JOURNAL OF AERONAUTICAL MATERIALS
ISSN: 1005-5053

Vol. 43, Issue-01, 2023
pp. 1557-1570

STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGES

Syed Minhajul Hassan[1] and Dr.Javed Wasim[2]

[1] Institute of Engineering and Technology,Mangalayatan University Aligarh,UP,INDIA
[2] Institute of Engineering and Technology,Mangalayatan University Aligarh,UP,INDIA

[1]20200937_syed@mangalayatan.edu.in, [2]javed.wasim@mangalayatan.edu.in

ABSTRACT

The modern world is data-driven. Cybersecurity is essential to prevent data loss. In recent years, cyberattacks have increased in sophistication and frequency. Cybercriminals will inevitably start using AI methods to hide in plain sight online and multiply their harm. Cybersecurity safeguards our digital infrastructure, but the number of potential cyberattacks grows daily. They are immune to standard algorithmic countermeasures. Experts' defensive measures are useless. Because of this, Artificial Intelligence (AI) is being used to protect networks better. AI models need specialized network safety guards and assurance innovations to counteract hostile AI, ensure AI security, and safeguard cooperative learning. We examine the intersection between AI and digital security based on these two vantage points. Today, artificial intelligence is a commonplace occurrence. It reflects the way people think, feel, behave, and learn. It has constructive and destructive applications, such as voice recognition, intelligent robotics, gaming, etc. The use of AI for everyday tasks opens the door to cyberattacks that might compromise the integrity of the work itself or steal sensitive information. Possible solutions to cybersecurity problems using AI are explored, along with some of the dangers that may arise from its use. Also discussed is the possibility of eliminating or at least lessening these dangers.

Keywords: Artificial Intelligence (AI), Cyberattacks, cyber security, cybercrime, hacking,

INTRODUCTION

With the complexity of malware and cyber-arms developing significantly over the last two years, it is evident that only intelligent technology can assist guard against such advanced cyber weapons. The Conficker worm compromised the French Navy's computer network, known as "Ultramar," on January 15, 2009. Due to the inability to make changes to flight schedules, the service has been quarantined, forcing planes at several airbases to return to the ground [1]. The British Ministry of Defense has admitted that some of its most important hardware and software has been compromised. The malware has infected over 800 devices at Sheffield institutions, including hospitals and government buildings. They claimed on February 2, 2009, that the German unified military forces, the Bundeswehr, had hacked over a hundred of their devices. The Greater Manchester Police Information Network preemptively disconnected the Police Central Database for three days in January 2010. In order to conduct routine searches of vehicles and people, staff have to coordinate with specific troops [2]. Network Centric Warfare (NCW) increases the risks of cyber accidents. Hence new approaches to cyber defense are urgently required. New offensive measures, such as the dynamic building of protective perimeters and, integrated crisis management, completely automated responses to assaults in networks [3], would need the employment of artificial intelligence techniques and knowledge-intensive technologies.

Security experts agree that 2019 had a record-breaking number of events [4]. There was a rise in the sophistication of cyberattacks across the board in 2017 [5]; this included everything from phishing and ransomware to the dark web as a service economy and assaults on civil infrastructure. The increasing trend continued until the year 2020. In the second quarter of 2020, researchers saw an increase of 44 malware attacks per minute or 12 percent. 27 Hackers took advantage of the Covid19 outbreak and people's and businesses' increasing reliance on the internet by exploiting flaws in remote equipment and network bandwidth. As of April 2020, Interpol has logged 907,000 Covid-19-related spam emails.

Additionally, 34% of respondents in the 2020 Remote Workforce Cybersecurity Report reported experiencing a breach themselves due to the transition to telework [6]. Using the high impact and financial reward possibilities, threat actors sent out themed phishing emails pretending to be from government and health authorities to acquire personal data and malware targeting vital infrastructure and healthcare facilities [7]. The push for ubiquitous connection and digitalization will continue to fuel economic growth in 2021. However, it will also 'unavoidably' provide a breeding environment for an increase in the magnitude and number of cyberattacks. The proliferation of ransomware and other forms of cybercrime, the rise of mobile cyber threats, the evolution of phishing techniques, the assaults on the systems that keep our society running, and the efforts of cybercriminals and state-sponsored hackers to seize any new opportunities they can find in the cloud are all contributing factors [8].

A. AI systems' support for cybersecurity

In light of this, businesses have begun using AI in their risk management strategies to better handle the wide variety of cybersecurity threats, technological difficulties, and limited resources they face. Companies are utilizing AI to improve cybersecurity, and the usage of police dogs as an example helps to illustrate why. While police officers rely on the specialized skills of police dogs to track out criminals, security analysts may use AI systems' capabilities to increase their job's efficiency drastically. To this end, the synergistic integration of AI systems and security operators is preferred to the alternative of pitting them against one another [9]. According to research, artificial intelligence (AI) in the cybersecurity market is expected to expand from $3.92 billion in 2017 to $34.81 billion in 2025, representing a CAGR (compound annual growth rate) of 31.38% [10]. A recent poll by Capgemini found that the use of AI in cybersecurity solutions is growing at a dizzying rate. From 5% of all organizations in 2019 using such a system, in 2020, that figure is expected to climb to 20% of all companies.

Regarding cybersecurity, 73% of the sample tried out AI apps. Network, data, and endpoint protection are often the first uses put to these technologies. The use of artificial intelligence (AI) in cybersecurity may be broken down into three broad categories: detection (51%), prediction (34%), and reaction (18%) [11].

Motivations for using AI in cybersecurity include the following:[12]:

1. Speed of impact: Organizations often feel the effects of large assaults within four minutes. In addition, modern assaults may shift and adapt depending on what their targets are doing; they are no longer limited to ransomware or targeting specific systems

or weaknesses. Such strikes' effects are felt instantly, leaving little time for human connection.

2. 2. Operational complexity: The widespread availability of cloud computing platforms today, and the fact that these platforms can be operationalized to deliver services in the millisecond range, means that you cannot have many humans in that loop and must instead consider a more analytics-driven capability.
3. Cybersecurity skill shortages continue to be an issue: Frost & Sullivan 35 estimates a need for an additional 1.5 million cybersecurity professionals worldwide. Due to the extreme lack of resources, businesses have been accelerating their use of automation technology.

Security teams may benefit from AI in three ways: increased system robustness, quicker reaction times, and more resilience. This approach is referred to as the "3R model" in the study [13]. AI's self-testing and self-healing software may increase a system's resilience or capacity to retain its original presumed stable configuration even while processing erroneous inputs. Artificial intelligence systems may enhance robustness testing by handing over verification and validation to machines. Second, AI may improve system resilience, or the capacity of a system to withstand and recover from an assault, by making it easier to identify threats and outliers. Third, AI may improve system reaction, or a system's ability to respond autonomously to assaults, detect flaws in other machines and use strategy by picking and choosing when and where to launch attacks and counterattacks. Organizations should do a risk-impact analysis when considering whether or not to give AI control over decisionmaking and reaction actions. Artificial intelligence (AI) will often be incorporated into systems that speed up reaction actions and supplement the decisionmaking of human security analysts.

RELATED STUDY

Today's cybercriminals may cause issues for the government, organizations, corporations, and people by using various AI-driven hack tactics. For this level of sophisticated cyberweaponry, the current state of cybersecurity is inadequate [14]. AI-driven cyberattacks are the malicious use of AI to breach digital security [15]. In these attacks, hackers may teach robots to engineer targets with human or even superhuman ability levels socially. Attacks aided by artificial intelligence can modify themselves to fit the host system. By analyzing its surroundings, a system might learn to mimic certain aspects of the internet or exploit its vulnerabilities [16]. Cyberattacks fueled by artificial intelligence are not some distant possibility. The components and infrastructure for an aggressive AI-driven cyberattack currently exist [17]. Recent AI developments have contributed to the explosive development of automation and new ideas. These AI systems may be put to good use in many contexts, but they also present the possibility of being put to wrong use. The use of artificial intelligence in cyberattacks has increased during the last several years. Many businesses still leave their data open to hackers even after moving to more secure technologies like cloud storage services [18]. The overall trend of AI-driven hacks will only increase, and soon, conventional cybersecurity systems will be unable to identify them. The choice between machines and people comes down to efficiency. Cybersecurity teams struggle to keep up because this tendency continues to expand in complexity and scale. However, highly trained cybersecurity experts, essential for effectively countering this danger, are becoming more scarce and costly. It is possible that these new forms of assault, powered by AI, may have catastrophic results. These covert assaults compromise data security and integrity, which may lead to catastrophic failures [18]. Cyberattacks powered by artificial intelligence (AI) will be quicker, more unexpected, and more sophisticated than anything a human-led cybersecurity team can counter. [19]. Cybersecurity researchers, practitioners, and governments will need to react with increasingly imaginative ways to effectively secure cyberspace from harmful actors as AI becomes a more potent weapon in the hands of bad actors [20]. In order to evade detection by behavioral and signature-based antivirus programs, AI-driven malware use complex obfuscation algorithms and constantly alter recognizable traits [21]. DeepLocker and other examples of malicious AI deployment in seemingly innocuous carrier apps show that AI is being used for malicious purposes. AI-driven cyberattacks, which combine classic cyberattack methods with artificial intelligence to wreak more significant harm in cyberspace while evading detection, are one example of cybercriminals' evolving and adapting attack strategies [22].

Cyberattack methods powered by artificial intelligence will be able to modify their operations based on their immediate context. They may attack the weaknesses through contextual data or information learning or pose as trustworthy system characteristics. Attacks grow increasingly integrated and immune to the host's objectives, surroundings, and countermeasures against cybersecurity defensive systems as time passes [14]. It is possible that these new forms of assault, powered by AI, may have catastrophic results. Because of this, this research looks at the growing danger of AI-driven assaults and discusses the drawbacks of such high-tech cyber warfare.

The White House acknowledges that many federal agencies are also using AI systems, joining the ranks of private corporations and industries that have previously accepted them. Why? Why? Since AI can quickly and efficiently save time and money by scanning standard data formats and thoroughly reading and analyzing large amounts of unstructured data, numerical patterns, and text, it is increasingly being used to supplement human labor in various fields. In reality, AI has the potential to protect both public funds and top-secret information.

Moreover, there exist voids. Hackers are likely attempting to get into the systems using vulnerabilities we are entirely unaware of. It might be years before an organization discovers a data breach [23]. That is too late since the hacker and any private information will be long gone. However, until a hacker gets nasty, AI has to sit back and gather data. For starters, whenever a password is typed or a user signs in, AI looks for irregularities in behavior that hackers are anticipated to demonstrate. Artificial intelligence may pick up on little clues that typically go unnoticed, blocking the hacker's outfit in their tracks. Every tool has its potential misuse, as Varughese pointed out. In the ongoing chess game that is cybersecurity, human hackers will always probe the weak places in any system, AI included. Because it is under human control, artificial intelligence still has a chance of being defeated.

Although AI's ability to connect and interpret data is extraordinary, it is limited by how it was programmed [24]. Programmers must implement new safeguards against hackers who have adapted to AI systems. Artificial intelligence is a powerful tool in the battle to keep sensitive information safe, and the game of cat and mouse will continue. Google developed a graphical data learning model for its Tensor Flow machine learning platform. The Neural Structured

Learning (NSL) open-source framework was implemented on 03/09/2019 and used the Neural Graph Learning technique to train data sets and data structures in neural nets. NSL is compatible with the machine learning stage TensorFlow and is made to work for qualified and incompetent machine learning professionals. Models for machine vision can be rendered in NSL, natural language processing (NLP) can be carried out, and interactive databases like medical records and data visualizations may be used to perform projections in NSL [25].

The area of artificial intelligence (AI) is quickly becoming a focal point for the computer security industry. We will examine how institutions, cybercriminals, and regular people are affected by AI and how security measures for the technology have progressed. Let us figure it out together. Automated information protection methods greatly enhance the internet's security. Numerous rapidly expanding businesses, like yours, likely use multiple layers of security, including those at the border, network, edge, device, and storage levels. Two examples are firewall rules (either hardware or software) and network security systems (which monitor and, among other things, establish which connected devices are permitted and avoid others). If bad actors circumvent these safeguards, they will be responsible for finding and implementing countermeasures against viruses and malware. Then they would have to deal with solutions like IDS and IPS.[26]

In addition to their research "Reinventing Cyber Protection with AI," which demonstrates the need to establish cybersecurity defenses using AI, the Capgemini Research Institute also looked at the state of information security. The poll found that 850 data security executives, IT information management, and IT operations professionals from 10 countries all agreed that AI-enabled solutions are crucial in the face of rising cyber-attacks. Some other highlights of the research include that 75% of respondents to the survey found that AI helped their company react faster to security breaches. Sixty-nine percent of businesses acknowledge the need for AI. [27] Three out of every five businesses believe that artificial intelligence improves the accuracy and productivity of cyber analysts. Artificial intelligence has the potential to not only improve the outlooks of current cybersecurity solutions but also to reconstruct the method by which new solutions are developed.

Using AI for cyber defense creates new vulnerabilities in physical security. Cybercriminals may leverage AI tools for progressive behavior assaults, making it just as critical to use AI technology to identify and counter malware threats. This is partly due to the decreasing costs of creating and deploying cutting-edge AI technologies, such as generative adversarial networks and deep reinforcement learning, which facilitate more access to these methods [28]. Cybercriminals can develop more complex and efficient harmful programs at a lower cost and shorter time. Because of all the many factors, users are vulnerable to cyber-attacks.

CURRENT AND EMERGING AI-DRIVEN CYBERATTACK TECHNIQUES

New methods and improved cyberattack tools are increasing the cyberattack arena and making cyberspace vulnerable to various destructive cyberweapons [29]. By inserting specific theoretical ideas into the digital, physical, and political security domains, Brundage et al. [30] created a scenario that alerts cybersecurity researchers and the industry to the malicious exploitation of AI. Researchers have shown the possibility of automated exploit creation in cutting-edge programs and have developed a few fundamental principles in this direction. Cybercriminals use fuzzy models to create advanced malware that can adapt to its surroundings, release new versions regularly, and infect systems without raising suspicion. Bad guys may use these ideas to launch a new generation of stealthy, high-tech cyber weapons.

A. AI-Driven Attacks in the Reconnaissance Stage of the Cybersecurity Kill Chain

The typical behavior and operations of a cybersecurity defensive mechanism, computer infrastructures, and devices may be studied using AI approaches [29]. If a bad actor can collect enough information about the user's devices, network flows, and architecture, they may establish a crucial connection with their intended targets. Artificial intelligence has the potential to be used by malicious actors to identify patterns of targeted assaults in large data sets. Reconnaissance attacks, which may also be categorized as AI-targeted attacks, need careful preparation before they can be launched successfully. In order to offer in-depth analysis and to design focused exploration procedures, AI may be used to overcome human constraints via its capacity to understand, uncover, and recognize patterns in enormous volumes of information [29]. The authors identified four AI-driven threat use cases as part of the reconnaissance phase of AI-targeted attacks. "These include intelligent target profiling, clever vulnerability detection/intelligent malware, intelligent collection/automated learn behavior, and intelligent vulnerability/outcome prediction."

Intelligent Target Profiling

The capacity to profile ICT users has already been proven to be affected by advances in AI. Bilal et al. [31] introduced a classification system for profiling methods and the corresponding artificial intelligence (AI) algorithms. The authors noted that there are two types of profiling—individual and group—and that the most popular artificial intelligence (AI) are fuzzy logic ontology, machine learning, and convolutional neural networks. Targets of cyberattacks may now be profiled in detail by analyzing their public social media profiles and online behavior, thanks to the development of AI methods. Groups may be able to target the appropriate message at the right moment with the help of AI technologies. Artificial intelligence (AI) technology may help bad actors enhance their chances of creating accurate profiles of their intended victims. Bad actors may use both DNNs and NNs for target profiling and classification. Evidence from research prototypes like SNAP R suggests a high probability of harmful end applications and a somewhat mature technological landscape for implementing intelligent profiling.

Intelligent Collection

Gathering information is similar to reconnaissance and is used to better plan and develop cyberattack policies. Such an assault uses artificial intelligence tools like natural language processing and deep neural networks. Due to their ability to automatically gather generic data on many assaults and variables that impact risk, these studies may be used for more than one purpose (both defensive and offensive) [32].

Intelligent Malware

Clever malware, by infecting environmental control systems, "may begin indirect cyber weaponries that masquerade to be unintended failures on computer infrastructure [33]. One sort of spear phishing that is more popular is the end-to-end kind, in which the bad guys do everything from finding their targets to sending them tailored, machine-generated messages.

Outcome Prediction

Artificial intelligence methods can look at what has happened in the past and now to make predictions about what will happen in the future. Improving AI prediction models may need new approaches to cyber-related assessment and simulation development. Offensive AI has the potential to provide hackers a boost of confidence to go after high-risk, high-reward targets to outwit cutting-edge cybersecurity solutions.

B. AI-Driven Attacks in the Access and Penetration Stage of the Cybersecurity Kill Chain

The next stage of a cyberattack is sometimes called an AI-aided assault. This investigation discovered six (6) access and penetration phase AI-driven assaults. These are examples of intelligent captcha/manipulation, clever aberrant behavior creation, brilliant AI model manipulation, and innovative fake review generation.

Automated Payload Generation/Phishing

Bahnsen et al.shown in DeepPhish: Simulating Malicious AI that bad actors may use machine learning algorithms as a weapon to bolster phishing attempts and render them undetectable by cybersecurity detection systems. DeepPhish is an artificial intelligence program that synthesizes new phishing URLs by learning patterns from the most successful phishing URLs in the past. The goal is to develop more sophisticated phishing URLs to evade AI detection and facilitate more efficient phishing attempts. In the past, attackers used randomly generated segments to construct phishing URLs. The authors proved the efficacy of phishing assaults by boosting the efficiency and success rate of these attacks by using an LSTM model to classify phishing URLs and generate new, successful synthetic phishing URLs. According to the authors, increasing the attack's success rate from 0.69% to 20.9% and from 4.91% to 36.28% was achieved via training DeepPhish on two distinct threat actors.

AI-Driven Password Guessing/Password Cracking

It was determined that there are three distinct kinds of password assaults powered by AI. These include the brute-force attack, the guessing attack, and the stealing attack. Haj et al. [34] suggested a deep learning model guess passwords. By studying the frequency of password breaches, the scientists refined a GAN-based automated password-guessing approach. Rule-based techniques include setting and generating rules for various password modifications like concatenation. In contrast, dictionary attacks involve utilizing a list of plausible terms and past password breaches in the hopes of successfully guessing.

Hitaj et al. [34] developed a technique for effectively training a GAN, allowing the generation of individually crafted samples from the training data. Passwords may be generated automatically by using GAN in the following ways: The GAN consists of two concatenated DNNs, one for generation (G) and one for classification (D) (D). Password samples, a trove of compromised credentials, are also available in a training dataset. The generator G, which stands for a random probability distribution and produces a series of vectors called false password samples, was trained using a noise vector. Discriminator D is trained to distinguish between actual and fake data by being fed both. G forces D to provide him with information to determine how accurately password leaks were first dispersed. PassGAN was trained using the RockYou dataset, a widely used password database, and it successfully guessed fresh, unique passwords and reproduced the RockYou dataset's distribution. Out of the 43,354,871 unique passwords stolen from LinkedIn, PassGAN successfully matched 10,478,322 (24.2%). Despite never having seen any LinkedIn information, GAN generated secure, memorable passwords from the RockYou words. When used in tandem with HashCat, PassGAN improved password prediction accuracy by 51%-73% over HashCat alone.

K-Nearest Neighbors (KNN), logistic regression (LR), decision tree (DT), linear support vector classifier (SVC), random forest (RF), support vector machine (SVM), gradient boosting regression tree (GBRT), and multilayer perceptron models were implemented by Lee and Yim [34] to classify data obtained from key presses. When it came to intercepting keystrokes, the ultimately deployed model was 96.2% accurate. This implies that real-world thieves may employ AI methods to acquire consumers' actual keyboard data. To create new candidate passwords with a similar pattern to previous passwords [35], Trieu and Yang [36] used Torch-run, an open-source machine learning approach.

Intelligent Captcha Attack and Manipulation

Using cycle-GAN, Li et al. [37] trained Captcha synthesizers to generate many phony examples for text-based Captchas. The fabricated data set was used to educate convolutional recurrent neural network-based basic recognizers. After that, the basic recognizer is fine-tuned with the use of a transfer learning method and a few labeled examples of real-world Captcha. Amazon (86.4 percent), Apple (0.877 percent), Sina (0.85 percent), Baidu (0.807 percent), Weibo (0.798 percent), eBay (0.743 percent), and Sogou (0.717 percent) are just a few of the famous sites whose Captchas were successfully bypassed using this method; Microsoft's two-layer approach had a success rate of 0.224, suggesting the attack is pervasive. The results show that using a combination of anti-recognition methods is possible to boost captcha security, although only by a small margin.

With deep learning, Gao et al. [38] could decipher text-based Captchas and develop their image-based alternatives. Four CNN models with 2, 3, 5, and 6 convolutional layers were used as recognition engines. The authors were able to break through the Roman-character-based Captchas used by the top 50 websites in the world and three Chinese Captchas that employ a more extensive character set, with success rates ranging from 0.10 to 0.90. This assault is proceeding at a rate that is, on average, far quicker than any previous ones. This aggressive AI approach can penetrate other current Captchas since its concentrated tactics encompass practically all known resistance measures. Using a GAN-based method, Ye et al. [39] created a tool to decipher textual Captchas. To do this, we first used a Captcha synthesizer, which automatically creates synthetic captchas, to develop a base solution. Then we used transfer learning to fine-tune the base solver on a small subset of genuine Captchas. The authors tested the model's performance with 33 distinct Captcha schemes, including 11 now used by 32 top 50 most visited websites. The authors proved the superiority of their approach by deciphering cutting-edge Captchas in less than 0.05 seconds. When bypassing Microsoft's two-layer Captcha, Gao et al. [38] offered a simple yet successful AI-driven approach. As the core of their recognition system, the authors trained an enhanced version of the revolutionary CNN model LeNet-5. On a regular desktop computer with a 3.3 GHz Intel Core i3 CPU, the implemented model had an average success rate of 44.6% and a speed of 9.05 seconds.

Smart Fake Review Generation

Yao et al. [40] developed a two-stage method for generating and personalizing reviews that can fool statistical detectors. The authors deployed an RNN-based fake review generator that can provide deceptive but plausible evaluations of eateries on the Yelp app. The high standard of these evaluations demonstrates the difficulties in spotting this kind of assault.

AI-Model Manipulation

Using adversarial approaches, bad actors may intentionally modify the data of machine learning models to make them inaccurate. Attackers may trick spam filters' categorization model by inserting a spoofed input set or changing the wording of spam emails. By manipulating the input and training data, cybercriminals may exploit the Naive Bayes (NB) model used for spam mail screening. Deep model poisoning attacks on federated learning were studied in depth by Zhou et al. [41]. In order to increase the durability, efficiency, and resilience of poisoning assaults, the authors injected rogue neurons into the redundant network space, using the regularization term in the goal function. Adversarial examples are samples that have been modified on purpose to fool DNN models. Adversarial examples are constructed with little alterations, yet they mislead DNN models into making inaccurate predictions.

C. AI-Driven Attacks in the Delivery Stage of the Cybersecurity Kill Chain

Intelligent Concealment and Evasive Malware

Using LSTM, Bahnsen et al. [42] created complex phishing URLs that evaded the most advanced cybersecurity detection systems. Hu and Tan [43] suggested a GAN approach that may generate undetectable adversarial malware to avoid detection by machine-learning black-box systems. Using a GAN, Anderson, Woodbridge, and Filar [44] suggested an autonomous malware URL generator that learns to evade detection by DNNs. The result demonstrates that domains created by the implemented GAN model are immune to detection by DNNs and GAN malware scanners. A random forest classifier that uses characteristics that have to be created by hand was also readily defeated. The sophisticated evasive malware presented by Kirat, Jang, and Stoecklin [45] may conceal its harmful payload assault in video conferencing apps without being seen by the user or the application's security measures. They used DNNs to hide their malicious intent and only activated them on specific targets.

CHALLENGES

Plans for future research, manufacturing, and deploying an AI approach to cybersecurity should clearly distinguish between short-term goals and long-term visions. It is possible to apply several AI methods to cybersecurity rapidly, yet pressing cybersecurity problems need more innovative solutions that are now in use. At this point, we have just discussed the currently available instant applications. It would be fascinating to see novel notions of information processing applied to managing future conditions and decision-making. It is a challenging technological sector to handle knowledge for networked central warfare. Only with fully automated information management can leaders and policymakers gain a commanding advantage at all times. This article provides a synopsis of the present command and control system of the Bundeswehr, including its centralized and decentralized information models. Considering the long-term future, we probably should not depend only on Narrow AI for the next several decades. Some may be tempted to believe that by the middle of the 20th century, we will have achieved the primary aim of AI, which is to create artificial cognition in the form of an AGI. The first AGI conference was held at the University of Memphis in 2008. The Singularity Institute for Artificial Intelligence (SIAI), founded in 2000, warns that robots' rapidly expanding intelligence poses a potential threat. Singularity, described as "the technological progression of cognition that is wiser than a person," is possible at this point. There is a lot of breakthroughs that are often mentioned as potential ways ahead. While AI is now the most talked about, many other advances also pave the way for the creation of intelligent intelligence, so long as they surpass a specific complexity barrier.

IMPACT OF AI-DRIVEN CYBERATTACKS

New AI-powered hacks have the potential to cause severe damage and even loss of life. Highly sophisticated and covert assaults will destroy faith in companies and could lead to systemic failures by eroding data confidentiality and integrity. Think of a doctor or expert delivering a diagnosis based on manipulated medical records or a drilling rig looking for oil in the incorrect place because of faulty geo-prospecting data. Due to AI's ability to learn and adapt, we are now living in an age when assaults may be launched in large numbers while being precise and mimicking human behavior. An attacking AI that learns from its environment will be sophisticated enough to infiltrate systems with minimal risk of being detected [46]. PassGAN is an example of an artificial intelligence-driven attack that can generate many effective password guesses, which may then be used to get past current cybersecurity authentication systems and do further harm.

CONCLUSION

Cybercriminals emphasize the use of AI-driven approaches in the attack process, and this emphasis is ever-evolving and improving. This research delves into the AI's offensive capabilities, which provide attackers the means to launch strikes on a grander scale, with more reach, and at a quicker rate. In order to assess the harmful effects of AI-driven cyberattacks, this research analyzed the available literature on the topic.

Researchers, policymakers, and industry professionals are urged to use AI to defend themselves against malicious AI and to develop cutting-edge defenses against AI-driven cyberattacks. In order to stop AI-driven assaults in the future, a reliable AI framework will be created to help explain critical elements that affect the detection logic.

REFERENCES

[1] Use of Artificial Intelligence Techniques / Applications in Cyber Defense. (n.d.). Retrieved August 14, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniqu es_Applications_in_Cyber_Defense

[2] Ahmad, I., Abdullah, A. B., &Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. https://doi.org/10.1145/1626195.1626252

[3] . Bai, J., Wu, Y., Wang, G., Yang, S. X., &Qiu, W. (2006). A novel intrusion detection model based on multilayer self-organizing maps and principal component analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial

Intelligence and Bioinformatics), 3973 LNCS, 255–260. https://doi.org/10.1007/11760191_37.

[4] In the first quarter of 2019, businesses detected a 118% increase in ransomware attacks. They discovered new ransomware families such as Anatova, Dharma, and GandCrab, which use innovative techniques to target and infect enterprises, MacAfee (2019), "McAfee Labs Threats Report," August.

[5] M.Drolet (2020), "The Evolving Threat Landscape: Five Trends to Expect in 2020 and Beyond", Forbes Technology Council; Orange Business Service (2020), "2020 Security Landscape".

[6] Fortinet (2020), Enterprises Must Adapt to Address Telework Security Challenges: 2020 Remote Workforce Cybersecurity Report", August.

[7] INTERPOL (2020), "INTERPOL report shows alarming rate of cyberattacks during COVID-19", August (www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-duringCOVID-19).

[8] Splunk (2019), "IT Security Predictions 2020"; ENISA (2020), "Emerging Trends – ENISA Threat Landscape," October 20 (www.enisa.europa.eu/publications/emerging-trends)

[9] K. Skapinetz (2018), "Overcome cybersecurity limitations with artificial intelligence," June (www.youtube.com/ watch?time_continue=10&v=-tIPoLin1WY&feature=emb_title).

[10] MarketsandMarkets, "Artificial Intelligence in Cybersecurity Market by Technology Machine Learning, Context Awareness - 2025", MarketsandMarkets (www.marketsandmarkets.com/Market-Reports/ai-in-cybersecuritymarket-224437074.html)

[11] CAP Gemini (2019), "Reinventing Cyber security with Artificial Intelligence. The new frontier in digital security", Research Institute.

[12] This section is taken from McAfee's contribution to the CEPS Task Force kick-off meeting.

[13] See M. Taddeo, T. McCutcheon, and L. Florida (2019) on this, "Trusting artificial intelligence in cybersecurity is a double-edged sword," Nature Machine Intelligence, November.

[14] Thanh, C., and I. Zelinka. 2019. A survey on artificial intelligence in malware as next-generation threats. MENDEL 25 (2):27–34. doi:https://doi.org/10.13164/mendel.2019.2.027.

[15] Brundage, M., S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Sc harre, T. Zeitzoff, B. Filar, et al. 2018. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. Oxford: Future of Humanity Institute.

[16] DarkTrace. 2021. The Next Paradigm Shift AI-Driven Cyber-Attacks. DarkTrace Research White Paper. https://www.oixio.ee/sites/default/files/the_next_paradigm_shift_-_ai_driven_cyber_attacks.pdf (accessed June 9, 2021)

[17] Dixon, W., and N. Eagan. (2019). AI will power a new set of tools and threats for the cyber criminals of the future. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/ (accessed December 3, 2020). [Google Scholar]

[18] Bonetta, S. (2020). Has an AI cyberattack happened yet? https://www.infoq.com/articles/ai-cyberattacks/ (accessed December 9, 2020).

[19] Cabaj, K., Z. Kotulski, B. Księżopolski, and W. Mazurczyk. 2018. Cybersecurity: trends, issues, and challenges. EURASIP Journal On Information Security. Doi:https://doi.org/10.1186/s13635-018-0080-0.

[20] Hamadah, S., and D. Aqel. 2020. Cybersecurity becomes smart using artificial intelligence and machine learning approaches: An overview. ICIC Express Letters, Part B: Applications 11 (12):1115–1123. D

[21] Babuta, A., M. Oswald, and A. Janjeva. 2020. Artificial Intelligence and UK National Security Policy Considerations. Royal United Services Institute Occasional Paper.

[22] Kaloudi, N., and J. Li. 2020. The AI-based cyber threat landscape. ACM Computing Surveys 53 (1):1–34. doi:https://doi.org/10.1145/3372823

[23] Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Bioinformatics), 1907, 93–109. https://doi.org/10.1007/3-540-39945-3_7.

[24] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., &Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

[25] IOS Press. (n.d.). Retrieved August 14, 2020, from https://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/.4

[26] Pachghare, V. K., Kulkarni, P., &Nikam, D. M. (2009). Intrusion detection system using self-organizing maps. 2009 International Conference on Intelligent Agent and Multi-Agent Systems, IAMA 2009, 4(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074

[27] Protect yourself from the Conficker computer worm. (2009). Microsoft. http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.

[28] Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461). https://doi.org/85-460-1

[29] Kaloudi, N., and J. Li. 2020. The AI-based cyber threat landscape. ACM Computing Surveys 53 (1):1–34. doi:https://doi.org/10.1145/3372823. [

[30] Brundage, M., S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Sc harre, T. Zeitzoff, B. Filar, et al. 2018. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. Oxford: Future of Humanity Institute.

[31] Bilal, M., A. Gani, M. Lali, M. Marjani, and N. Malik. 2019. Social profiling: A review, taxonomy, and challenges. Cyberpsychology, Behavior and Social Networking 22 (7):433–50. doi:https://doi.org/10.1089/cyber.2018.0670.

[32] Cheap, V. 2017. AI in cybersecurity: A balancing force or a disruptor? https://www.rsaconference.com/industry-topics/presentation/ai-in-cybersecurity-a-balancing-force-or-a-disruptor (accessed February 13, 2020).

[33] Chung, K., Z. T. Kalbarczyk, and R. K. Iyer. 2019. Availability attacks on computing systems through alteration of environmental control: Smart malware approach. Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, Montreal, Quebec, Canada, 1–12.

[34] Hitaj, B., P. Gasti, G. Ateniese, and F. Perez-Cruz. 2019. PassGAN: A deep learning approach for password guessing. Applied Cryptography and Network Security 11464:217–37. doi:https://doi.org/10.1007/978-3-030-21568-2_11.

[35] Lee, K., and K. Yim. (2020). Cybersecurity threats based on machine learning-based improper technique for password authentication. Applied Sciences 10 (4):1286.

[36] Trieu, K., and Y. Yang. 2018. Artificial intelligence-based password brute force attacks. Proceedings of Midwest Association for Information Systems Conference, St. Louis, Missouri, USA, 13(39).

[37] Li, C., X. Chen, H. Wang, P. Wang, Y. Zhang, and W. Wang. 2021. End-to-end attack on text-based CAPTCHAs based on cycle-consistent generative adversarial network. Neurocomputing 433:223–36.
Doi:https://doi.org/10.1016/j.neucom.2020.11.057.

[38] Gao, H., M. Tang, Y. Liu, P. Zhang, and X. Liu. 2017. Research on the security of microsoft's two-layer Captcha. IEEE Transactions On Information Forensics And Security 12 (7):1671–85. doi:https://doi.org/10.1109/tifs.2017.2682704.

[39] Ye, G., Z. Tang, D. Fang, Z. Zhu, Y. Feng, P. Xu, X. Chen, and Z. Wang. 2018. Yet another text captcha solver. Proceedings of The 2018 ACM SIGSAC Conference On Computer And Communications Security, Toronto, Canada. doi:https://doi.org/10.1145/3243734.3243754

[40] Yao, Y., B. Viswanath, J. Cryan, H. Zheng, and B. Zhao. 2017. Automated crowdturfing attacks and defenses in online review systems. Proceedings Of The 2017 ACM SIGSAC Conference On Computer And Communications Security, Dallas Texas, USA. doi:https://doi.org/10.1145/3133956.3133990.

[41] Zhou, X., M. Xu, Y. Wu, and N. Zheng. 2021. Deep model poisoning attack on federated learning. Future Internet 13 (3):73. doi:https://doi.org/10.3390/fi13030073.

[42] Bahnsen, A. C., I. Torroledo, L. Camacho, and S. Villegas. 2018. DeepPhish: Simulating malicious AI. In APWG Symposium on Electronic Crime Research, London, United Kingdom, 1–8.

[43] Hu, W., and Y. Tan. 2021. Generating adversarial malware examples for black-box attacks based on GAN.https://arxiv.org/abs/1702.05983 (accessed August 12, 2021).

[44] Anderson, H. S., J. Woodbridge, and B. Filar. 2016. Deepika: Adversarially-tuned domain generation and detection. In Proceedings of the ACM Workshop on Artificial Intelligence and Security, Vienna, Austria, 13–2409

[45] Kirat, D., J. Jang, and M. Stoecklin. 2018. DeepLocker concealing targeted attacks with AI locksmithing. https://www.blackhat.com/us-

18/briefings/schedule/index.html#deeplocker—concealing-targeted-attacks-with-locksmithing-11549 (accessed December 4, 2020).

[46] Dixon, W., and N. Eagan. 2019. AI will power a new set of tools and threats for the cyber criminals of the future. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/ (accessed December 3, 2020).