Boones & Banes of using Artificial Intelligence for Cyber Security

By :

Name	P.Y.Meeriyagalla

Table of Contents

Abstract

In the modern world, artificial intelligence (AI) is used to make cybersecurity section smarter. Using AI for smart cybersecurity is an emerging topic today. According to that, today the tendency to use AI in cybersecurity is increasing. There are boons and banes of using artificial intelligence in cybersecurity. AI and cybersecurity do not have a long history. However, Artificial intelligence in AI is highly beneficial because it helps security experts to analyse cybercrimes easily and it can detect cybercrimes quicker than humans. In present, there are successful uses of AI in cybersecurity, for instances, anomaly detection, misuse detection, data exploration and, risk management. There is also banes of using AI in cybersecurity. Cybercriminals also can use these technologies to do cybercriminals. not only that but also as a result of the development of AI, it also has the ability to create new types of cyber threats. In present, there are malicious uses of AI in cybersecurity, for instances, automated social engineering attacks, automation of vulnerability discovery, sophisticated hacking and so on. When moving into the future AI-based security systems, they will be more improve than today. Future AI-based security systems will be more effective and will be more secure than today and that will be a huge step in the cybersecurity field. Using AI for cyber weaponization also will be more improve than today. That will be the worst effect of using AI for cybersecurity.

Introduction

Cybersecurity, one of the most important topics in the modern world and artificial intelligence, is using to make cybersecurity smarter and as a dark side of it, cybercriminals are using artificial intelligence to do cyberattacks.

Cybersecurity is the protection of computer systems, networks, programs and their hardware, software or electronic data from theft and damage from the digital attacks, Not only that but also cybersecurity helps to protect the systems from service Misdirections and disruptions.

Today the cybersecurity field is becoming more important and interesting due to increased trust in computer systems and increased reliance on the internet and wireless network standards, for instance, Bluetooth and Wifi, and also due to the development of smart devices, for example, smartphones, televisions etc. Therefore, the implementation of more effective cybersecurity measure is very important. However, it is a particular challenge today because the attackers are more innovative.

Therefore, to have more effective cyber-security measures, companies have taken the help of Artificial Intelligence for security improvement and protection of their data, networks and systems.

According to complex science, Artificial Intelligence is one of the sections which is dealing with the simulation of intelligent behaviour in computers, The capability of a machine or complex system to imitate human intelligence processes, learn from experiences and to be adaptable to new information and perform activities similar to human activities defined as Artificial Intelligence.

Artificial Intelligence is cybersecurity is advantageous because it helps security experts to analyze, study and understand cybercrimes easily, Artificial Intelligence can detect security errors very quicker than humans, Artificial Intelligence heightens the cybersecurity technologies that are used to fight cybercriminals and help to keep the important data, systems and networks safe. However, Artificial Intelligence may not be practical in all applications.

There is also a dar-side of using Artificial Intelligence in cybersecurity. In the present time-period, cybercriminals are using Artificial Intelligence as a new weapon to do attacks easily and smarter than before.

However, the modern world has paid its attention to use Artificial Intelligence for cybersecurity.

1. Evolution of the topic

The idea about Artificial Intelligence (AI) and robotics, first being appeared in the ancient Greek myths. The roots of the Artificial Intelligence are long and deep; however, the history of AI is not long as a century.

In 1943 Walter Pitts and Warren McCullough come up with the idea about the first mathematical model for building a neural network. Since 1943, organizations and companies tried to build intelligence machines and trying to apply AI into computer systems. In the 1990s, Bayesian logic was used to sift malicious email messages, and also use huge neural networks to categorize spams. These logics were included in early applications.

Information technology has paid attention to Artificial Intelligence to solve various kind of problem in Information Technology. The most important section is security in data, systems and networks. Therefore, the important one is developing a security-focus AI system for the networks. Automated systems for the security of networks can create using AI. To get a brief idea of that process, can take the human immune system's process as an example. In the human's body, when a problem is detected, white blood cells automatically take actions and fight for the problem to keep the body safe. As similar to that AI also can use to detect the threats and attacks in the networks and combat with them to keep the system safe.

The first generation of AI was designed to use machine learning standards to learn and integrate everything they could on specific tasks and then determine a specific sequence of action. Stimulating an artificial neural network and a central database, machine learning systems go through heaps of data to give analysis and apply machine learning tactics to decide a proper sequence of action, all at network speeds.

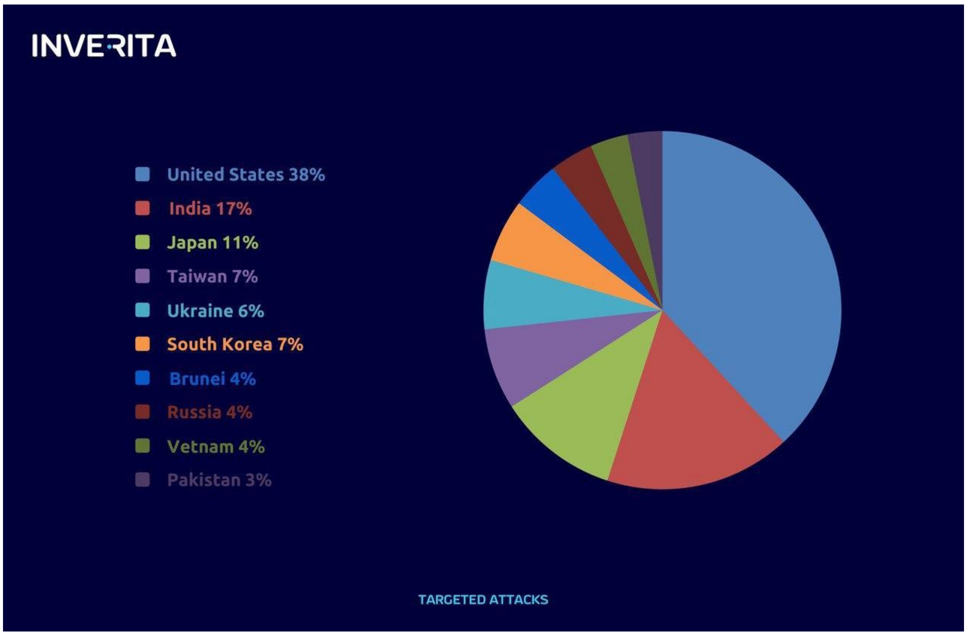
When AI moves into its second generation, AI uses its frequently modern ability to recognize patterns to significantly improve things like access control by disseminating learning nodes across an environment. In the present time, we can check and recognize fingerprint, face recognition and some patterns for instance iris pattern using the technology. However, with the second generation of AI, will be able to recognize persons who are using a more complex bio-footprint that are difficult to copy and theft like typing patterns, heartbeat rhythms. This is possible because, rather than depending on a single, centralized system, regional machine learning nodes can gather and process local data over time. This permits the system to recognize more special and unique characteristics that can then be shared back to the central AI brain.

These regional machine learning nodes could also be leveraged to point even the most subtle aberrations in normal network traffic to detect malicious actors and malware. This involves modern learning machines, and examples of this are now emerging in research and development laboratories. Artificial Intelligence can be used to develop

regionalized models base on the unique characteristics of each environment. As a result of it, cybercriminals' ability to persist undetected will be more inhibited.
As a result of the evolution of AI, organizations have opportunities to use AI for cybersecurity to develop and evolve the cybersecurity section.

Artificial Intelligence and machine learning system able to take over many of the menial and details-oriented tasks previously allocated to human resources will take a substantial bite out of the developing cybersecurity skills gap. By giving responsibilities to self-directed, self-learning processes which functions similar to human autoimmune systems – by tracking, for identifying and responding to security events – valuable cybersecurity experts will be able to focus their unique skillsets on higher-order planning and tactics.

However, all the high technology companies, for instance, Microsoft, Google, Cisco and Symantec as well as anti-virus companies are spending millions of dollars annually on AI and cybersecurity. However, within the previous few years (2015 - 2020), there has been a growth in startups around security tools that tout machine learning and AI.



Today, cybersecurity system can divide into 2 types. Those are expert systems and automated systems.

Expert Systems

Expert systems are built up, developed and maintained on the basis of, the identification of threat signatures which are designed to detect different types of threats to prevent attacks, for instance, methods or malicious code which are used to detect criminals.

Expert systems work well, but there is one problem. Signs of threats can be recognized after only the attack has been completed and accessed to the goal. In the future, it is much more difficult to avoid similar attacks. Consequently, these kinds of systems cannot secure opposed to the attacks called "zero-day" attacks, which are earlier unknown

Automated System

This software can be used to recognize the malicious and threatening attacks which can be developed in a system or networks. These recognitions are based on an analysis of old data. Resolving common classification problems is one such primary problems of machine learning. Since the system acts better, this approach can successfully prevent "zero-day attacks".

Artificial Intelligence uses for cybersecurity in many ways. Using modern AI techniques cybersecurity experts try to fulfil several tasks that allow developing security systems and preventing attacks.

- Anomaly detection

  The task that identifies normal behaviour falling within a specific range and recognizes every other behaviour as an anomaly and as a potential threat.

- Misuse detection

  An opposite task that recognizes malicious behaviour is recognised based on training with marked data and permits through all traffic not categorized as malicious.

- Data exploration

  Data exploration is a technique to recognize the features and attributes of the data, oftentimes using visual exploration which directly helps security analysts by rising the 'readability' of incoming requests.

- Risk management

  This is the task that evaluates the possibility of a particular user's behaviour to be malicious, which can either be done by attributing a definite risk score or categorizing users based on the possibility that some of the successful examples of Artificial Intelligence in cybersecurity.

(1) Automation Malware Defence

Traditional systems oftentimes unsuccessful to control the complete number of malware properly monthly. AI systems are useful to train and instruct to recogeize even the simplest behaviors and actions of malware and ransomware attacks before it accesses the system and then set apart them from the system.

How does Automation Malware Defence work:

To recognize potential threats, conventionally in the binary code of a program it is necessitated to utilize signatures to check for the existence of a specific sequence of characters. However, always malware does not come from binary code. Therefore skilful hackers know the method to access to a system without being getting caught. There is a behaviour-based algorithm. It uses probability models to take into account multiple scenarios and attributes of malicious or harmful code but does not analyse the code directly. This behaviour- based algorithm has lots of shortcomings. It is not popular as to the high cost and ineffectuality and maybe it identifies threats and malicious things when there is damage.

There is a more strong tool which is created by using AI. It is the 'Heuristic Algorithm'. The AI used to decide in case of analyzed code is dangerous and malicious and benign code. The main power is that the 'Heuristic Algorithm' can evolve and adapt like any other machine learning algorithm.

How does it use in practice :

There is a project called AI 2. The system using inputs from human experts foretells 85 per cent of cyber-attacks. AI2 compacts through data and identifies unusual activities by grouping the data into meaningful patterns. It fuses three different learning techniques which are unsupervised, and present the priority cases to analysts, to put the labels. Then, it makes an overseeing model. By continuous active learning system, it can revive frequently. Human analysts take these data and detect the real attacks, and combine that feedback into its models for the up-coming dataset.

(2) Automated Phishing Detection

Lots of phishing sites take your important data for instance login, password, phone numbers and credit card details by performing as trustworthy sites. Using machine learning algorithms can detect phishing attacks and can prevent it. AI and Machine Language(ML) can help to detect phishing attacks by categorizing messages similarly to email spam filters. Machine learning algorithms can increase its accuracy by the process of constant learning.

(3) Detection of Automated Data Theft

Data violations are one of the most prevailing threats which face by organizations in the present time. To mitigate issues similar to this, can use AI and machine learning-based algorithms to move slowly through secret channels like the deep or dark web and recognize data that has been shared by unknown malicious individuals.

The dark web is a part of the internet and that is the last layer of the internet. It is much more difficult to access the dark web. It is only can do with a special web browser for instance ‘Tor browser’.

Even though the dark web only can reach through encrypted an unnamed peer-to-peer communication channels, it needs to use specific safeguards for instance ‘CAPTCHA’. AI can necessarily mislead these systems mentioned above, to make them trust that the AI system which gathers information is a human and can range from answering small captcha using NLP(Natural Language Processing) to ask for invitations to private groups of malicious parties. Using machine vision can analyse images in real-time.

To be more effective :

ML algorithm should have the capability to identify various categories of data amendments, the ability to analyse the sensitivity of these identified types based on an examined model using natural language processing that is trained upon compliance mandates, the ability to track and record all transformations, genealogy, origin and provenance of such sensitive data types and it should have the ability to measure if such sensitive data types are breaking or disrupting any current or future expected compliance constraints.

(4) Context-aware Behavioral Analytics

Context-aware behavioural analytics are fixed on the grounds where an attack could be triggered by unusual behaviour. It acts as a model or a concept. To confirm the risk of the activities done by the user in close to real-time, these type of assessments are done using big data and machine learning. This approach is also called User Behavioral Analytics and in short form, it is called as 'UBA'

Why do we need this?

All of the security products and systems are converted and stored as a binary code. Expanding the common users' norm pattern behaviour support to deal with UBA.

By examining the historical tasks and comparing them within peer groups, ML models are instructed to construct baselines for each user, since it is complexed to create codes what behaviour can be usual.

If unusual events are being triggered they can be added by using a scoring method and the user can be provided with a combine risk score. Users who get a high score are separated and introduced to an analyst. They are presented with contextual data and along with their tasks and duties.

The formula for this is – risk probability impact Applications using UBA are able to give an actionable risk intelligence by following it.

(5) Honeypot-based Social Engineering Defence

Attackers can gain private information to make a deal with security systems by misleading people and abusing human minds. These attacks cannot be prevented by hardware and software alone. Applying social honeypots and fake persona ticks use to hold attacks is one practicable countermeasure.

Honeypots

Honeypot is a trick that uses in the Information Technology(IT) field by the malicious hackers, expecting that they will interact with it in a way that gives useful intelligence.

It can be used to find attackers by pretending as a fake user. The probability of preliminary agreement being spam is high since all the interactions with the honeypot is unrequested. To analyse whether the sender is malicious or harmless, machine learning can be used. This analysis is mechanically disseminated to all true employees' devices and these devices will mechanically prevent the attempts of communicating further from the malicious groups.

Banes of using AI in Cybersecurity

Hackers and even terrorists can use AI to do their attacks and harmful works. In the present time, with the excellent possibilities and uses of Artificial Intelligence, the likelihood of cyber attackers weaponizing it and using it to increase and expand and to improve their attacks is an enormous threat.

One of the biggest problems is that cybercriminals can use AI to automate cyber attacks on a large scale. In the present time, adversaries are depending on human resources to organise and coordinate their attacks. Cybercrime and cybersecurity path is going to change not only for the better but also for the bad because cybercriminals are using AI to do their malicious works.

Another issue is that cybercriminals can use AI and machine learning to complement the lack of human resources and save cost in cybercrimes, The investments and resources needed for implementing and coordinating such attacks will reduce massively and this kind of attacks can do more threat to cybersecurity. By relatively lower investments, cyber attackers can do more threat to cybersecurity.

As a result of the development of AI, it also has the ability to create new types of cyber threats. AI can find vulnerabilities, and by going through these vulnerabilities AI can hack into systems quicker than human attackers. AI can be used to hide attacks more effectively that one might never know that the network or device has been hacked.

Cyberattacks, divide into the most common triads of confidentiality, availability and intertwined to form three main areas.

AI Security threats

- Espionage

In terms of cybersecurity, espionage means to gain insight into the system and using the collected information for plotting more advanced attacks. As another define, and the attacker can use the AI-based engine to learn more about the internals, as an example, dataset.

- Sabotage

Disabling the functionality of a system by using AI, with requests or model modification.

- Fraud

It means misclassifying tasks by using AI, as for examples, data poisoning, which means introducing incorrect data to the learning stage machine and interacting with a system at learning or production stage.

Malicious uses of Artificial Intelligence in cybersecurity

(1) Automation of social engineering attacks

NLP tools allow imitating the writing style of the victim's contacts. Thereby, AI systems are collecting online information to automatically create malicious websites, emails and links that are likely to be clicked on by victims.

(2) Automation of vulnerability discovery

Old patterns of code vulnerabilities can help to speed up the detection of new vulnerabilities. AI can use to identify the old code patterns and to detect the new vulnerabilities. Cyber attackers can go though these vulnerabilities and access to the systems illegally.

(3) Sophisticated hacking

AI can be utilized in hacking in various ways. It can give automatic means to better target selection and prioritization, avoid from identification and do intellectually react to changes in the target's behaviour, and it can mimic behaviour similar to human behaviour pushing the target system into a low secure state

(4) Automation of service tasks in criminal cyber-offence

Using AI techniques can automate many tasks that form the attack path, as for examples payment processing or conversation with ransomware victims.

(5) Exploiting Artificial Intelligence

In information security, using AI, attackers can do data poisoning. Data poisoning attacks are used to secretly maim or create illegal access points in user machine learning models.

(6) Simulating faces and voices

An attacker can imitate voices and videos by using modern advancements in neural networks and speech synthesis.

In the past, immoral videos were created by using the faces of famous actors. They were relatively innocent jokes. But this may transmit negative effects to the society, with the advancements of technology. It may mess up the global networks of fakes in enormous scales. Secondly, it may lead to the appearance of fakes which are really difficult to recognize from the real ones. It elaborates, Politically motivated, capable of making economics or social results

A malicious chatbot could be permitted to identify the complaints of the customer online and then act as a representative of the customer service trying to rectify the event by improvements in Natural Language Processing and conversational bots.

The user may grudgingly hand over sensitive information, for instance, answers to security questions, passwords and more. This could develop into more numerous modern phishing and also spear-phishing email messages. Targeting the party, which is going to be attacked, by imitating official writing methods or also the victims special writing pattern.

(7) Artificial Intelligence - driven malware

Cybercriminals can too use Artificial Intelligence to inquire their malicious things such as malware and develop and improve it to probably become AI-driven themselves and that is another shortcoming. In point of fact, AI-driven malware can be very harmful as it can learn from exciting artificial intelligence mechanisms and improve more further advances crimes to be capable to infiltrate conventional information security applications or equivalent AI-boosted systems.

In 2016, a cybersecurity company names “Zerofox” in an experiment back, create an AI algorithm called SNARP. That algorithm has the capability to post 6.75 spear-phishing tweets per minute and that reached 800 people. Among them, 275 people clicked on that malicious link in the tweet. This algorithm has far surpassed the performance of a human, who has the ability to generate 1.075 tweets per minute. That human attacker can be reaching to only 125 people and convincing 49 persons to click.

Furthermore, a digital marketing company named “Fractl” shown how AI could unleash a tidal wave of fake news and disinformation. Using AI tools, it created a website that includes 30 very polished blog posts, and also there was an AI-generated headshot for the non-existent author of the posts. That AI tools are publishing available.

Not only that, but there is also the rampant use of deep fakes, which employ AI to match pictures and use to create videos, that in many cases are almost difficult to recognize as fake.

Researchers in compute vision are always trying to prevent attacks created to disrupt the quality of their machine learning systems. By attackers, this machine learning systems can be hacked. Third parties can identify how a machine learning system works and then introduce code that confuses the system and reasons it to misidentify images. The worst thing is there is no proper way to completely stop these attacks.

Recent Attacks

One of the most recent AI-based cyber-attack happened in 2018. The victim is TaskRabbit, which an internet marketplace for freelance labourers and their customers. That online marketplace was attacked by hackers using AI. In April 2018, 3.75 million users of the website were affected because of this AI-based attack. Their social security numbers and bank account details were scooped from their user data by hackers. Attackers did this cyber-attack by, using a large botnet controlled by an

AI which used glave machines to do a large DDOs attack on TaskRabbit's servers. The attack was such a serious that the whole site had to be deactivated until security could be restored. Unfortunately, in the meantime, an additional 141 million users also were affected. Wordpress has recently reported that its websites have come under huge botnet attacks. Over 20,000 WordPress sites had been infected with a botnet-style cyber-attack, which may ultimately allow hackers access to users' personal and sensitive information, for instance, credit card numbers. This attack broke the faith in WordPress for numerous users, even those with great hosting services.

In 2019, Instagram which is one of the most popular social media had been forced two cyber-attacks. Since in August 2019, numerous Instagram users noticed that their account information had been modified by hackers and locking them out of their social profiles. In November 2019, a bug in Instagram's system had been used to a data breach and that displayed user's passwords in the URL of their browsers. That was a massive security issue to Instagram. Instagram is failed to release detailed information about the attack, the Instagram company has guessed that hackers had used AI systems to scan Instagram user data for potential vulnerabilities.

2. Future developments in the area

Impacts of using AI for cybersecurity in future

AI us already a significant tool in cyber defence in the modern world. In the present time period, the world tends to use more cloud-based services and virtualized networks. It is becoming utterly essential to fighting cyber-attacks, with conventional prevention strategies becoming increasingly absolete.

Security vendors have created broad use of machine learning algorithms for numerous years. Today, more improvements have combined machine learning algorithms with advanced data visualisation to build smart security interfaces. By using AI to process huge amounts of information intreal-time, response times are highly decreased, while it can analyse trends and patterns to prognosticate cyber-attacks before they happen.

AI is now increasingly being used in the improvement of security immune systems. By applying the leaning of human immune system's behaviours models to the networks, can train AI system to examine various defence strategies to reduce or stop the spread of malware during a cyber-attack, controlling the infection and destroying the causes. By analysing the AI response can allow humans to develop their knowledge, understanding and preparedness against cyber-threats.

In future, as AI becomes much better, able to observe successful responses to cyber-attacks and it will also act as a self-healing system. It will dynamically recreate the best defence strategies designed by human analysts. This will allow a greater speed of responses and performance to take on more complex investigations.

In future, AI systems will be used for every cybersecurity systems and using those AI-based systems could detect malicious activities and attacks, not only that but also will block attacks and create antimalware systems. Future AI-based security systems will be more complex and will be more secure than today. AI-based cybersecurity systems performances will transcend human security expertise because of the storing knowledge to the system, in future. AI security systems will gather the power and knowledge of human expertise and it will be a super powerful tool to solve the cybersecurity problems, for instance, it will be work similarly to the human immune system. AI system will be used to protect the sensitive data and companies will reduce the employees' deployment for the cybersecurity section, in future. That is kind of a problem, however, the job market for the AI-based cybersecurity system operators will increase.

Dark side of the future

AI already has the ability to improve malware. By that, it can develop and modify to counter security defences. Machine learning is used to analyze risks in targeted networks. Using machine learning tools, attackers can detect vulnerabilities and can attack to the system.nd can attack to the system.

Artificial Intelligence will be higher intimidation to national state's level and also the military grade crucial infrastructure because AI will be available as an alternative beside more conventional techniques of cyber wars.

In the present time period, cybercriminals use AI as a cyber weapon. This weaponization will be more increase in the future because it could be easy to use AI systems to do cyber-attacks. When moving to the future AI systems will be technically more improve as well as cyber weapons also will be more improve. Future AI systems will be more intellective to do activities similar to humans. Using that ability hackers could be use AI-based systems to perform to do malicious works. In future, AI will have the ability to do works similar to humans and it will use hackers to do their malicious works. It will be more difficult to identify that they are not humans. Malware and other kind of attacks also will be improved with AI.

3. Conclusion

In the modern world using Artificial Intelligence for smart cybersecurity is an emerging topic. The today cybersecurity field is becoming more important and interesting. Cybersecurity is the protection of computer systems, networks, and hardware, software or electronic data from the theft and, prevent the damage from the digital attacks. The capability of a machine or computer system to imitate human intelligence process, learn from experiences, and to be adaptable to new information and perform activities similar to human activities are defined as artificial intelligence. Artificial intelligence in cybersecurity is advantageous because it helps security experts to analyze, study and understand cybercrimes easily.

In 1943, the first artificial intelligence system architecture was introduced. In 1990, Bayesian logic was used to sift malicious emails and, also neural networks used to categorize spam messages. When AI and cybersecurity moving forward the technology of those were more improved. As a result of the evolution of AI, organizations have opportunities to use AI for cybersecurity to develop and evolve the cybersecurity section.

Artificial intelligence use for cybersecurity in many ways. Those are to detect anomalies, to detect misuses, to data exploration and, to risk management. There are successful examples of AI in cybersecurity. Those are automation malware defence, automated phishing detection, automated data theft detection, context-aware behavioural analytics and, social engineering defence.

There is also a dark side of using AI in cybersecurity. Cybercriminals can use AI to do their attacks and harmful works. Cybercriminals can use AI to automate cyber attacks on a large scale. As a result of the development of AI, it also has the ability to create new threats to the cybersecurity section.

There are numerous malicious uses of AI in cybersecurity. Some of them are automated social engineering attacks, automation of vulnerability discovery, sophisticated hacking, automated service tasks in criminal cyber-offensive, exploiting AI, simulating faces and voices and, AI-driven malware. In 2018 & 2019 there are several AI-based cyber-attacks happened. Some of the victims are TaskRabbit marketplace and Instagram.

In future, AI systems will be used for every cybersecurity systems. AI-based systems could detect malicious activities and attacks quickly, not only that but also will block attacks and create antimalware systems. AI security systems will gather power and knowledge of human expertise and it will be a super powerful tool to solve the cybersecurity problems, for instance, it will be work similarly to the human immune system. Developing an AI system such as the human immune system for information security will be happening in future. These improvements will allow a greater speed of response and performance to take on more complex investigations.

There also be a dark side of the future of using AI in cybersecurity. In the present time period, cybercriminals use AI as a cyber weapon. When moving to the future AI systems will be intellective to do activities similar to humans. Using those ability hackers could be used AI-based systems to perform to do malicious works. It will be more difficult to identify that they are not humans.

According to that cybersecurity field must be a step ahead of that. By using and creating a more powerful tool than cyber weapons, can protect systems and mostly preventable from future attacks.

4. References

- https://www.information-age.com/ai-a-new-route-for-cyber-attacks-or-a-way-to-prevent-them-123481083/
- https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/
- https://towardsdatascience.com/cyber-security-ai-defined-explained-and-explored-79fd25c10bfa
- https://becominghuman.ai/designing-ai-solving-snake-with-evolution-f3dd6a9da867
- https://becominghuman.ai/why-you-should-use-artificial-intelligence-in-cybersecurity-204dbe33326c
- https://medium.com/sciforce/artificial-intelligence-for-cyber-security-a-double-edge-sword-6724e7a31425
- https://www.thesslstore.com/blog/artificial-intelligence-in-cyber-security-the-savior-or-enemy-of-your-business/
- https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/
- https://www.normshield.com/cyber-security-with-artificial-intelligence-in-10-question/
- https://ciostory.com/cxo-perspective/use-of-ai-in-cyber-security/
- https://www.nap.edu/read/25488/chapter/5#39
- https://www.securitymagazine.com/articles/91516-the-evolution-of-artificial-intelligence-as-a-system
- https://www.ishir.com/blog/5014/artificial-intelligence-ai-impacting-cyber-security.htm
- https://www.entrepreneur.com/article/339509
- https://www.productivecorp.com/blog/security-posture/ai-and-the-future-of-cybersecurity/
- https://hub.packtpub.com/6-artificial-intelligence-cybersecurity-tools-you-need-to-know/
- https://www.cisomag.com/hackers-using-ai/
- https://www.infoq.com/articles/ai-cyber-attacks/
- https://builtin.com/artificial-intelligence/machine-learning-cybersecurity
- https://builtin.com/artificial-intelligence
- https://www.information-age.com/adversarial-artificial-intelligence-winning-cyber-security-battle-123487325/
- https://resources.infosecinstitute.com/ai-in-cybersecurity/#gref
- https://www.zdnet.com/article/exploring-the-cutting-edge-of-ai-in-cybersecurity/
- https://www.plugandplaytechcenter.com/resources/how-artificial-intelligence-transforming-cybersecurity/
- https://www.cio.com/article/3515730/ai-automation-emerge-as-critical-tools-for-cybersecurity.html
- https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#26d73e56117e

- https://www.cio.com/article/3201147/why-ai-is-crucial-to-cyber-security.html
- https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/
- https://artplusmarketing.com/why-and-how-to-implement-ai-for-your-cybersecurity-goals-8338bc935092
- https://invidgroup.com/applying-machine-learning-and-ai-to-improve-cyber-security/
- https://builtin.com/artificial-intelligence/artificial-intelligence-cybersecurity
- https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/
- https://www.dataversity.net/brief-history-artificial-intelligence/
- https://venturebeat.com/2020/02/11/is-ai-cybersecuritys-salvation-or-its-greatest-threat/
- https://www.military.com/defensetech/2008/02/06/cyber-sabotage
- https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf
- https://www.cisomag.com/the-future-of-ai-in-cybersecurity/
- https://www.cbronline.com/opinion/the-future-of-ai-and-cybersecurity
- https://www.rapidsslonline.com/blog/artificial-intelligence-is-the-future-of-cybersecurity-and-probably-the-end-of-the-world/
- https://www.ccsinet.com/blog/what-to-expect-from-ai-and-cyber-security-roles-in-the-future/
- https://www.cybersecurityintelligence.com/blog/the-future-of-cyber-security-is-ai-4550.html
- https://www.weforum.org/agenda/2019/09/4-ways-ai-is-changing-cybersecurity-both-in-attack-and-defense/
- https://www.infosecurity-magazine.com/next-gen-infosec/ai-future-cybersecurity/
- https://analyticstraining.com/how-will-ai-impact-cyber-security-in-the-future/