PSYCHOLOGY AND EDUCATION (2021) 58(5), ISSN 1553 - 6939
Article Received: 22th November, 2020; Article Revised: 26th March, 2021; Article Accepted: 26th April, 2021

Education Regarding Impact of AI on Cybercrimes and Liability for AI

Dr. Anusuya Yadav*
Assistant Professor, Law Department, MDU, Rohtak, Haryana, India.

Abstract
Artificial Intelligence is a well-known branch of computer science which remained positioned on the top inrecent years. There are numerous applications of AI, most often we use them every day. Talking to Digital Assistant, Spam Email Filtration, Getting the Shortest Available Path on Google Maps, all of these are basic applications of AI. We use these on daily basis. AI proves itself to be a very powerful tool for the digital future. With the tremendous popularity that AI has gained over the years, it has major drawbacks too.AI initiated cyberattacks are not uncommon things anymore.In the 2010s, it has been seen that AI and ML (Machine Learning) were used by hackers in data breaches and in exploiting systems. Thus both AI and ML are becoming threats to the future. Numerous Cyber Laws comment on the Liability of AI. This paper focuses on the impact of Artificial Intelligence on Cyber Crimes and Cyber Laws, and the limitations of the use of Artificial Intelligence on a very large scale.

Keywords: Artificial Intelligence, Machine Learning, Cyber Crimes, Cyber Laws, Cyber Security.

Introduction

In a world that is running on social networking, online transactions, cloud storages, self-controlled devices and big data, information security and digital privacy are facing permanent threats. Cyber Crimes and their damage are increasing everyday due to excessive use of the internet and computers. Digital Illiteracy is a very huge problem among internet users. In 2021, the Internet has about 4.7 billion active users [1]. In the year 2020, Asia ranked first with nearly 2.6 billion active internet users and Europe stood second with 900 million [2].This massive usage of the internet is inviting several advanced technologies to ease our life. Whether it's smart gadgets, self-driving cars or robots. Blockchain, Internet of Things, Machine Learning, Artificial Intelligence, Computer Vision, Augmented Reality, and Virtual Reality, are some of the modern-day technologies that uplifted human life to a very high standard [3]. A modern-day terrorist does not need a bomb, explosives or a gun, he can cause a lot of havoc just with the help of a small computer. This vulnerability is only originated due to the excessive use of the Computer.

As the use of these cutting-edge technologies is increasing, digital privacy and security are becoming weak. Where the creator of the technology has to work on every aspect, an unethical hacker or a cyber-criminal has to find only a small

deficiency to exploit the same thing. Many types of cyber-crimes have taken birth today. As their age is increasing, we get to see their more fiery form. Where earlier cyber-attacks were only on large scale organizations, today the same cyber-attacks also happen to individuals. Phishing is the most occurring cyber-attack in the world [4]. It is a social engineering attack in which fraud is done by claiming someone else's identity. Even online transactions are causing big problems. Money laundering is a big problem since old times which is promoting cyber-crime and illegal activities, but today where there are untraceable transaction technologies like monero and pirate chain, it is making it even more harmful [5].

Every day there is a new cyber-attack and its impact tumbles on security infrastructure and these effects have led to what we see cybersecurity today. In the 1990s viruses and worms were the only security threats, but today hackers seem to reach so far. This can be easily understood by looking at the growth of the cybersecurity industry in recent years. Looking at the current situation of the cybersecurity industry it can be said that hackers are one step ahead.

When similar technologies throughout economies are used without alteration, then it increases the chances that cyber-attacks can infiltrate several organizations at the same time. This results in the crumbling of multiple supply chains simultaneously. This way when the implementation of modern-day technologies is increasing rapidly, it also becomes easy to target more organizations/individuals at the same time.

Definition of AI and Examples

A computer simply is an electronic device that works on the instruction of a human being. It cannot execute any taskon its own. Normally it only calculates and makes logical decisions, and that too when humans give them instructions [6]. For example, when we ask a virtual assistant to play a song, then we give instructions to it by voice command. And it is already present in its memory, that whenever any user asks to play a song, then the assistant should play that song. Thus whenever we give instructions to the computer either by voice command or from keyboard or through any other input device, the computer executes the tasks according to the command or instruction that a user gives. This is the traditional working of a computer. But Artificial Intelligence has completely changed this thing.

Artificial Intelligence means we are giving computers the ability to think on their own so that they can learn by themselves and solve problems and have the capability to make decisions on their own. In other words, Artificial Intelligence refers to the human-like intellect demonstrated by any computer, robot or any other electronic gadget, such as greeting people, automatic score prediction, etc. Thus an AI System will automatically take inputs and give the output by analysing the input accordingly [7]. Nowadays smartphones have more powerful chargers that can charge the batteries in very little time, but the shortcoming of the powerful chargers is that if the charger is plugged in for a long time, even if the battery is charged, they can damage the battery. And the biggest problem is that what if a user plugs in a charger at night? The battery will get charged in very little time, but usually, an

adult sleeps an average of 6 hours. An efficient solution to this came with the implementation of AI. The proposed system detects the time whether it's day or night and limits the charging speed accordingly. Similarly, there are a lot of other examples as well.

Working of AI

Building an Artificial Intelligence system is a watchful process of reverse engineering because the making of an AI system requires combining the qualities of human intelligence and machines. The desired objectives of an AI system are learning, reasoning, and acuity [8]. Deep dive into an AI system shows that the working of it is a combined form of all its subdivisions. The subdivisions of AI are as follows:

- **Machine Learning:** ML deals with the making of theoretical computational learning and learning machines. ML teaches a machine how to perform based on the previous learning and provided data. Just like we think about what to do based on the present situation and our past experience. The goal of ML from an AI perspective is to understand the learning phenomenon in humans and computers and to accomplish learning proficiency in computers [9].
- **Deep Learning:** Deep Learning is a subdivision of ML which mainly concerns about the algorithms related to artificial neural networks. These artificial neural networksemulate how the human mind learns and thinks [10]. Deep Learning usually has three or more neural networks. Online Fraud Detection can be done using deep learning.
- **Computer Vision:** Computer Vision teaches a computer or a machine to understand and deduce digital images and videos similar to what humans think after looking at a picture or the real world [11]. Computer Vision basically provides the capability to the computer to see the world as humans see it. When a computer detects facial expressions like a smile, it uses Computer Vision only to determine that. It helps a machine to give better output decisions grounded on prior interpretations.

- **Cognitive Computing:**Cognitive Computing mimics and learns the thought process of humans. Where AI tries to replace human efforts, instead Cognitive Computing only tries to assist humans in decision making [12].

- **Neural Networks:** Neural networks include several layers. These layers are divided into three types, input, output, and some hidden layers. Figure 1.1 shows the Neural Network structure.The other names of Neural Networks are Artificial Neural Networks and Simulated Neural Networks [13]. Neural networks learn from input data and improve their accuracy over time.

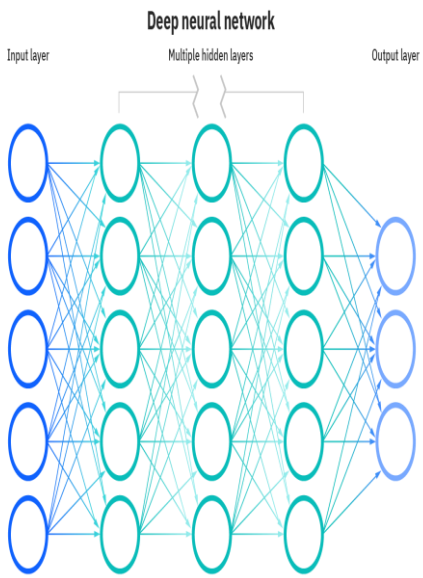

Fig 1.1: Neural Networks Structure (Source:https://www.ibm.com/cloud/learn/neural-networks)

- **Natural Language Processing:**NLP deals with the automatic manipulation of linguistics in a computer. Voice typing uses NLP, behind the scenes speech to text conversion is done [14]. Thus In this way, the more natural languages are processed, the more efficiency we will get when we give voice commands to the computer.

The following Venn diagram shows the relationship of AI and its subdivisions:

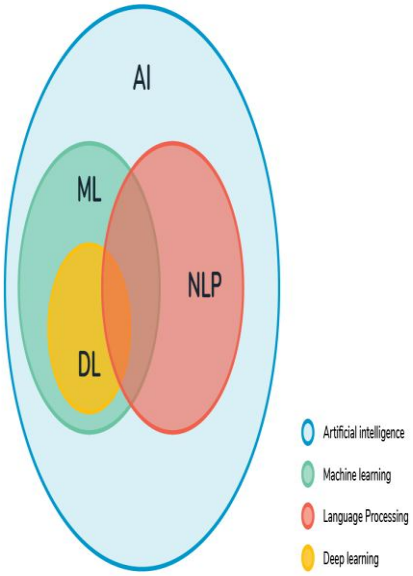

Fig 1.2: AI and its Subdivisions (Source: Sathiyakugan 2018)

Cyber Crimes and AI

AI and ML have positive and negative effects on Cybersecurity, likewise, AI and ML support and eradicate cybercrime.

AI supporting Cybercrimes:AI has changed the face of ever-growing Cybercrimes. In the 2010s, AI was first seen to be used in cybercrimes[15]. Ever since a rapid growth of the use of AI in committing cybercrimes has been seen. Just as we are getting new achievements in the field of AI, the use of AI in cybercrimes is also taking place on a large scale and with much thought. Because of Artificial Intelligence, both precision and accuracy are increasing in cybercrimes. Following are some of the real-world cyber-crime incidents in which the use of AI has been seen:

- **Deepfakes:** Deepfakes are fake images and videos which are created using AI. These can easily be used to defame an organization or individual. In February 2021, a

video of a person claiming to be Tom Cruise went viral on social media,though it didn't contain any hateful or misleading information [16]. This type of activities have been done before too, but the optimising algorithms of AI make it almost real. In 2018, an application called Deepnude was banned, that application was capable of making intimating pictures by removing clothes of people [17]. The pictures were found to look real. It used an open-source algorithm pix2pix developed by researchers at the University of California, Berkeley in 2017 [18].

- **AI-supported password guessing:** The process of hacking has a phase called recon or reconnaissance. In this phase, all the information is collected about the target. Generally, the people with high privilege are targeted, whether the attack is on an organization or an individual. Once the information about the targeted personis collected [19]. With this huge amount of data, it is possible to make AI models that may behave like individuals. Hence the password guessing can be done easily. Similar things are done, when we search for something on social media or digital entertainment platforms, they collect the data that we searched about and then algorithms are used to analyse this data. Then ads of similar things are shown to us if we don't have ad-free services.
- **Human Impersonation:** The first bot was used in 1994 to crawl web data. Since then bots are used to automate tasks, whether it is social media or online games, bots are present everywhere. To prevent these automated tasks, captcha verifications and human verifications are mainly used [20]. AI bots are so advanced that they can mimic human behaviour and pass the verifications.
- **AI-powered Cyber Attacks:**Similar to other fields, Hacking is now been automated. Nowadays AI is used to automate manual hacking tasks. Tools like Deepexploit use combinations of several hacking tools and automate the hacking tasks [21].
- **Voice Cloning:**Sound is just vibrations at some particular frequency. It's no very hard to clone a voice with the help of a computer, but there may be some differences when the voice is cloned by human instructions [22]. But AI can efficiently be used to clone voice with much accuracy.
- **Lamphone:**Lamphone is a technique that is used by hackers to listen to distant conversations by reading the vibrations of the light source present near the communication parties. When sound travels, the medium vibrates. So when this wave hits any surface, the surface vibrates [23]. Likewise, the incoming light from the source also vibrates. These vibrations are studied and algorithms are used to produce sound. And hence the conversation can be heard. The

threat model of lamphone can be seen below.

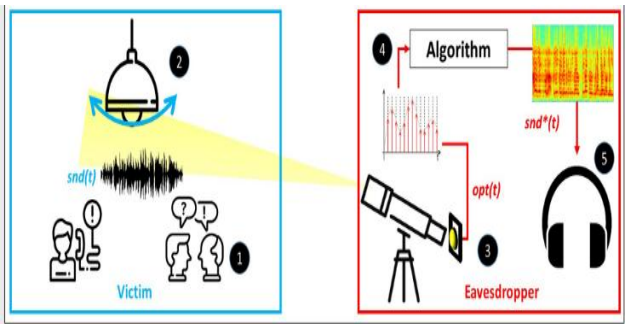

Fig 1.3: Lamphone's Threat Model(https://www.zdnet.com/a/hub/i/2020/06/13/f0be67b4-8311-4c03-b42a-67564397db04/lamphone-1.png)

Several other cyber-crimes often take place with the involvement of AI. There are many other incoming threats too to the other technologies. These include self-driving cars, and AI and IoT applications, etc [24].

AI eradicating Cybercrimes: Though AI helps cybersecurity a lot, cybersecurity sometimes seems to be slow in this game of cat and mouse. AI has many advantages in the field of cybersecurity. AI makes an organization more resilient to cyber-attacks [25]. Some of the applications of AI in the field of cybersecurity are:

- **Spam Detection:** Most of the spam is delivered through emails. The algorithms used by email service providers filter these spam emails [26]. And blocks them before they cause any damage.
- **Vulnerability Management:** When a system is continuously monitored, it is easy to detect what affects the system performance. Malware will either downgrade system performance or will create unwanted processes to run [27]. Hence the monitoring will detect the malware. Antivirus also follow a similar process, they detect malware either by digital signatures or by monitoring system processes.
- **Authentication Improvement:**The traditional authentication method of Login Id and password is good, but the best practices are having unique passwords of different accounts, regular password updation, good password strengths, etc. This method seems to be difficult [28]. Also, most of the users either don't change their passwords or have the same passwords for several accounts. This gives rise to vulnerabilities. The new Authentication methods like Iris scan seem to be quite better and easy. With almost no efforts, users need not to remember credentials.
- **Phishing Control:**It is the most common cyber-attack. By injecting fake forms into websites, and other web services hackers collect the login credentials of the users. Or hackers inject malware into systems by fooling users [29]. AI can prevent and report phishing. With the analysis and past experiences, AI can block or report most phishing sources.
- **Improved IDS:**IDS or Intrusion Detection System is a monitoring system that detects suspicious activity on any network and generates alerts. Thus when AI is integrated with IDS, it can predict

the risk factor and can provide a much more detailed report of the attack [30].

Cyber Laws and Liability for AI

As the development and use of AI are increasing rapidly, it is also true that we will be able to see the incidents of its failure. Whenever an autonomous system fails, who should be held responsible for that? The owner, or the manufacturer,or the user, or the system itself, the debate on it is still going on.In the 1980s, in Canada, a radiation therapy machine delivered excessive dose of radiation to cancer patients [31].The excessive delivery was due to some software flaw.Hospitals are still debating the liability. There are several parties involved in an AI system, and hence it becomes difficult to establish liability when something bad happens. Many factors can be considered to establish the liability.

The major reasons for the failure of AI include:

- Insufficient Data
- Flawed Implementation
- Complex Applications

Individually or a combination of these major causes can cause great harm.

The discussions on the liability of AI comes down to the Legality of AI systems. However, the debate on the legality of AI systems is also going on.Several researchers favour the grating of separate legal status to AI [32]. But there are others researchers as well, who think that granting separate legality will give rise to many new problems. Several other recommendations like the modifications in the present laws are also given. Australia, Estonia, and Germany have established policy positions while the Russian Federation and Japan have made several recommendations. Whereas the USA, India, China, UAE, UK, Finland, Sweden, and other few countries have ongoing preliminary discussions on this liability [33].Saudi Arabia is the only country to give human rights and duties within the state, to the AI humanoid robot named Sophia [34].

Impact of AI on Indian Legal System

The Indian legal sector is not so dependent on technology. Even today, lawyers consider their centuries-old methods better. The problem that comes in a little bit is that of data management and it can be solved a little with the help of a computer, for now, this is the only use of computer in the Indian legal system.

The legal system of India is very large and there are changes in it from time to time, so the difficulty is to find desired information out of the heap. The only help thatartificial intelligence can doin this work is, with the help of a computer, we can find the information we need within a few seconds.

It is not that AI is an unknown thing. Many AI startups related to the Indian legal system have started such as SpotDraft, CaseMine, and NearLaw [35]. Instead of the full use of AI, in these startups, only natural language processing has been used so that we can get the desired information quickly by inputting a keyword in any language [36].

There is a myth about AI in the Indian Legal System that AI can replace Lawyers. Those who think that AI or Robots can replace lawyers, then their thinking is absolutely wrong. It seems impossible from both the technical and the legal view

because the extensiveness of the Indian Legal System makes it very difficult to train AI models, and as per the Legal view, there's a lot more than just the decision making in the law sector. Hence AI or Robots cannot replace lawyers. However, there can be many helpful applications of AI in the Indian Legal System, which are as follows:

1. Due Diligence
2. Data Analytics
3. Document Review and Discovery
4. Electronic Billing
5. Intellectual Property

Conclusion

It is not a lie that both cybersecurity and cybercrime are taking advantage of artificial intelligence. As artificial intelligence changes, so are the change in its applications. Specifically, talking about cybercrimes, artificial intelligence is being used in big attacks these days. The reason for not able to control this thing is that cybercriminals can find any vulnerability to exploit systems, wherein cybersecurity everything is taken care of. That is why it becomes difficult for the Cybersecurity providers to find any shortcomings,before cyber-criminal does. It is not that only cybercriminals are taking advantage only, we also use a lot of artificial intelligence in everyday life. So now there are 2 faces of Artificial Intelligence like this.

Cyber Law and legal systems have also led to many changes due to artificial intelligence, but this does not mean that artificial intelligence can replace humans. A lot of legal systems are investing in artificial intelligence because, in reality, there are also many applications of artificial intelligence which help Lawyers or other members of the legal systems.

References

1. "Digital Users Worldwide 2020." Statista, www.statista.com/statistics/617136/digital-population-worldwide/.
2. "Internet Users by Global Regions 2019." Statista, 14 July 2020, www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/.
3. Russell, Stuart. "Artificial Intelligence." Ethics of Artificial Intelligence, 2020, pp. 327-341.
4. Zhu, Yada, and Jingrui He. "Social Phishing." Encyclopedia of Social Network Analysis and Mining, 2018, pp. 2762-2768.
5. Möser, Malte, et al. "An Empirical Analysis of Traceability in the Monero Blockchain." Proceedings on Privacy Enhancing Technologies, vol. 2018, no. 3, 2018, pp. 143-163.
6. Bohanec, Marko. (2009). Decision Making: A Computer-Science and Information-Technology Viewpoint. Interdisciplinary Description of Complex Systems - scientific journal. 7. 22-37.
7. Dick, S. (2019). Artificial Intelligence. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.92fe150c
8. Varghese, Mathew. (2021). Creative Work Versus Artificial Intelligence. 10.1007/978-981-15-9263-8_13.
9. Mishra, Vidushi& Agarwal, Manisha. (2020). Machine Learning. 10.1201/9781003054115-4.

10. "What is Artificial Intelligence? How Does AI Work, Applications and Future?" GreatLearning, 17 July 2020, www.mygreatlearning.com/blog/what-is-artificial-intelligence/.
11. Solyman, Ahmed. (2019). INTRODUCTION TO COMPUTER VISION (Computer Vision and Robotics).
12. Pagel, Peter &Portmann, Edy & Vey, Karin. (2018). Cognitive Computing. Informatik-Spektrum. 41. 1-4. 10.1007/s00287-018-1091-4.
13. Tanaka, Akinori&Tomiya, Akio & Hashimoto, Koji. (2021). Basics of Neural Networks. 10.1007/978-981-33-6108-9_3.\
14. Haney, Brian. (2019). Applied Natural Language Processing for Law Practice. SSRN Electronic Journal. 10.2139/ssrn.3476351.
15. "Cybercrime: AI's Growing Threat." Dark Reading, 20 Nov. 2020, www.darkreading.com/risk/cybercrime-ais-growing-threat-/a/d-id/1335924.
16. Vincent, James. "Tom Cruise Deepfake Creator Says Public Shouldn't Be Worried About 'one-click Fakes'." The Verge, 5 Mar. 2021, www.theverge.com/2021/3/5/22314980/tom-cruise-deepfake-tiktok-videos-ai-impersonator-chris-ume-miles-fisher.
17. "DeepNude App Banned on GitHub After Spreading to Multiple Platforms." Rogue Rocket, 10 July 2019, roguerocket.com/2019/07/10/deepnude-app-banned-on-github-after-spreading-to-multiple-platforms/.
18. "DeepFake Nudie App Goes Viral, Then Shuts Down." Medium, 28 June 2019, medium.com/syncedreview/deepfake-nudie-app-goes-viral-then-shuts-down-577e8c168dfb
19. "Artificial Intelligence Just Made Guessing Your Password a Whole Lot Easier." Science | AAAS, 15 Sept. 2017, www.sciencemag.org/news/2017/09/artificial-intelligence-just-made-guessing-your-password-whole-lot-easier.
20. Hitaj, Briland&Gasti, Paolo &Ateniese, Giuseppe & Perez-Cruz, Fernando. (2019). PassGAN: A Deep Learning Approach for Password Guessing. 10.1007/978-3-030-21568-2_11.
21. Kaloudi, Nektaria& Li, Jingyue. (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys (CSUR). 53. 1-34. 10.1145/3372823.
22. Arik, Sercan& Chen, Jitong& Peng, Kainan& Ping, Wei & Zhou, Yanqi. (2018). Neural Voice Cloning with a Few Samples.
23. Cimpanu, Catalin. "Lamphone Attack Lets Threat Actors Recover Conversations from Your Light Bulb." ZDNet, 13 June 2020, www.zdnet.com/article/lamphone-attack-lets-threat-actors-recover-conversations-from-your-light-bulb/.
24. Kh, Ryan. "Navigating the Benefits and Challenges of AI Implementation As New Threats Loom." Infosecurity Magazine, 14

Jan. 2021, www.infosecurity-magazine.com/opinions/benefits-challenges-ai/.

25. Dilek, Selma &Çakır, Hüseyin&Aydın, Mustafa. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications. 6. 10.5121/ijaia.2015.6102.
26. Gupta, Suparna&Saha, Soumyabrata& Das, Suman Kumar. (2021). SMS Spam Detection Using Machine Learning. Journal of Physics: Conference Series. 1797. 012017. 10.1088/1742-6596/1797/1/012017.
27. Raju, Godwin &Zavarsky, Pavol&Makanju, Adetokunbo & Malik, Yasir. (2019). Vulnerability assessment of machine learning based malware classification models. 1615-1618. 10.1145/3319619.3326897.
28. "How AI-Based, Zero-Effort Authentication is Changing the Customer Experience." BrightTALK - Discover and Learn with the World's Brightest Professionals - BrightTALK, www.brighttalk.com/webcast/635/342258/how-ai-based-zero-effort-authentication-is-changing-the-customer-experience.
29. Basit, Abdul & Zafar, Maham& Liu, Xuan &Javed, Abdul Rehman & Jalil, Zunera&Kifayat, Kashif. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems. 10.1007/s11235-020-00733-2.
30. Kanimozhi, V. & Jacob, Prem. (2019). Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing. 0033-0036. 10.1109/ICCSP.2019.8698029.
31. "A Civil Liability Regime for AI?" Lexology, 4 Nov. 2020, www.lexology.com/library/detail.aspx?g=8eb614b4-5067-482d-a49f-9a638bbf4621.
32. Zech, Herbert. (2021). Liability for AI: public policy considerations. ERA Forum. 22. 10.1007/s12027-020-00648-0.
33. "Civil Liability of Artificial Intelligence." Home, indiaai.gov.in/ai-standards/civil-liability-of-artificial-intelligence.
34. Chaudhary, Gyandeep. (2020). Artificial Intelligence: the Liability Paradox. SSRN Electronic Journal. 10.2139/ssrn.3709095.
35. "Impact of Artificial Intelligence on Indian Legal System." Legal Service India - Law, Lawyers and Legal Resources, www.legalserviceindia.com/legal/article-631-impact-of-artificial-intelligence-on-indian-legal-system.html.
36. Haney, Brian. (2019). Applied Natural Language Processing for Law Practice. SSRN Electronic Journal. 10.2139/ssrn.3476351.