Artificial Intelligence& Cyber Crimes

Kalpana Thakur

Assistant Professor, University Institute of Law, Sant Baba Bhag Singh University, Jalandhar

Kalpanathakur31@gmail.com

Abstract:

There's a lot of talk about the impact of new technologies on the cybersecurity domain. Artificial intelligence, in particular, is seen as a potential game-changer. Artificial intelligence is considered as blessing as well as curse to businessman, customers etc. It is a technology which provided us with speech recognition technology like Siri; Google's search engine and Facebook's facial recognition software. Even there are some companies deals with credit card are using AI to help financial institutions in order to prevent billions of dollars in fraud annually. But what is the role of this application in cyber security? Is this an advantage or a threat to company's digital security?

1. Introduction

With the advancement in Information Technology, this technology is used by criminals to commit several Cyber-crimes. With these growing trends of information technology, Internet computing raised important questions about the information security and its privacy. Infrastructures of cyber are weak to intrusions and other threats. With the development of technology, many devices like sensors and detectors are not sufficient to monitor and protected the cyber infrastructures. So, there is a need of more refined Information Technology that can check and detect the problems. The cyber defense system needs to be flexible so that it can be easily adaptable and capable to detect a wider variety of threats and make knowledgeable decisions. Human interference is not sufficient for analysis of cyber-attacks and suitable response. Most of these cyber-attacks are conceded out by computer worms and viruses which are considered as intelligent agents and that is a biggest fact; now here we need an intelligent representative to combat cyber-attacks which can detect, evaluate and respond to cyber-attacks[1].

[1] Dilek, Selma et. al., "Applications of Artificial Intelligence Techniques To Combatting Cyber Crimes: A Review", *International Journal of Artificial Intelligence & Applications (IJAIA),* Vol. 06, Issue No. 01, January 2015, p. 21.

Cyber interventions are a risk which poses threat to any kind of computer system. Once there was a time, when these cyber-attacks were committed by the educated and the specialist. But in today time as the development and expansion of internet, everyone has the knowledge more or less or even they have a tool to use in the commission of the cyber-crimes. The Conventional fixed algorithms have become ineffective to fight these cyber-attacks. This is the reason that we need pioneeringdevices like techniques of Artificial Intelligence which can provide learning ability to software to assist humans in fighting cyber-crimes[2].

Cyber Crimes: In the cyber world, cyber-crime is the most complicated problem. They are the crimes which are committed with the use of computer on internet as a tool or some target. Cyber-crimes are those sorts of which genre is the conventional crime in which computer is either an object or an subject of the conduct constituting the crime or we can say cyber-crime can be defined as any criminal activity which uses a computer either as an target or a way for perpetuating crimes which comes within the ambit of cyber-crime. In order to commit the cyber-crimes like Financial Crimes, Sales of Illegal Articles, Pornography, Online Gambling, Intellectual Property Crimes, E-mail Spoofing, Cyber Defamation, Cyber Stalking etc, computer is used as an apparatus[3].

Conventional and Cyber-crimes: Ostensibly, there is no distinction between conventional and cyber-crime. But we can say there is a sleek line of difference between conventional and cyber-crime which lie in the connection of the medium of cases of cyber-crime[4].

Artificial Intelligence:

> **"***Super smart algorithms won't take all the jobs, they are learning faster than ever, doing everything from medical diagnostics to serving up ads".*

Well, Siri, Cortana and Google today are all intelligent digital personal assistants on various platforms (IOS, Android and Windows Mobile). In short, whenever we ask anything through our voice, they help us in finding the useful information for example: Say "where is the nearest

[2] Tyugu, E., "Artificial Intelligence in Cyber Defense", *3rd International Conference on Cyber Conflict (ICCC),* 2011, pp. 1-11.
[3] Singh, Prof. Gagandeep, "Cyber Crime in the Society: Problems & Preventions", *One Day National Seminar on Criminal Justice System and Theories of Punishment in India: Emerging Issues and Dimensions,* UILS, Punjab University S.S.G. Regional Centre, March 08, 2019, Hoshiarpur, p. 257.
[4] Ibid.

Chemist Shop?" or "Remind me to pick X at 9 o' clock" and in this they will respond by finding the information. When they find then that information relay on phone, moreover they send the command to her apps. Today our house, banks, cars, games, calculators, smartphones etc. all uses the Artificial Intelligence daily. It is the encouragement of human intelligence which is administered by the machines, especiallyour computer systems[5].

2. **Artificial Intelligence: A gate for cyber-crime:**

Cybercriminals are now permitting to use, the technology like never before only because of artificial intelligence, and thethings on internet relies on it immensely. Simply we can say Artificial Intelligence developments are making it quite easy for cybercriminal to breach the computer systems and steal the data. Moreover, Artificial Intelligence is developing at a speedy rate; there is now reason for concern.Cybercriminals are generally adopted the latest technologies such as AI. They do this only to create such attack which is more powerful, less detectable and has farther-reaching effects. Also, because of the huge extension in cloud computing the entire cybersecurity environment is as complex as it has ever been.As AI capabilities become more powerful, it is only normal that AI systems will be used to create new threats and aid for existing ones. Additionally, the ever-greater influence that AI is having on the physical world - think drones and automobiles - could, in theory, result in some frightening results[6].Unfortunately, cybercriminals are well aware and are taking advantage of this weakness.Unprepared and understaffed companies can do very less in order to prevent such attacks, or respond finally when they happen. This cybersecurity skillsshortage means that demand is cosmic, prices are high, and access to reach the cybersecurity professionals have many blockades. These are very difficult to overcome, particularly for smaller companies[7].

Artificial Intelligence (AI) to truly hold digital transformation, on the other hand cyber criminals are using the same technique to weakenthe cybersecurity systems in place in order to carry out cyber-crimes. Therefore, it is the time for the companies to start discussing the sharing ideas that how to deal with this peril. Subsequently, in an interview with DataQuest, *Venkat Krishnapur,*

[5] Sood, Sneh, "Artificial Intelligence", *Hello!!! Artificial Intelligence – The Future of Human Mind,* Annual Magazine, JCI Jalandhar.
[6] James, Luke, "How Artificial Intelligence Will Fight Modern Hackers and Cybercrime", *MUO,* October 24, 2018 available at https://www.makeuseof.com/tag/artificial-intelligence-fight-cybercrime/.
[7] Ibid.

Vice-President of Engineering and Managing Director, McAfee India, spoke out on how the cybercrime domain is evolving, how organizations like *CERT-In and the Government of India* has handled this issue and there is need to take the steps in order to develop a robust cybersecurity system[8].

3. New Cyber Crime Threat: AI

According to *Silvino Schlickmann Jr, Assistant-Director Research & Innovation* at the international policing agency,"with the increaseclevernessaccessible to criminals such as chat bots will make them to rapidly upscale the scope of their targets. Now the machines can use natural languages, they can talk to people which they will never know that they are dealing with a machine. There is no longer one computer attacking the one person but has one computer which attacked the hundreds of thousands of victims. If AI is taken and apply it to somewhat like Block chain, it can seehow many transactions are making and what the amounts are? It is that information which cyber criminals can use easily. Though, Artificial Intelligence and Machine Learning also plays a vital role in order to protect from crime, and also in catching the criminals", said *Schlickmann*. It is an exceptional data and collection tool which can help to understand the bigger picture. For example, Police can take this and with its help try to identify money laundering schemes. Every single day, a new family of malware or ransomware is created around the world and the nature of the danger means that it can be very difficult to effectively deal because if you break into a house and steal a single key, it will leave some evidence for the police. But that is not true in cyber space. Once you are in, you can do nothing but steal everything, and leave the same amount of evidence. The size of the crime is no longer connected to the amount of effort which is required to examine it. In this, there is no need to be an important person, but the data is important to you and this thing is known to the criminals. Every single area of the society is susceptible to this attack. Today criminals are targeted everyone with the help of technology and collected the profit one by one[9].

---

[8] R, Supriya, "Cyber Criminals are using the Artificial Intelligence to Break into Advanced Security Systems', *DATAQUEST,* available at https://www.dqindia.com/cyber-criminals-using-artificial-intelligence-break-advanced-security-systems/.

[9]IFSEC GLOBAL, "Artificial Intelligence: the new cyber-crime threat", available at https://www.ifsecglobal.com/ifsec/artificial-intelligence-threat/.

4. Conclusion

In today's alphanumeric world, Artificial Intelligence created a bang and become advanced with the change of time and development. But, what will happenif Artificial Intelligence became the main reason for a Cyber-attack? By the year of 2021, Artificial Intelligent seemed to be answerable for cybercrime losses. If Artificial Intelligence can boost and improved the cybersecurity effectively, it can also lead to make the task even more complicated. Now Hackers will find the new ways to use and modify Artificial Intelligence in the market to cause harm. To tackle with this issue, there is no cyber security strategy. Most of the applications of Artificial Intelligence, summits the introduction of the Machine Learning capabilities. Thereis the software, protocols or raw code, which is added to the IT system of a company. Thereafter, another layer of security is added to the safety protocols, which has an ability to learn from threats, security breaches and other data collected through their mechanisms. Thus, AI works through thousands of data and learns from the same.However, whatever works for cybersecurity experts also works for the hackers. All the data found out on the internet, can be used from the other side of the cybersecurity spectrum. This is how, security breaches could be prevented by AI-powered systems through the data.