. Pathways are built by malicious and offensive behaviours that allow attackers (hackers) unauthorized access to computer systems or networks. These acts are referred to as cyber threats. Predators exploit defects and weaknesses in the device or software to construct these channels. There are several cyber hazards, such as:

1. Virus- Its full title is Vital Information Resources under Seize. This virus repeats itself by inserting and altering its code into applications. Its deployment is dependent on an individual launching the software. Viruses create damage by distributing across consumer email, file corruption, data loss, and wiping data from the hard drive.

2. Spyware- Malware that attempts to acquire data on the activity of the infected system collects passwords and all system activities. Such malware includes adware, data breaches, botnets, key loggers, and networms.

3. Trojans- Trojans do not multiply themselves; instead, they appear essential. It takes the route of a Denial of Service (DoS) attack. It deletes saved data and creates paths for hackers. Trojans are spread through online file repositories and archives.

4. Worms- Worms, unlike Trojans, duplicate themselves without modifying the user-approved software data. Its sudden duplication eventually absorbs all network resources (like bandwidth and CPU cycles), resulting in a lack of resources for user-approved applications. Certain worms also attempt to steal sensitive information from vital files. Worms can be spread using the Internet Relay Chat protocol or attachments sent via email.

Cyber security provides the availability, confidentiality, and integrity of your system or network, allowing it to operate effectively while maintaining security.

AI IN SECURITY IMPLEMENTATION

AI has emerged as a reliable alternative to dealing with cyber-world threats. Machine learning and artificial intelligence (AI) are being used to track illegal and malicious activities by comparing the actions of entities in a similar environment; AI in security systems is frequently used to distinguish "good" from "bad." More advanced AI security systems can go beyond recognizing good or bad behavior by analyzing large amounts of data and piecing together related activities that may signal suspicious behavior by anonymous entities. Because of widespread networked computers, the internet, and mobile applications, cyber-attacks have grown increasingly prevalent and diversified. Many connected gadgets present cyber thieves with a plethora of attack vectors. Furthermore, the access points lack security. The rise of IoT has resulted in a larger-than-ever surge of cyber-attacks. Cyber fraud is a common topic in the news and media. Traditional cyber-security measures are sometimes referred to as "signature-based techniques." Conventional cyber security approaches need enormous human effort to identify risks, derive risk features, and integrate threat characteristics into software to detect attacks. Furthermore, traditional tactics are not as complex as modern cyber-attacks. The CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) illustrates how AI and cyber-security are linked. The user must enter the alphabet in a masked picture or with another distortion in this assessment.

When traditional security systems prove slow and ineffective, artificial intelligence approaches improve overall security architecture and performance by providing excellent protection from a growing variety of complex cyber-attacks. Firms using Artificial Intelligence in their internal and external processes have already improved their business processes and financial outcomes. AI-powered cyber security solutions have also aided in rapidly developing data-driven security models across domains. Some cybercriminals modify their malware code to make it undetectable, so security software fails to recognize it as dangerous. Moreover, detecting all types of malware is a huge challenge. Artificial intelligence and machine learning are both excellent anti-malware defence technologies. When a new type of malware is discovered, the system can cross-reference it with the database, evaluate the code, and prevent an attack. This method is effective even when harmful code is buried beneath a large amount of innocuous or useless code. An artificial intelligence monitoring technology can track everything users do regularly and respond appropriately by detecting anomalies. In today's environment, this is a significant advantage.

INTERNATIONAL CONTEXT

Many governments worldwide are evaluating the implementation of AI applications and systems to assist them in carrying out their missions, specifically to aid in recognizing and projecting crime. Furthermore, national security and intelligence agencies have recognized AI's capacity to foster and achieve national and public security goals. Significant advancements in AI technologies, including facial recognition in criminal justice, unmanned aerial vehicles, fatal autonomous weapons, and self-driving automobiles, have the ability to be used for destructive activities and harm persons' rights and liberties if not designed correctly or controlled. There is presently an open dialogue in global policy and legislative circles about revising and improving the liability structure and limits for AI systems and equipment. However, given the complex nature of the subject matter and the various legal perspectives on civil liability worldwide, there is unlikely to be a general agreement on a harmonized and uniform answer in the coming years.

The prevalent use of technologies based on biometric identification merits additional attention in the global political realm since facial recognition is very enticing for certain government agencies to improve elements of social security and protection in order to prioritize national security actions, such as terrorist activities, this technology may also raise pertinent and controversial problems regarding the enforcement of fundamental rights, such as privacy and data protection in accordance with established international conventions and multilateral treaties.

Deepfake misuse and overuse have now become a significant cause of concern in national politics and enforcement agencies. Deepfakes have been used to imitate legislators, public figures, and company CEOs, and they can be used in conjunction with social engineering techniques and system automation to perform malicious, illegal activities and cyberattacks. Deep fake methods are increasingly used for nefarious reasons and are currently being abused globally by cybercriminals. Spoofing of sounds and recordings raises pertinent and complicated legal hurdles for investigating and prosecuting such offences. To begin with, numerous law enforcement agencies around the world still do not have full potential and trained professionals to secure proof across territorial boundaries, and the absence of legal structures, especially procedural metrics in criminal law, to order the retention of electronic information and investigate cybercrime is another major impediment.

Second, because the majority of these breaches are generally concocted by well-organized criminal organizations based in different territories, there is a specific need for multilateralism, particularly close partnership with worldwide service providers to safeguard consumer and traffic information and also to undertake more timely inquiry and law enforcement actions with other nations through the rollout of joint operation teams in order to be able to detect the perpetrators. Cross-border cybercrime findings are complicated and time-consuming, and the offenders are not always convicted.

The European Commission released its long-awaited Regulation proposal for Artificial Intelligence Systems on April 21, 20021. The proposition includes broad and stringent guidelines and obligations until AI facilities can be introduced into the European market, depending on the risk assessments at various levels. The European Commission's legislation also expressly prohibits AI practices that may breach EU principles and individuals' fundamental rights. It establishes the European Artificial Intelligence Board (EIAB) as the authorized agency overseeing the regulation's implementation and enforcement in the EU. The United Nations Interregional Crime and Justice Research Institute's Centre for Artificial Intelligence and Robotics (UNICRI), a research organization of the United Nations, is very involved in the organization of seminars, documentation, and reports to better understand the realm of robotics and Artificial intelligence and to enable an in-depth insight of the offences and dangers performed via Ai technologies among law enforcement officers, lawmakers, professionals, academia, and civil society.

DISADVANTAGES OF ARTIFICIAL INTELLIGENCE

Though there are numerous benefits to using artificial intelligence in cyber security, there are some drawbacks as well.

- One of the most significant problems in applying AI in cyber security is that it necessitates more funds and resources than conventional non-AI cyber security solutions. This is due, in part, to the high cost of cyber security solutions based on AI systems. As a result, they have typically been too costly for many firms, particularly small and medium-sized enterprises (SMBs). However, emerging security-as-a-service (SaaS) technologies are lowering the cost of AI cyber security solutions for enterprises
- Artificial intelligence in cyber security creates additional risks to cybersecurity. Much like AI technology may be used to detect and thwart cyberattacks quickly, hackers can utilize it to conduct more complex cyberattacks. This is due, in part, to the fact that exposure to robust artificial intelligence solutions and machine learning tools is becoming more widespread as the expense of creating and deploying these technologies fall. This implies that attackers may construct more complicated and adaptable harmful software more simply and at a smaller price.
- Another underappreciated threat is that if a firm incorporates AI and machine learning into its cyber security plan, individuals will feel protected and lower their guard, known as human complacency.
- Another concern of artificial intelligence in cyber security is adversarial AI, which is the creation and use of AI for harmful reasons. Adversarial AI is when machine learning systems misread data entering the system and respond in a manner that benefits the perpetrator. This happens when the neural networks of an AI system are misled into failing to identify or mislabel things as a result of purposely changed inputs.

FUTURE SCOPE

In cybersecurity, artificial intelligence has several uses. As cloud-based solutions become more common, the necessity for AI cybersecurity will rise. As the threat environment evolves, AI-driven systems taught and tuned by professionals using high-quality data will become increasingly essential to protect digital assets. AI cybersecurity is expected to grow at a CAGR of 30.12% to $40.61 billion by 2026, up from $4.89 billion in 2018. In the near future, AI will be capable of predicting occurrences and taking preemptive measures in cybersecurity. It is also expected that preventative measures would be widely used, allowing firms to breathe easier and remain poised in the event of a cyberattack. Furthermore, AI will be able to recognize complicated cyber-attacks, interrupt them, and avoid potential efforts by cybercriminals by identifying their credentials and implementing solutions against them. Furthermore, we may anticipate enhanced automated detection systems that recognize attacks with a strong likelihood without enormous running costs.

CONCLUSION

Artificial intelligence (AI) has evolved as a necessary tool for supplementing the work of human information security teams. Because people can no longer fully expand to guard the dynamic business attack vector, AI delivers much-needed analysis and threat detection that cybersecurity experts can act on to decrease attack risk and enhance security infrastructure. AI in security can spot potential risks, quickly detect malware on a network, direct incident response, and detect attacks before they occur. Action plans and more collaborations are required in the context of Ai and cybercrime to guarantee that involved parties, especially law enforcement and the judicial system, gain a deeper understanding of the intricacies and aspects of AI systems and begin developing collaboration alliances that may aid in identifying and locating culprits who abuse AI systems with the assistance of the corporate industry. It is a complicated task and requires the cooperation of the technology and commercial communities; or else, secluded investigatory and law enforcement attempts against criminals using AI systems are likely to fail.