Global Journal of Multidisciplinary Sciences and Arts

ISSN: 3078-2724

Volume 1: Issue 1

Cybercrime and Cybersecurity in the Age of AI: Exploring the Challenges and Opportunities Presented by ChatGPT

Noman abid

American National University USA

nomanabid12345@gmail.com

Article History

Submitted: 08-07-2024

Revised: 27-07-2024

Accepted: 01-08-2024

Corresponding Author

Noman abid

Email: nomanabid12345@gmail.com

Abstract

One of the most hopeful trends in cybersecurity specialization is the utilization of artificial intelligence (AI) in the anti-cybersecurity movement, which provides specialists with rather elaborate tools to identify, thwart, and respond to newer, and more diverse, digital threats. While AI programs compliment traditional approaches of the identification of cyber threat and other measures, the former stands advantages in the way it can pin-point future threats and act on them. Nevertheless, as the usage of AI grows so does new threats emerge; first of all, AI is hackable which means that it can be used by offenders, thus the threats are consistently evolving exist. In this work the author also described more important role of AI in cyber space for both defense and offense. The FCA has indeed eyed the regulations and governance aspect as being at the heart of the ethical AI, privacy issue and reporting. In order to avoid the situation when security is dominated by technology, and within cyberspace threats are solved cooperatively at the international level, there is an appeal to open, non-discriminatory, and constantly developing architecture. It is anticipated that new trends, such as self-managing systems, computational prognostication, self-healing models, will emerge in the sphere of cybersecurity using AI, however, it is necessary to mention that this field has to be applied at the right level due to potential unfavorable outcomes. Finally, the achievement of a synergy in artificial intelligence alongside human decision-making will create robust digital environments that this author shall use towards the safe development of the new technology alongside the fight against emergent cybercrime challenges.

Key words

AI, cybersecurity, cyber threats, Big Data, rule, policy, ethic AI, data privacy, responsibility, probabilistic approaches, autonomous system, threat, cooperation international, self-correcting system, protection, AI military, AI warfare, ethic, openness, regulation, digital.

1. Introduction

In a society where technological advancement has become the order of the day two of the most current subjects of discussion are the cyber criminals and the cyber security. Hence, these concerns have Gone to the new level due to the progress of Artificial Intelligence (AI) Technologies such as Chatgpt integrated to different fields. High level of AI in adopting the technologies of big data and digital technologies were followed by megascopic opportunities and brusque threats in the field of cyber security [1]. This article focuses on the different ways that AI in general, and generative models such as Chatgpt, threatens cybercrime and cybersecurity and the advantages it opens up in fighting those threats. It has progressed from simple crimes such as hacking, identity theft to the sophisticated and more complex crimes such as cyber espionage, ransom ware attacks, which are possibly to be carried out by intelligent bots, AI integrated frauds etc. Since every aspect of human life has been included in the use of digital systems, persons and entities have been vulnerable to cyber threats. This means that the cybercriminals are now employing technologies such as artificial intelligence to step up, escalate and boost the rate of their cyber threats. For example, AI do a very well there in executing designing phishing attacks or even developing new strong fake accounts to target innocent persons.

On the other hand, cybersecurity has now become a key element in the battle against the growing threat incidence in the digital environment. Till date information security techniques have been based on strategies such as fire walls, anti-virus programs, encryption techniques among others. However, since the threats are more complex and diverse, the security professionals are using artificial intelligence (AI) and ML [2]. With velocity, AI, can improve threat identification or response to cyber threats in the areas of threat identification and analysis. Both, cybercrime and cybersecurity have the potential to be introduced to the use of artificial intelligence – or more specifically – generative AI, such as Chatgpt. This is so because in the field of cybercrime, these AI tools can also be used by the attackers for various unpleasant work such as creation of disturbing messages for phishing, clones of identity and many other frauds. Since with the help of AI certain complicated calculations can be executed within the shortest time and exceptional accuracy, cyber criminals are especially interested in using AI as a tool for attacking vulnerabilities in the life of people. However, instances like the generative AI models, such as the Chatgpt, make it possible for new fake messages to be created almost in the actual message's likeness meaning that there is high likelihood that among all the messages which the user receives some of them are fake [3].

In the same perspective, cybersecurity has assigned the same significance to Ai. AI is also useful for constructing and training behaviors and patterns in networks and for risk identification and further threat development. Such patterns could be dangerous – and algorithms can spot them in big data; prescriptive-analytics models could be used to generate automatic responses to the aforementioned tactics. It will also make it possible for tools like Chatgpt in cybersecurity for instance to assist the security teams in writing incident reports, briefing stakeholders, or indeed offering bespoke customer relations during a breakthrough. However, there exists a catch when it comes to the transactions that relate to cybercrime, cyber security as well as Artificial intelligence. But luckily or unluckily the same resources that are available to the AI system to enhance security are available to the hackers therefore cybersecurity is more of offence technology rather than a defense technology [4]. In this way, the application of AI in both attackers and defenders of cybersecurity appears periodically as opportunities and threats in an arms race. For this, the future emergence of new AI technologies like but not limited to the Chatgpt remains a ground upon which its consequences on cybersecurity and potential cybercrimes can be understood. For these technologies, the potential is nearly limitless when it comes to digital security, which has many flaws when cheaters seek to take advantage of it. Thus, in this article, we stated our intent to depth discuss how advanced AI tool impact the world of cyber criminals, the opportunities for the cybersecurity business regarding the studied AI tool, and the challenges regard to the application of this tool.

2. Cybercrime: Source, consequence and learning from computerized society

The computer crime becomes much more sophisticated due to the technical appearance of new categorizing technologies in the contemporary environment. Considering the traditional definitions of cybercrime we might regard it as a direct translation of the traditional crime with the only tool being the computer/internet –mainly identity theft/hacking. Nevertheless, by exploiting modern technology devices that use AI ability to manipulate cyber criminals are able to go further deeper invasion knowing fully well that the warfare against cybercrime is on the increase and desperation [5].

Types of Cybercrime: From Phishing to Ransom ware

However, a wider view of cybercrime relates to crime that includes the application of technology in the commission of those crimes. Some of the most common forms of cybercrime include:

Phishing: This include cases whereby an email or a message containing an imitation of a genuine looking company, organization or individual with the intention of defrauding the targets into providing for them their passwords or credit card numbers [6].

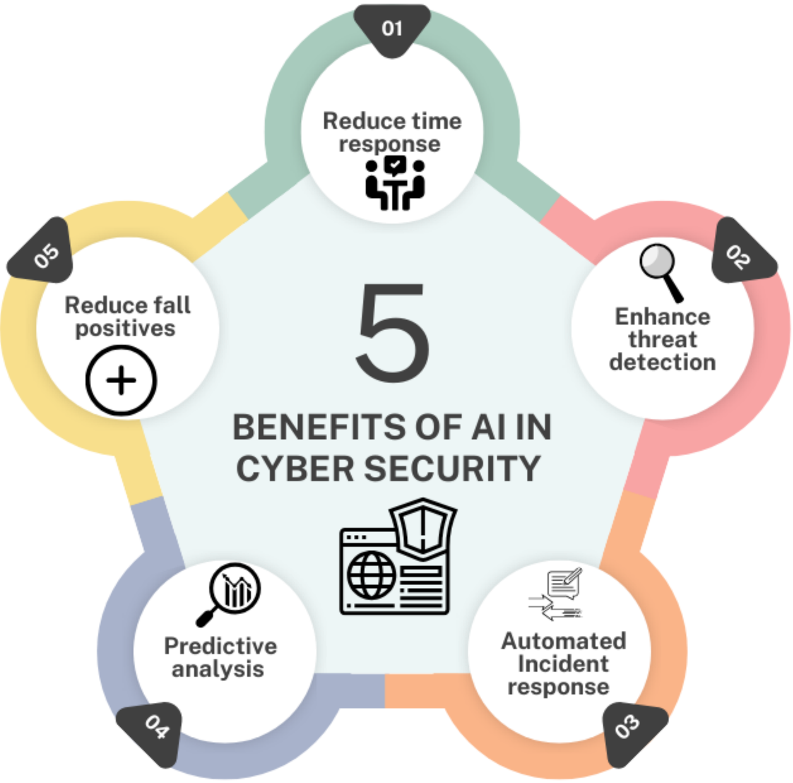

Figure: 1 showing benefits of AI in cybersecurity

Ransom ware: This is type of attack where the criminal encrypts a victim's files or an entire system, and then requires the victim to pays certain amount of money, preferably through bit coins, to un-encrypt the files. Ransom ware is considered to be one of the most active and aggressive sort of malware kind, which threatens absolutely everyone, from ordinary users to corporations and governments. Ransom ware attacks have recently become harder for organizations to prevent in the following ways advanced artificial intelligence algorithm program for encryption and decryption of data [7].

Data Breaches and Identity Theft: They also 'steal' databases and take away such other tangible and tangible properties as identity information, social security numbers, credit cards, user-ids and passwords etc. Then they have been used for a rather more evil intent or to make some green, reselling them in the latter black market place in black website [8].

Distributed Denial of Service (DDoS) Attacks: DDoS is a short form of Distributed Denial of Service from the intention of the attacker that the particular computer is hesitant to perform its function due to internet traffic. It has lately become very common to have such attacks Very often the attacker uses a botnet for launching these attacks.

AI-Powered Attacks: However, due to advanced technological sophistication of AI solutions and tools, so is the AI's utilization in cybercrime. AI can be used for such purposes as, let's say, searching for the weakness in great databases, writing a pretty believable phishing letter or even mimicking someone's writing to perform a fraud. Technology, the application of deep learning on humongous amounts of data to produce answers that are as natural as any human being does scale the size and efficiency of these crimes even more. As the threat actors are becoming more organized, the sophistication of cyber criminality is growing too. In general, new attacks can be caught or prevented by standard security technologies such as firewalls and antispyware software [9]. Marketers have been using AI and ML in advertising to create more sophisticated malware than it is possible for antimalware solutions to see and prevent since they adjust as per the environment in which they exist. The advancement in artificial technology has offered better aid in the implementation of large scale damaging attacks to persons and persons group.

Another a important component of the contemporary cyberspace criminal environment is the so-called as-a-Service model of delivery of cybercriminal tools. This means in deed that even an ordinary person with no any special engineer technological knowledge does not need to have any hacking skill in order to practice cybercrimes. Yet another hurdle to the police effectively combating digital crime is that the dark markets available to the criminals make it easier for them to access these resources. In the context of cybercrime AI has a two-fold role. In other words, it may become the tool that some hackers will employ to advance their endeavors, while at the same time, it is the gold mine of intelligence and knowledge for the ones who stay abreast of cyber threats every single day [10].

The most important is that AI and Big data can have much capability impact data processing, patterns, and decisions much faster than human on offense and defense for CyberOps. To hackers and cyber criminals AI helps in a number of ways – it can automate some of the processes that might be used in phishing, identity theft or perhaps avoiding detection, or even scraping data from sites. Favourable for the cybersecurity professional, these applications of AI are in the identification of threats, the assessment of vulnerability prospects as well as an efficient response to emerging threats. However, seeing the simple truth of the ongoing arms race attackers vs. defenders any addition of technology to the side of the attackers is inevitably followed by similar innovations on the defenders' side when it comes to AI, the advancement of cybercrime in the digital age has been immense [11]. racing in their spectrum from frauds that even IT laymen can perform up to state cyber-terrorism along with hacking the systems of technologically advanced states, during the recent years, the cyber criminals have been seeking new opportunities in the cyber space with rather diverse and constantly growing level of complexity. Now that hackers are employing newer technologies including AI in their operations, the larger cybersecurity community is in a desperate need of formulating better ways of shielding against these threats. To achieve better protected environment one has to understand how various hackers act in modern society and what is their connection with AI-operating systems [12].

3. Cybersecurity as the Method of Protection of Digital Assets

Amid the framework of interaction globalization, cybersecurity can be considered as the critical component of the support of information, its confidentiality, integrity, and availability. As such, because cyber gangs operating are becoming more professional, the need to guard against cybercrime becomes more urgent. Cyber security defines the protection offer to computer, communication networks, software, data and information against harm, loss or misuse. Such measures may be required not only for safeguarding of information but also to provide the continued operation of commercial entities, governments, and people in informational society. The previous strategies towards cybersecurity were just basic techniques such as firewalls, antivirus, IDS, and even encryption among others [13]. These technologies have been used right from the front line to counter cyber security threats. Firewalls control and manage the traffic to the network while antivirus are used in detecting and deleting viruses. Firewalls are used to identify intrusion in a network and correlation to information attacks and invasion; intrusion detection systems help in drawing attention to break-ins in a network; encryption is the process of making data difficult for unauthorized users to access the information exclusive to the users.

While these techniques may be somewhat effective to some degree, these techniques have many disadvantages or weaknesses; these techniques are not designed to confront the current sophisticated cyber threats. The current hackers are fully aware of the tricks used in check and balance, they engage in phishing, social engineering and APT to have a free access to company's systems. Also, main tools are rather ineffective in case of combating a great number of attacks that take place with a high speed when more and more hackers employ AI and ML to their practice. This has made it necessitate that security solutions which are protective in nature are to be developed to meet these emerging threats [14]. AI and automation are also being subscribed to in cybersecurity every day because it is a discipline that works with these threats, which escalate yearly. AI defense is employed to alarm a threat, to identify threats in practice, for monitoring huge data, as well as to foresee probable threats in advance. This change in the society's adoption of artificial intelligence to counter cybercrime is helping organizations to stay a step ahead of the criminals. Of all the above enumerated AI techniques, only machine learning presents a proper way towards such change.

One can build special purpose algorithms from large databases like traffic patterns, user's behavior and so on, and once trained, is able to identify those that are likely to be malicious. Traditional paradigmatic approaches of rule-based decision-making techniques offer just answers to current and known threat and are incapable of working on new unidentified threat whereas the machine learning systems can. Some of them are EDR that works mainly for such unnoticed threats such as zero day or APT or for which other solutions that utilize a database of signatures cannot identify. Another improvement claimed is a broader and more extensive threat identification and combating, the chief improvement made in cybersecurity is automation [15]. Automate also facilitates easy grouping of all security incidences and how to handle them which entails; this removes a certain device, block this IP address, notify this person. In the case of cyber attackers, automation of containments aids in raising the rate of response on episodes of cyber-attacks and therefore minimizes the effects on organizations. It can also be used to avoid spending time on mechanical work such as patching one's vulnerability in order that the professional can deal with complicated ones.

First of all, it has been possible for several organizations and government parties to incorporate artificial intelligence features in cybersecurity programs. For example; google and all this technology industries are in intelligence and machine learning to fight billion spam e-mails and cyber-attack daily . Equally so, AI and automation is useful in that governments across the globe are involved in measures to protect their organizations and institutions from cybercriminals. Today, in cyber security, DHS is attempting to create information sharing systems among various organizations and businesses, and the government [16].

One example to look at here is the Threat Intelligence Platforms that can support the integration of massive datasets, analysis of that data for patterns, as well distribution of intelligence on information accrued from multiple sources in real time fashion. These platforms can notify the cybersecurity teams about the new threats; threats that may be out there and; there are some which are open need attention since they need to be patched. What is more, some of these systems can work autonomously in reaction to a frequent attack and their removal makes it impossible to transform attacks into massive ones. Therefore, there are many pros of Using AI and machine learning in cybersecurity, as well as some challenges brought by AI machine learning in cybersecurity. That is why protective systems have to be replenished for new threats that is being developed almost every day [17]. In addition, the systems that use AI are not the ones that cannot be attacked, moreover, it can be easily penetrate. In recent cybersecurity, Adversarial AI appeared as a future threat that builds methods to deceive AI models in order to remain unnoticed. However, any time AI is integrated into security systems, it must be important that such weapons can in fact be defended against such influence.

However, introducing artificial intelligence into the cybersecurity utility is another question that causes concerns about overloading coupled with ethical concerns and privacy as well. As AI systems depend on quantity of data in learning as well as threat detection, one starts to wonder how the data was gathered, where is it stored and how is it processed. We have to ensure that norms and guidelines of data privacy rules including GD PR in the European Regulation are followed whenever customer's data comes into picture. Security is highly valued in today's world which is packed with more and new threats that are present today. Comprehensive AI is emerging rapidly as a powerful addition to the traditional layers of protection as the AI solutions have the variety in mobility and counteraction to threats. However, as with any threat in the cyberspace domain, so also does the method and tools by which we seek to counter such threats. AI and atomization in cybersecurity is not a mixed blessing because while facing hackers, organizations must protect privacy, ethic, and laws [18].

4. Chatgpt and what it will be to Cybercriminals

New AI language models, notably Chatgpt and others of high impact have revolutionarily changed the Look &Feel of Cybercriminals and Cybersecurity. Where generative AI tools created new opportunities by generating text that was fairly realistic and indistinguishable from manually created content they also created new avenues of AI abuse by cyber criminals New that the risks

They also came up with new ways to manage the risks. This means is that for anyone to understand the extent to which AI/ congratulate the field cybersecurity there is no way he or she can discount either the possibility of helpful tools like Chatgpt or their capacity to cause massive harm. For perhaps more hazardous is the assurance that the spelling its display affords one leaves one able to transcribe phonetic text that would sound reasonable [19]. This feature may be useful in relation to all sorts of cyber threats and activities of cybercriminals. The biggest risk is associated with social engineering attacks where the attack messages are created by the AI to make the recipient reveal his or her identity and other details or vice-versa be told certain actions to take that are fatal to his/her security.

Phishing: Chatgpt is not the opponent of the cybercriminals and can help to improve more convincingly fabulous phishing mail or message. These messages may appear to come from a business partner, or any organization of any kind, through which a predator is trying to reach an intended target's information. Chatgpt also has the capability of forging comforting and convincing messages because of the kind of messages that the artificial intelligence is designed to generate, in addition to simple text posting regarding a target's identity, for instance using name, interests, connections or job of the target [20].

Impersonation and Scams: The elaborate scams exist since utilizing Chatgpt, a hacker can pose as the boss, a coworker or a family member. For example the attacker would be in a position to develop two text message conversion, which from the glance of it, appears to be from a close acquaintance, hence the victim parts with his or her money, accounts or information.

Automated Content Generation for Fraudulent Websites: In an as an instance of chatgpt, would be to post content in scam websites such as fake job offers, fake investment scams, or fake shops online. It also opens the avenue whereby such sites can con an innocent person under the pretext of enabling them unleash more of their cash sensitive information or they engage in transactions in fake web spaces which will badly defraud the participants [21]. It is analyzed under a trend of using the AI tools at a broader level in order to optimize and rationalizing the cyber threats where the major part of the tasks will be carried out by AI tools with majority of the functions would require manpower otherwise. For example:

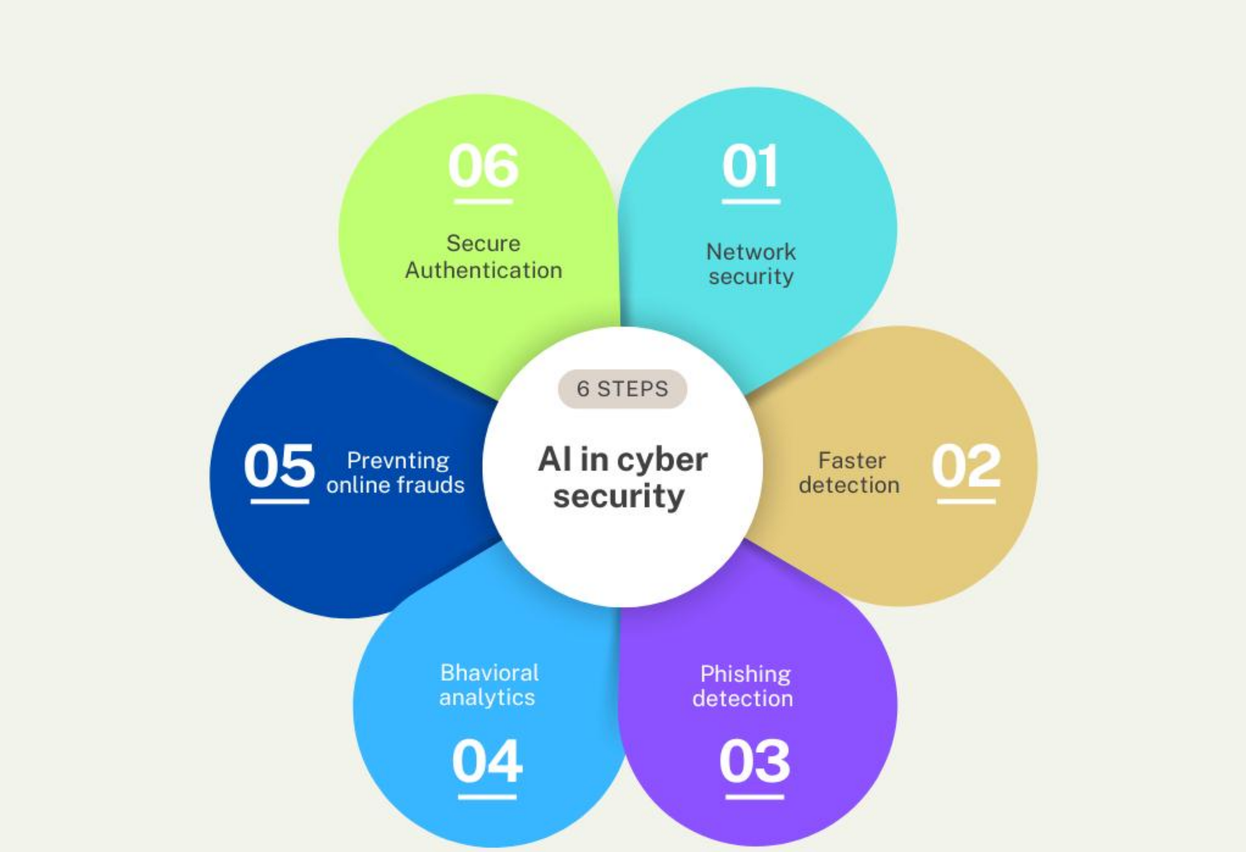

Figure: 2 showing steps of ai in cybersecurity

Social Engineering: It is also used in mimicking natural language and makes attacker's more informed in social engineering. Incredibly, you can understand just how one can write even better messages to even manipulate Chatgpt of it: Since relatively much is known about the psychological characteristics of the communication process, AI can adjust its words and intonation, which will strengthen its effectiveness in persuading—regarding the instances of detecting and preventing such phenomena, however [22].

Phishing on a Larger Scale: As this paper will also demonstrate, the above damage entails the capability of developing millions of phishing mails for various people, all through artificial intelligence. Worse still, with the help of NLG Chatgpt, the attacks herein can be repeated and Even unnoticed given that the majority of spam filters work in such a manner that they detect this many phishing attempts.

Deep fake Technology: Thus while Chatgpt when used together with voice and image generator technologies can be used in the making of deep fakes this being forged audio or video of a real individual purporting to make or do something they never did. To the cyber criminals, deep fakes is more useful because they can post a statement, create an impersonation of reliable individuals and then con. This means that in the case of generative AI models and HOWTOs such as Chatgpt, the level of complexity of a given attack is expected to go down or in other words the amount of real content which is technical will be required in a given attack will be very low [23]. These models also bring the capability of cybercrime to the people, and to make it easier, they bring it to the bots. Despite the fact that there are real life scenarios for each of the posts each present the chance for a more sinister form of fraud that may be out of the reach of traditional methods of anti-cybercrime.

Having entrusted the given scenario for its ability to analyses as well as process a large quantity and quality of information as an experimental system; then it can be deduced that this very system can be used by cyber criminals for different complex reconnaissance tasks. From social networking sites, company's website among other source of information available in the real public domain it is mostly possible to get very detailed information of an individual or an organization on which these attacks might be launched on. Such a technique is much different from other generic scams that are simply placing probability of the scams success to the side of the cybercriminals. Now they are available without charges and the options like Chatgpt are of deep concern to cybersecurity personnel – There are measures that must be taken to prevent the use of such free modules [24]. One of the potential solutions are development and strengthening of the AI defense measures which would detect and inform on the content originated by AI and thus potentially malicious such as emails, deepfakes and identity thefts. For example, while cybersecurity products may be built to answer the questions of writing and the tone of the conversation, those products are searching for files with indications that the files were written and not by a human being.

Nevertheless, there is still a deficiency of awareness and training headed against AI-oriented cybercrimes. The user has to be trained to search something, which he/she should not type on the screen, not to answer to a message which has appeared from nowhere, and to follow at least the rules ABC for safety which as for example a request of different sources for personal data. People are going to need to be told about new threats which have appeared because of the advanced artificial intelligence [25]. While application possibilities of Chatgpt and other artificial intelligence based software may be growing by several orders of magnitude the degree of cybersecurity, new opportunities are opening up for cybercriminals to penetrate digital systems. While AI increases and diversifies the rates and sizes of cyber-attacks, it at the same time makes them simpler and VIOLENTLY dangerous. In the long run, the sign *k is larger for AI than for L; ‘It will be? Something’ to have technology walls, or, at least, positive AI risk management strategies.” cybercrime.

5. AI-Powered Cybersecurity: Enhancing Defense Mechanisms

The advancement in threats by hackers has, therefore, seen an addition of artificial intelligence technologies in cyber defense. The antivirus or firewalls that have been installed are rarely sufficient because threats are being created at a very high rate. Moreover, current innovation in the area expands abilities beyond conventional methodologies for identifying, avoiding, and managing cyber risks, including Machine Learning (ML) and Deep Learning (DL). AI is now becoming that revolution that cybersecurity specialists need to help them protect the digital assets from the impressionism of cybercriminals [26]. I’ve witnessed that AI is incredibly valuable in the protection space to quantify threats and stop them from ever happening in the first place. The legacy Security models are for their part endowed or rearmed with a set of/rule to identify an attack and then to regulate it. Although, these approaches are ineffective particularly when used to address newer forms of threat that may not have been previously experienced. Particularly, machine learning can weed through these mountains of data and locate some sort of anomaly that might have gone unnoticed to some extent.

Anomaly Detection: By this it means that normal throughput traffic patterns can be taught to the so called machine learning algorithms from previous experience. Such models once trained, can notify the system of anomalies for instance late night log-ins, or high data traffic that may indicate an intrusion [27]. AI can also learn normal behavior broadly over time, and boost the surveillance value of a system as the architecture expands.

Real-Time Threat Detection: AI can assess the information presented in the process and provides an on-the-fly impression of the threat conditions prevailing in the surroundings. This is crucial coming to terms with the fact that a Cyber-attack can occur in as much as a few seconds, hence the urgent action to be taken. For example, Intelligent Network Intrusion Detection Systems (IDS) allow machines to monitor the traffic of a network and once an unusual pattern of a possible threat is detected the cyber security team is notified.

Predictive Capabilities: The probability of enormous data solution expresses identification of risks that can be activated predicting future dangers based on past occurrences. AI can, for instance, block a cyber-attack or a malware outbreak, for example by closing down sources of prohibited traffic or isolating infected nodes when these early symptoms are noted. However, beyond a detection and prediction perspective, AI is also changing how cybersecurity is conducted given that many a mundane task have been automated [28]. They have a pile of notifications most of which are valid, but most of which are just noise or potentially a very low risk. Organizations require triage automation to allow these specialists to focus more on critical incidents out of the information overload that is characteristic of the digital age.

Automated Incident Response: AI can be programmed to act on the threats at the occurrence, it can be programmed to do things like: unplug any device that is infected, ban any certain IP or initiate system recovery. This means that there is a short time lapse between the time an attack is detected and the time it is prevented as well as the time it has a low impact [29].

Security Orchestration: Technologies established under the AI concepts can automatically and smoothly connect with other security instruments to optimize the management of different incidents at various systems. For example, in case an attack is detected in one of its systems, AI does notify the other connected systems to take specific measures that will assist in preventing through the attack [30].

Threat Intelligence Sharing: It can then pull effectively the threat intelligence from blogs twitted and other cyberspace and other platforms to produce threat intelligence data in real time. It means that this data could be shared randomly among all the organizations contributing to the strengthening of various organizations' defense measures and increasing the world awareness of threats. Gaining control and identification of unauthorized actions is the second of the most effective AI approach to cybersecurity, which is behavioral analysis. Traditional security measures are bias toward phenomenon, for example viruses, malwares like and others [31]. However, a style that is used in today's threats that a even more sophisticated and termed as an advanced persistent threat does not cause these alerts as it is not a direct attack. Compared to other security solutions AI can assess user and system performance over time of behaviors though they themselves do not pose the threat on own but are capable of being trained toward familiarity or pattern concerning a malicious activity.

For instance; take an audit of the login points the clients used, the machines that were most probably engaged or the data applied to establish that there is an irony of cross activity that could point to the compromise of malicious insiders. This approach of scanning serves as a method of identifying an attack which may not be detected by the normal scanning procedure using signatures. It again plays a larger role in security automation; this reduces human errors and improves organization's function. AI systems can be employed to help provide first-level support to security teams, including: urgent fixing and patching as well as firewall installation and risk scanning. All these tasks, when solved through technology, free considerable time that cybersecurity professionals spend on trivialities enabling them to be more effective if called upon to resolve security challenges or even make decisions [32].

Automated Vulnerability Management: While SIEM is less effective is in its capacity to self-teach on system setting-up to discover fresh vulnerability pertinent for attention; or to self-govern the process of applying patching with a view to mitigating security risks across the network. This reduces the occasions for penetration by taking advantage of existing vulnerabilities [33].

Automated Compliance Monitoring: Many firms and businesses encounter high levels of requirements set by different data privacy and protection laws such as the GDPR and HIPAA standards. What AI can do is to support ongoing security management and generate reports that can be beneficial to evaluate compliance with certain norms. However, when it comes to employ Artificial Intelligence in cybersecurity, which as we have s humans have revealed many problems, have some of the difficulties below revealed as well. Among these threats, these are cyber threats and adversarial threats to AI systems [34]. Likewise, AI is also flexible in honing the security threats, and other more menacing cyber threats are now being created using machine learning to get past the AI security measures. For example, one of the possible actions that the attacker might take in relation to the application of the AI models we discussed above is to feed the model with specific and/or rather distorted data, and then the model would make wrong decisions.

First of all, and most importantly, application of technologies based on artificial intelligence in the sphere of cybersecurity raises a number of issues connected with the protection of data and their processing. AI systems indeed use big data but in the process they require data including at times personal data. For this reason, it is essential that data protection applies to AI and that the latter must justify the conclusions made by the AI-based tool. In recent years, feelings are growing that artificial intelligence is very effective in protecting against threats in the field of cybersecurity [35]. This paper is going to outline some of how AI is aiding in threat detection, response actions and in overall cyber security effectiveness against malicious users for organizations. However, for AI, there are new problems for discussion, including adversarial attacks and ethical issues. The cybersecurity industry will have to follow the AI advancement and ensure that new technologies are utilized correctly in the defense of digital resources.

6. A future review on the use of artificial intelligence in the combat of cybercrime

AI helps in cybersecurity both in the developments in the product and services and in the innovations that the protection problem faces on the sides of the attackers and defense. This implies that even as the techniques in use by such hackers get better and better, AI is emerging as the solution to cybercrime. But here AI presents several problems for future concept of operations; remembering that AI is a two edged sword where AI can be used by both the enemy and the defender. From the analysis of the results, certain factors may be identified to forecast future developments of applying AI to the problem: the enhancement and development of the AI application, the integration of the current AI with the models of cyber security as well as ethic and legal aspects regarding the usage of the artificial intelligence system. At the core, what it means is that the capability of the same in enhancing the cybersecurity is enhancing with the improving AI technology [36]. Future AI system are independent and the much can be expected from them in future as they may require intervention from man on threats that may emerge in future. Several advancements are already on the horizon:

Advanced Machine Learning Models: When the techniques such as ML have evolved, the AI will further classify new as well as complex and improved forms of analyzing the big data set that help in increasing the rate and efficiency of threat detection. This will allow those who design architectures of security systems to give the risks of zero-day or hitherto unplanned for catastrophes before they occur [37].

Self-Healing Systems: AI in near future, have applicability in developing self-protecting system which will identify the flaw on their own and combat against feared virus in similar way. For instance, the following reasons may be had: maybe AI is able to handle the threats separately from people’s intervention and can remove or neutralize suspected viruses or threats fast, or just isolate the threats that were identified, reduce the extent of the blow from attacks.

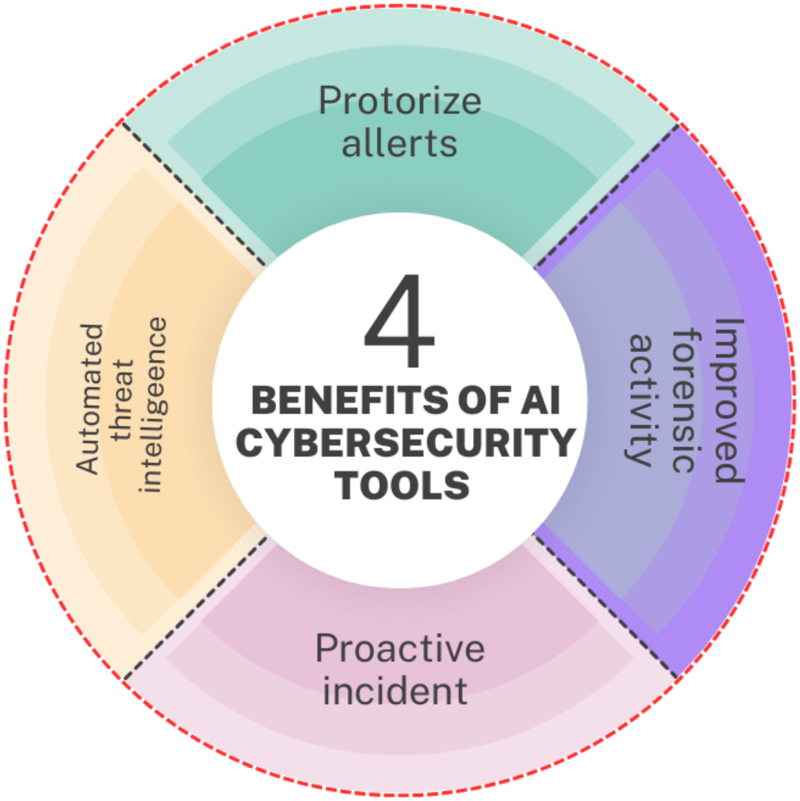
Protorize allerts
Improved forensic activity
Proactive incident
Automated threat intelligeence
4
BENEFITS OF AI CYBERSECURITY TOOLS

Figure: 3 showing benefits of AI in cybersecurity tools

Autonomous Response Systems: Sub terrorists will become more independent to conduct their attacks because self-developing AI control platforms will go on enhancing their capability in addressing cyber events. Some of these systems could not only detect threats and perform the analysis, but could also immediately and autonomously respond to it, for example, isolate a sick system, stop suspicious traffic, or install temporary protection measures before contacting the security staff. Nevertheless, this fast reaction could minimize the impacts of the cyber threats. One more segment, where AI will be most suitable against the cyber crooks, is in predictive analysis and threat intelligence [38]. The use of historical data analysis in AI systems will be beneficial when presenting patterns which help in the ability to predict future cyber-attacks. These measures will eliminate exposure of organizations to various risks before they occur due to planning. AI in Threat Intelligence Sharing: AI could assist in the dissemination of threat intelligence and in almost real-time, not only between organizations but Governments and Industries. Thus, the tire threshing and analyzing of threat data can be useful when it comes to providing information on the TTPs of the attackers to AI. This means that collective defense shall be raised and overall capacity to identify the threats in the world shall increase.

Proactive Threat Hunting: Thanks to AI, cybersecurity specialists will be able to step up the activity of threat hunting even more. With this, unlike conventional methods in which a system must await an alert, AI is capable of scouring the network, systems, and data for guilt. It also means that AI systems can simply become more intelligent and can make assessments on how effective the newly emerging threats are, within the context of the identified pattern and behavior of the threats. But if and when cyber criminals get to the next level of AI applications than is currently seen then strong AI applications will become the only way. New generation of AI models themselves will have to develop with the plan and strategy that was intended while creating the generative AI tools, Machine Learning, automated attacks etc [39].

AI Against Adversarial Attacks: Being one of the new emerging perils, risks to the AI systems consist of adversarial attacks. In adversarial attacks, these cyber criminals modify input data fed to the AI algorithms in a wrong way which makes the machine learning show its weak link. In response, researchers are encouraging the researchers the emergence of new algorithms with higher levels of resistance against adversarial manipulation [40]. Most importantly, future security systems using AI must have some type of security no matter the kind of attack.

AI for Deep fake Detection: Deep fake technology will make a larger role of identification of the manipulated images and videos, and this will be done by the help of AI. AI can be taught to identify these differences of the audio, video and image manipulation so as to stop deep fakes from being used in social engineering and identity theft and fake news. Automated Security Audits and Penetration Testing: AI could be vital for automation of penetration tests and security audits because their implication surely has a positive impact on the result. AI can help business organizations pinpoint and map out what needs to be done when it comes to the failure points of their IT applications and networks by simulating actual-style cyber-attacks [41]. This will improve security features and will also ensure that an organization’s systems are always under review for threats. Several ethical and privacy issues can be pointed out following the analysis of this innovative technology in cybersecurity as follows. While AI can significantly enhance security efforts, its deployment must be handled carefully to prevent misuse and protect individual privacy:

Privacy Issues with AI: AI-based cybersecurity at some point may require analyzing a lot of data, and most of this data are likely to be personal or business data. Something that you should ensure is that those AI tools are conformant with privacy laws (For instance, GDPR or CCPA). Another risk is that AI will be used to infringe on people's rights as concerning to privacy since they can spy on their users or take their information with their approval. Bias and Fairness in AI: AI systems are never exempt from bias that influences the choices made by any other machine learning system. In cybersecurity, for instance, could be realized where a specific set of users or a specific behavior is marked as suspicious solely because it is linked to a particular data set [42]. It can also be noted that it is crucial to encourage the fairness of the models & the AI implementation for the good functioning of cybersecurity Applications.

Regulation of AI in Cybersecurity: Because the technology that has boosted the use of AI will be established by the governments and other regulatory bodies, guidelines on how the technology is to be used for cybersecurity will also have to be formulated. Sub-topstrate recommendations thus include strategies for proper use of AI in design and implementation, in which proactive addressing of security concerns could be initiated without negating the freedom of citizens or intrusion of their privacy. To the surprise of many, artificial intelligence is going to be one of the most important tools used to protect our systems in the future, but it won't put the people working in the field of cybersecurity out of business. At the same time, AI will enrich the field of practice of the expert, providing repulsive services for carrying out time-consuming traditional operations and timely and accurate data analysis and decision-making support [43]. The future of AI in cybersecurity will include people AI and cybersecurity personnel, who are going to sit down to figure out more effective ways of handling cybersecurity risks live.

AI is somewhat promising since it will uncover it amid a set of opportunities and threats to curb future cyber threats. It will, in due course, become useful in the improvement of the AI elements within an organization, allow the cybersecurity specialists to deal with harder threats as and when they appear, all in the most efficient way possible. But, and it is a big but, any such advances should be achieved with due regard to good ethical practices, privacy as well as the security… It is clear that the future of cybersecurity relies on best methodologies and use of artificial intelligence along with its human counterparts in order to develop new efficient and effective approaches to dealing with increased threat posed by cyber criminals [44].

7. The AI employment and utilization in Cyberspace Security: Rules and Management

AI application for cybersecurity advances essential novelties in the technology used to identify the threats, to avoid them and counter them effectively. That is why as deep AI algorithms become even more important for security measures, there is a need to step up the elaboration of new compounded legislation, and functioning and facilitating rules. Potential risks associated with misuse or lack of adequate control to artificial intelligence are; infringement on privacy, discrimination, and actually the usage of artificial intelligence for ill purposes. Therefore, if AI in cybersecurity has to be efficient and reliable, its design, deployment and application cannot be bereft of well stipulated legal frameworks [45]. Indeed, the move towards AI adoption in the cybersecurity field has been quite fast and questions about liability, transparency, and governance emerge from it. As AI models can make decisions autonomously and without human supervision, and as AI models can change security parameters, such levies of how these systems should perform have to be created.

Data Privacy and Security: AI systems incorporate much input data and can frequently apply the personal or organizational data of the subject. Policies like the GDPR or the CCPA for that matter are already around the corner for how the personal data should be processed. However, as these AI solutions become usual canvass in all aspects of people’s lives, there is a need for radical legislative amendments covering AI risks, such as data bias, decision-making algorithms, and consent [46].

Accountability for AI Decisions: We run into an issue of responsibility, or lack thereof, because the autonomy of AI systems makes it almost impossible to pin the blame for certain actions on these systems. If an AI system misclassifies a threat or drops a legitimate connection or misses a cyber-attack, someone has to be held responsible for that. At present, particular rules should establish legal responsibility for artificial intelligence to ensure that any person or legal entity who uses AI for the purpose of cybersecurity adhered to a particular line of action. AI systems should be designed respecting certain important ethical variables and in particular the system should have a certain degree of openness [47]. Possible solutions are provided at the disposal of organizations to ensure that the deployed AI systems act in a ethical manner as well as meet organizational needs. Some key areas of focus in AI governance include:

Bias and Fairness: So, as data is fed to an AI algorithm, and in case the data is bias, then the model derived from the same, would be bias too. This is even more worrisome in the area of cybersecurity for example unfair decisions may have damaging consequences to individuals or groups of people. To make regulation fair some regulation may assert that unlike data other data has to be used while training AI and also on how corrections for biases in the AI models were done [48].

Transparency in AI Decision-Making: Therefore, this paper stresses that decision making in AI systems for cybersecurity should be made transparent. Hard law has to specify that explainable artificial intelligence in systems has to provide the capability for people to make rational decisions about an AI's actions. This is especially so where the AI system is operating in the real time – say diagnosing and filtering out cyber threats [49].

Ethical AI Usage: Employment of the AI technologies must respect to the human and privacy rights of individuals; any technology with rights must be designed in compliance with the privileges set. Ethical consideration should therefore be part of the equation with the envelopes to contain basic guidance on the right development of the AI model for securing the citizen's security and rights. To this end, it should be mandatory for organizations to adhere to high standard of ethics to prevent evil use of Artificial Intelligence including monitoring or monitoring of the end users. Cybersecurity through Artificial Intelligence is a global issue and tackling this issues need cooperation at the international level [50]. As the majority of the cases are general, the cyber criminals exploit the legal jurisdictions available. To this end, there is the necessity to pact together with the intention of coming up with simultaneous regulations that would provide protection in nations.

Global Standards for AI in Cybersecurity: For example, ISO and IEEE, there is motion to develop the international standards for AI technologies. Such standards can advise on how AI can be both, designed and implemented in an ethically sound manner in relation to the context of cybersecurity, and can ensure that countries use similar policies.

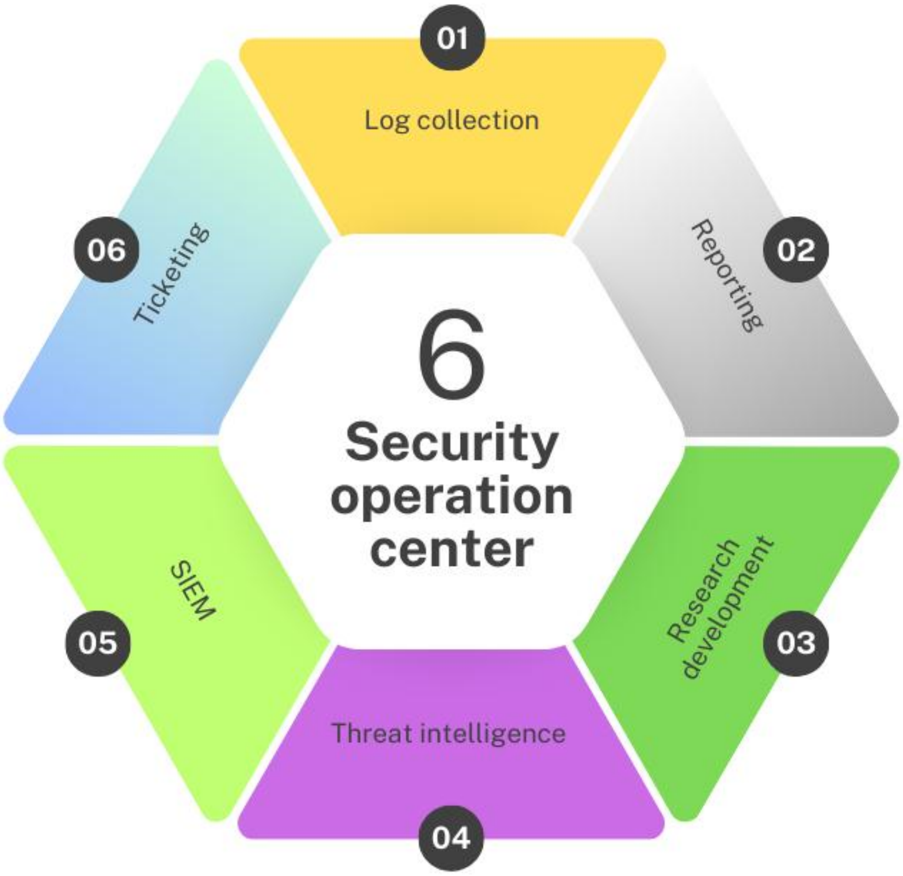

Figure: 4 showing security operation center

Cross-Border Data Flows and Cooperation: As cyberspace threats target organizations and companies globally, exchanges of data and cyber Threat Intelligence are also required. These treaties ought to allow the flow of data across the borders for the purposes of being used by AI while at the same time conform to the privacy laws and hence allow AI to work across countries without infringing on people’s rights. It is also possible to pose such a question that poses the very problem of AI governance – cyberspace, into which AI can be applied to aggressive activities. The same way it is much easier and probable to use AI to attack or even compromise other systems. The opponents such as terrorists, cyber criminals or even certain states would use AI to create qualitatively new, more complete and elaborated cyber operations starting from using AI to generate malware using deep Fake or AI-based hacking infrastructure [51]. It must be foregrounded what kind of the AI utilization and its use in the cybersecurity field is considered ethical and what kind of AI utilization and its use in the cybersecurity is allowed to weaponries AI technology. Maybe, there is a way multilateral treaties and conventions might help in regulating the utilization of AI for warfare or cyber spying to make sure that AI driven cyber aggressiveness will not reach the genereal war or backlash existing international laws. And the dilemma for the regulators will still be the question of how to develop the growth of AI while maintaining security. It is always dangerous when government pay extra attention to over-regulate AI as are does it a disservice in curtailing innovation; few organizations could scale up to use new technologies strengthen their prowess. Too little or no regulation on the other hand can be dangerous for the various AI systems we interphase in day to day life since some might be $('#'||“)misused”$('#’||‘)” or they may not comply with the best ethical standards of civilization.

Agile Regulatory Frameworks: It is for this reason therefore that regulations have to be partly relativistic. As AI technology advances, our lawmakers should be mindful that cybersecurity rules, as well as new legislative approaches, act in a pace that reflects fully AI advancement, whereby the old problems and threats are addressed without stopping the development of the raring opportunities. Several authorities have leverage sandbox and pilot schemes in which the regulators and the related implementing businesses can try out these new AI solutions and incorporate the required adaptation measures within a closed environment [52].

Industry-Specific Regulations: Cyber risks are different for different industries. For instance financial services and health care and several of the critical sectors of the economy are in dire need of certain types of cybersecurity. This means that, any future regulation should consider the above-discussed risks so that, while the regulation addresses a certain sector, it also provides principles of general governance on the use of AI across sectors [53].

AI in cybersecurity is a very broad concept because it brings in to the table the ability to revolutionize all aspects of cybersecurity at the organizational level. However if there is no sufficient laws or rules governing and regulating AI then the following is at risk-Invasion of privacy, Biased AI decision making, use of the technology in launching cyber-attacks. It is therefore important to have continuing and worldwide evolving consensus on the rules in order to have proper application of AI in the cybersecurity opportunity [54]. Cybersecurity can therefore build on AI at the same time as it develops constraints and concepts on a suitable application of the technology together with the safeguarding of the civil liberties.

8. Conclusion

The relationship between AI and Cybersecurity and between cybercriminals is one of the most unique and dynamically improving directions in the cyber space. Due to the increase in technologies AI is more relevant today in combating cyber-criminal activities. As it is capable of detecting an attack or threat and informing the security personnel, and in some moments even determine the kind of attack that maybe launched, then artificial intelligence is the solution to the current challenges that come with complex systems and a continuing mira of threats. But this has new opportunities which in fact come with the drawback especially when this is looked at from the morality, privacy and legislation perspective. With the help of artificial intelligence in cybersecurity people can obtain accurate threat identification and counteraction, and faster results than with manually incorporated systems with the possibility to enhance the management of threats as newer and more complex threats emerge. AI using the powerful features of machine learning and deep learning shall be in a position of finding out many patterns that may not be available to other analytical methods, and at the same time analyzing numerous iterations at a very short period of time, nhân power and time as well as identify many unknown security gaps. These capabilities albeit a quite distinctive, also makes Artificial Intelligence a double edged sword as the hacker can use the AI gadget to the following; Ability to develop AI malware or very complicated social engineering attacks.

9. References

[1]. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J.D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A.: Language models are few-shot learners. Adv. Neural Inform. Process. Syst. 33, 1877–1901 (2020)

[2]. Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A.: Training language models to follow instructions with human feedback. Adv. Neural Inform. Process. Syst. 35, 27730–27744 (2022)

[3]. Abdullah, M., Madain, A., Jararweh, and Y.: Chatgpt: fundamentals, applications and social impacts. In: Ninth international conference on social networks analysis, management and security (SNAMS), pp. 1–8. IEEE (2022)

[4]. Radford, A., Narasimhan, K., Salimans, T., Sutskever, I., et al.: Improving language understanding by generative pre-training (2018)

[5]. Schneider, E.T.R., Souza, J.V.A., Gumiel, Y.B., Moro, C., Paraiso, E.C.: A GPT-2 language model for biomedical texts in Portuguese. In: IEEE 34th international symposium on computerbased medical systems (CBMS), pp. 474–479. IEEE (2021)

[6]. Clark, E., August, T., Serrano, S., Haduong, N., Gururangan, S., Smith, N.A.: All that's' human is not gold: evaluating human evaluation of generated text. arXiv preprint arXiv:2107.00061 (2021)

[7]. Ippolito, D., Duckworth, D., Callison-Burch, C., Eck, and D.: Automatic detection of generated text is easiest when humans are fooled. arXiv preprint arXiv:1911.00650 (2019)

[8]. Dale, R.: Gpt-3: what's it good for? Nat. Lang. Eng. 27(1), 113–118 (2021)

[9]. Kolides, A., Nawaz, A., Rathor, A., Beeman, D., Hashmi, M., Fatima, S., Berdik, D., Al-Ayyoub, M., Jararweh, Y.: Artificial intelligence foundation and pre-trained models: fundamentals, applications, opportunities, and social impacts. Simul. Modell. Pract. Theory 126, 102754 (2023)

[10]. Noever, D., Williams, K.: Chatbots as fluent polyglots: revisiting breakthrough code snippets. arXiv preprint arXiv:2301.03373 (2023)

[11]. Checkpoint: cybercriminals bypass ChatGPT restrictions to generate malicious content. www.checkpoint.com 24. Karanjai, R.: Targeted phishing campaigns using large scale language models. arXiv preprint arXiv:2301.00665 (2022)

[12]. Heaven, W.: A GPT-3 bot posted comments on reddit for a week and no one noticed. https://www.technologyreview.com/

[13]. . Ben-Moshe, S., Gekker, G., Cohen, G.: OPWNAI: AI that can save the day or hack it away. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

[14]. Patel, A., Satller, J.: Creatively malicious prompt engineering (2023) 28. Zhai, X.: Chatgpt user experience: implications for education. (2022)

[15]. Susnjak, T.: Chatgpt: The end of online exam integrity? arXiv preprint arXiv:2212.09292 (2022)

[16]. Pang, Z.-H., Fan, L.-Z., Dong, Z., Han, Q.-L., Liu, G.-P.: False data injection attacks against partial sensor measurements of networked control systems. IEEE Trans. Circ. Syst. II: Express Briefs 69(1), 149–153 (2021)

[17]. Morris, T.H., Thornton, Z., Turnipseed, I.: Industrial control system simulation and data logging for intrusion detection system research. 7th annual southeastern cyber security summit, 3–4 (2015)

[18]. Jolfaei, A., Kant, and K.: On the silent perturbation of state estimation in smart grid. IEEE Trans. Ind. Appl. 56(4), 4405–4414 (2020)

[19]. Pei, C., Xiao, Y., Liang, W., Han, X.: Detecting false data injection attacks using canonical variate analysis in power grid. IEEE Trans. Network Sci. Eng. 8(2), 971–983 (2020)

[20]. Al-Hawawreh, M., Sitnikova, E., Den Hartog, F.: An efficient intrusion detection model for edge system in brownfield industrial internet of things. In: Proceedings of the 3rd international conference on big data and internet of things, pp. 83–87 (2019)

[21]. Feng, Y., Huang, S., Chen, Q.A., Liu, H.X., Mao, Z.M.: Vulnerability of traffic control system under cyberattacks with falsified data. Transp. Res. Rec. 2672(1), 1–11 (2018) 36.

OpenAI: Open AI privacy policy. Accessed on: 2022-02-15. https://www.openai.com/privacy

[22]. Balash, D.G., Wu, X., Grant, M., Reyes, I., Aviv, A.J.: Security and privacy perceptions of fThird-Partyg application access for google accounts. In: 31st USENIX security symposium (USENIX Security 22), pp. 3397–3414 (2022)

[23]. Roy, S.S., Naragam, K.V., Nilizadeh, S.: Generating phishing attacks using chatgpt. arXiv preprint arXiv:2305.05133 (2023)

[24]. Renaud, K., Warkentin, M., Westerman, G.: From ChatGPT to HackGPT: Meeting the cybersecurity threat of generative AI. MIT Sloan Management Review (2023)

[25]. Sebastian, G.: Do chatgpt and other AI chatbots pose a cybersecurity risk?: an exploratory study. Int. J. Secur. Priv. Pervas. Comput. (IJSPPC) 15(1), 1–11 (2023)

[26]. Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 67-76.

[27]. Sebastian, G.: Privacy and data protection in chatgpt and other AI chatbots: Strategies for securing user information. (2023)

[28]. Wright D., Kumar R. (2023) Assessing the socio-economic impacts of cybercrime. Societal Impacts. https://doi.org/10.1016/j.socimp.2023.100013

[29]. Cascavilla G., Tamburri D. A., Van Den Heuvel W-J (2021) Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security. https://doi.org/10.1016/j.cose.2021.102258.

[30]. European Convention on Human Rights (1950). Council of Europe. Ragan S. (2022). What is “Convention 108”?. Babovic M (2004). “Kompjuterska prevara I Internet prevara”,

[31]. Stahl B. C., (2021) Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies. Springer Cham.

[32]. Bai M., Fang X., (2022) Cybersecurity Analytics: AI’s Role in Big Data Threat Detection, 11 Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal. Pg 392 (2022).

[33]. Juneja A. et al., (2021). Artificial Intelligence and Cybersecurity: Current Trends and Future Prospects, in The Smart Cyber Ecosystem for Sustainable Development. Pg 431.

[34]. Morel B., (2011) Artificial Intelligence and the Future of Cybersecurity. In Proceedings of the 4th ACM workshop on Security and artificial intelligence. Pg 93.

[35]. Kaur R., Gabrijelčič D., Klobučar T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion. Pg 97. Patel H. (2023), The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML). doi:10.20944/preprints202301.0115.v1

[36]. Sarker I. H., Furhad M. H., Nowrozy R., (2021) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions, Vol.:(0123456789)SN Computer Science (2021) 2:173. https://doi.org/10.1007/s42979-021-00557-0.

[37]. Briggs, M., & Kodnani, N. (2023, March 26). The potentially large effects of artificial intelligence on economic growth. Goldman Sachs. Retrieved from https://www.gspublishing.com/content/research/en/reports/2023/03/27/d64e052b-0f6e45d7-967b-d7be35fabd16.html

[38]. Chamberlain, J. (2023). The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective. European Journal of Risk Regulation, 14, 1–13. https://doi.org/10.1017/err.2022.

[39]. European Commission. (2020, February 19). White Paper on Artificial Intelligence - A European approach to excellence and trust (COM/2020/65 final). Brussels. Retrieved from https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065

[40]. S. Zhou, C. Liu, D. Ye, T. Zhu, W. Zhou, and P. S. Yu, "Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity," ACM Computing Surveys, vol. 55, no. 8, pp. 1–39, 2023

[41]. A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "A survey on adversarial attacks and defences," CAAI Transactions on Intelligence Technology, vol. 6, no. 1, pp. 25–45, 2021.

[42]. F. Aloraini, A. Javed, O. Rana, and P. Burnap, "Adversarial machine learning in IoT from an insider point of view," Journal of Information Security and Applications, vol. 70, 2022.

[43]. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI's Revolutionary Role in Cyber Defense and Social Engineering. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 57-66.

[44]. A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors," Progress in Nuclear Energy, vol. 161, 2023.

[45]. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566-578.

[46]. B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," Applied Artificial Intelligence, vol. 36, dec 2022.

[47]. T. C. Truong, Q. B. Diep, and I. Zelinka, "Artificial Intelligence in the Cyber Domain: Offense and Defense," Symmetry, vol. 12, p. 410, mar 2020.

[48]. L. Fritsch, A. Jaber, and A. Yazidi, "An Overview of Artificial Intelligence Used in Malware," Communications in Computer and Information Science, vol. 1650 CCIS, pp. 41–51, 2022.

[49]. J. Chen, C. Su, and Z. Yan, "AI-Driven Cyber Security Analytics and Privacy Protection," Security and Communication Networks, vol. 2019, 2019.

[50]. B. Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era," BMC Medical Ethics, vol. 22, no. 1, 2021. [51] R. Blackman, "A Practical Guide to Building Ethical AI," tech. rep., 2020.

[51]. V. Liagkou, C. Stylios, L. Pappa, and A. Petunin, "Challenges and opportunities in industry 4.0 for mechatronics, artificial intelligence and cybernetics," Electronics (Switzerland), vol. 10, no. 16, 2021

[52]. Thiyagarajan P., "A Review on Cyber Security Mechanisms Using Machine and Deep Learning Algorithms," pp. 23–41, 2019.

[53]. T. M. Ghazal, M. K. Hasan, R. A. Zitar, N. A. Al-Dmour, W. T. Al-Sit, and S. Islam, "Cybers Security Analysis and Measurement Tools Using Machine Learning Approach," 2022 1st International Conference on AI in Cybersecurity, ICAIC 2022, 2022.

[54]. Arif, A., Khan, A., & Khan, M. I. (2024). Role of AI in Predicting and Mitigating Threats: A Comprehensive Review. *JURIHUM: Jurnal Inovasi dan Humaniora*, *2*(3), 297-311.