www.ijecs.in
International Journal of Engineering and Computer Science
Volume 14 Issue 04 April 2025, Page No. 27073- 27084
ISSN: 2319-7242 DOI: 10.18535/ijecs/v14i04.5076

AI and Cyber Threats: A Battle of Intelligence

Yasir Khan [1], Manish Kumar [2], Sharik Ahmad [3]
[1] Department of Computer Science & Applications, SSCSE, Sharda University, Greater Noida, India
[2] Department of Computer Science & Applications, SSCSE, Sharda University, Greater Noida, India
[3] Department of Computer Science & Applications, SSCSE, Sharda University, Greater Noida, India

Abstract
The fast-paced technological development drives periodic evolution of cyber dangers. Every day novel attack techniques appear which display specific features that enable digital system and data breach. The examination in this paper reviews cyber threat historical progression while inspecting modern threat patterns and expected future dangers alongside an analysis about Artificial Intelligence (AI) cyber threat functions and protective mechanisms. Security professionals now use artificial intelligence for defensive and offensive actions throughout their cybersecurity work. AI makes cyber defense improvements but still provide advanced attack technology to hackers which overcomes standard security protocols. AI-driven security threats are predicted to become greater challenges in the future because they may exceed human-operated cyberattacks in size and speed. The self-learning quality of AI systems functions as both an advantage and a problem in cybersecurity operations. This paper examines previous cyber threats together with existing AI-driven security risks and proposed countermeasures that defend against upcoming AI-powered cyber-attacks

Keywords: Cyber threats, Artificial Intelligence, cybersecurity, AI-powered attacks, malware

1. Introduction

A cyber or cybersecurity threat is any cyber harm which is intended to destroy, capture, or otherwise infringe upon, that occurs in the digital. A cyber threat is something like malicious software, unauthorized access, web-scanning, denial of Service attacks or any attacks of this kind. [1,2] The field of cyber threats includes illegal systems activities which try to break digital security systems by targeting their integrity and confidentiality and availability. Malware and unauthorized access and phishing and Distributed Denial-of-Service (DDoS) attacks comprise the threats [18]. The upgradation of digital technology makes attackers use AI for developing advanced threats which overcomes traditional security systems [12]

Cyber criminals use AI to develop malware that adapts automatically and to make advanced phishing tool or threat and operate automated hacking tools [17]. Real-time security defense analysis by AI-driven cyberattacks enables them to adapt their plans which produces strong barriers for detection and prevention [15]. This research explores historical cyber threats along with contemporary trends and predicted AI-driven cyber-attacks and discusses suitable methods to defend against them. Especially with regard to this category, there are the so-called individual hacker, who are involved in the penetration of systems for the purpose of receiving certain advantages, or make provokes. It also means if employees and contractors who are to be trusted with the information, if they misuse the opportunity then they are dangerous to the organization. This can happen most often if a person who has some sort of power, uses that permission in a wrong manner. In all cases, cyber threats may be external and

internal and so there's need to constantly defend against them

2. Literature Review

Artificial Intelligence functions in cybersecurity as an advanced defense solution along with being an instrumental technology for creating more elaborate digital threats. The advancement of digital technology makes attackers use AI for developing powerful threats that bypass traditional security systems [6, 12, 25]. The speed of AI-based cyberattack evolution results from automated systems and machine learning and deep learning which make attackers capable of easily defeating standard security solutions [14]. Cybercriminals now use Artificial Intelligence to enhance their cybersecurity operations which enables them to execute major cyberattacks that require fewer human operators. The attackers use AI to strengthen phishing techniques and craft deepfake illusions as well as generate sophisticated malware that they perform massive cyber breaches with heightened speed [16]. Cybersecurity experts remain concerned about AI-empowered cyber threats because they require modern defensive systems which can combat the developing security risks effectively [19].

AI-controlled phishing operations emerged as one of the most dangerous cyber threats because these operational tactics have become so deceptive that detection has become more difficult [20]. Attackers employ Natural Language Processing together with data analysis to create personal phishing emails by AI which differs from generic traditional phishing methods [21]. AI analyzes social media profiles and public database information and online activity to create personalized phishing messages which cyber security systems find challenging to detect as fake communication [22]. Phishing scams achieve much higher success rates because of enhanced personalization which has made them into a major security concern for modern organizations.

A major cybersecurity concern resulting from AI technology involves deepfake technology because it generates new security risks that endanger digital identity protection. Through AI algorithms deepfake technology carries out highly realistic digital imposture creation by exactly sending persons voice alongside mimicking their facial movements and ensuring accurate digital duplications. Modern criminals use this technology for financial crime while also carrying out corporate intelligence theft along with sophisticated social engineering attacks [16]. BEC perpetrators exploit deepfake technology through audio-video forgeries for impersonation scams that trick corporate employees to send funds or release vital corporate data. Deepfake technology has reached advanced stages that cause organizations and people to lose their ability to discern real content from fabricated ones thus making cybersecurity defense systems more complex [22].

The integration of AI tools with cybercriminal tactics proves that cybersecurity threats grow more sophisticated thus requiring businesses to develop permanent security innovation platforms. AI technology progress leads cybercrime techniques to advance which demands organizations and security professionals to create better defensive solutions powered by AI. Visit the link for the full article where Wolter Buma discusses AI as the future of cybersecurity protection against evolving AI-assisted cybercriminal tactics. AI's security potential can be secured through combined effort between research communities and policy creators and technology development specialists [22].

3. Different Famous Threat in The Past

a) Morris-worm

On November 2, 1988 the Morris Worm gained its place as the first massive computer worm to spread through the early internet which was based on the ARPANET. The worm originated from Robert Tappan Morris when he developed it as a Cornell University graduate student to discover the number of networked computers. Morris did not create the Morris Worm with destructive

intent but the worm successfully took advantage of Unix system vulnerabilities through the finger command and weak passwords and send mail service to multiply itself.

The fast-multiplying worm struck 6,000 computers while it generated substantial system inefficiencies that led to an estimated $10 million financial loss. The worm duplicated automatically which created complexities for stopping its spread and resulted in system failures for all infected computers. After the initial response system administrators cut off the infected systems and created security fixes. Prosecutors charged Morris with breaking the Computer Fraud and Abuse Act which led to his receiving probation along with financial penalties.

The Morris Worm initiated vital change in cybersecurity history because it inspired the development of CERT and highlighted the necessity of network security maintenance and ethical hacking practices [3]. The incident initiated a critical stage in securing the modern digital industry.

b) I love you

The Love Bug Trojan, known as the Love Letter virus managed to spread quickly in May 1999 to become among the most famous computer attacks launched through email. The bait appeared as an ordinary love message through its subject heading "I love you" and its attachment named LOVE-LETTER-FOR-YOU.TXT.vbs. The attachment presented itself as an ordinary text file named LOVE-LETTER-FOR-YOU.TXT.vbs yet it functioned as a Visual Basic Script (VBS). Upon opening the Trojan executed the script which destroyed files and stole sensitive data such as passwords and email login details and automatically dispatched itself to all email contacts increasing its rapid transmission speed.

The worldwide impact of the Love Bug virus infected millions of PCs throughout the entire planet. The destructive damage of the Love Bug resulted in an estimated $10 billion in expenses which went toward system recovery and data restoration for infected systems as well as the cost of addressing network slowdowns. The virus caused severe email server congestion while simultaneously impacting personal computers and corporate networks thus creating an unstoppable denial-of-service (DoS) condition because email servers filling with automatically cloned messages.

The Love Bug demonstrated the risks of social engineering attacks because social engineering methods used emotional manipulation and human curiosity and affection to get users to open harmful attachments [3]. Email systems demonstrated their weaknesses during this incident since they were universally used for communication in that era. After the attack email security gained increased importance since new security procedures included antivirus software implementation as well as attachment restrictions and user education regarding suspicious communications.

c) RAT (Remote Access Trojan)

RAT is a type of malware that provide a backdoor for administrative control over the targeted computer. RATs enable intruders to do almost anything on the targeted computer, such as monitoring user behavior, accessing confidential information, activating the system’s webcam, and distributing more malware.

Furthermore, in 2009, the attack organizations used a RAT, Gh0st RAT in the targeted attacks on the organizations. As it is clearly understood this type of threat is not easy to be detected and mostly is generally treated as out of the system consideration. They allow unauthorized third parties to gain full control of the affected device and was used in espionage-based attacks.

Cisco Talos Threat Intelligence said this threat has changed, as pointed out by a malicious That could have started as early as August 2023 with a new RAT called sugargh0st [4]. The termed shows that the threat actor is currently targeting the users in the Ministry of Foreign Affairs of Uzbekistan and the South Korean citizens. SugarGh0st RAT is an improved version of Gh0st RAT trojan which is

over ten years old and has been found using new attacking sets of commands to execute the remote administrative tasks as directed by the C2 apart from the new string set that was developed due to the similar structure of the commands used in the code.

d) Ransomware

The malware known as Ransomware secures computer files from users by using encryption, so the files become inaccessible and unusable until payment is made. After encrypting the victim's files, the cybercriminal asks for money through ransom as the price for providing the decryption key that gives users access to their files. The criminals choose Bitcoin and other cryptocurrencies for ransom payments since these digital currencies allow them to stay hidden from identification.

The victim faces permanent data loss consequences when attackers set an explicit deadline for payment that must be met before they will erase the encrypted files. Data violation threats are used by attackers to disclose vulnerable information consisting of personal data or business or financial records unless the victim pays the demanded ransom. The consequences of refusing to pay can result in serious problems including legal or financial troubles which drives victims to make swift payments because non-payment can harm their reputation.

Research shows that ransomware attacks specifically target two groups consisting of both individual users and organizational targets using entry methods including phishing emails with malicious attachments and unsecured system vulnerabilities. “Cisco’s Cyber Threat Trends Report (2024) explains how ransomware attacks have transformed through attacker development of sophisticated tactics involving unmanaged vulnerability detection and social engineering strategies [4]. The payments of ransom to attackers do not always result in restored file accessibility and attackers can choose to continue exposing or selling the stolen data.

4. Present Threats

a) Dropper

Droppers represent malware created to deliver further malicious software into target systems. First impressions can be deceiving because droppers serve an intricate harmful agenda. A dropper malware operates without damaging the system directly or precipitating disruptions during its operation. The dropper category Activity levels for January went high during this cycle and maintained an upward trend throughout its time period. the end of the time frame. Droppers remain frequently reported since they perform the delivery of multi-stage malware attacks requires droppers because they play an essential part in these cyber operations. the discreet delivery of payloads. Their ability to bypass the dropper first by sets initial security measures to install additional payloads [4]. The ability of destructive malware to replicate through droppers has made this tool essential within cyber-attacks. the cybercriminal arsenal. As droppers evolve to evade the detection avoidance methodology of malicious software keeps these tools vital for multi-stage malware deployment operations [4]. infections keep them relevant.

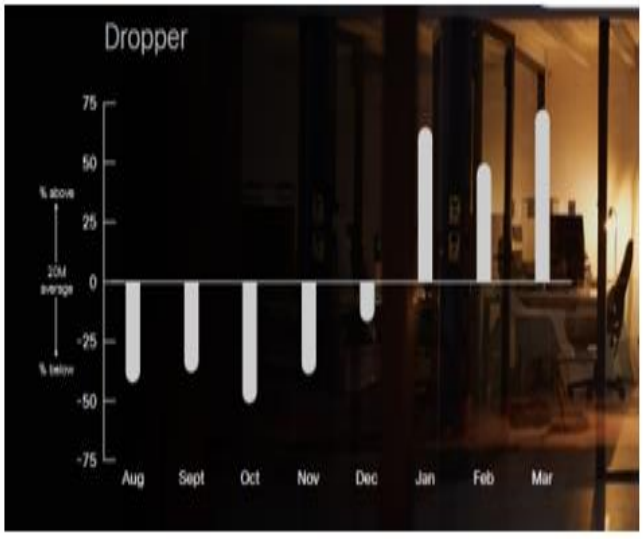

Fig 1: Chart showing the impact between 2023 Aug – 2024 Mar [4]

b) Backdoor

The software access point known as backdoor lets authorized users enter computer systems through

hidden entry systems. Users bypass typical authentication procedures to access the system because backdoors function as unauthorized access routes across network and computer systems. A computer system has several such entry points that developers create either in the software code or hardware components. Cobalt Strike is a legal penetration-testing evaluation platform which attackers misuse for malicious purposes while its developers intended it for security assessments and penetration testing. The platform contains powerful tools that attackers currently use to execute criminal actions while retaining its regular commercial use capabilities. Illegal users exploit this tool for conducting digital criminal activities. Cobalt Strike functions as a security threat because unauthorized hackers conduct attacks by abusing the proper use of its tools. Through the "beacon" payloads criminals use Cobalt Strike tools to gain remote control over infected systems. Compromised systems receive control through command and control (C2) interfaces by utilizing Cobalt Strike components that designers developed for this purpose. The malleable C2 profile system accepts portable codes which let attackers transform beacon network protocols easily. Attackers benefit from this technique by using it to manufacture beacon network traffic which matches regular network patterns thus making detection systems fall short [4].

The tool makes its actions so stealthy that network defense systems find it challenging to detect dangerous communications. The platform provides an entire collection of post-exploitation features which support privilege elevation and lateral movement and reconnaissance functions [4]. These tools serve attackers as they enable them to develop more entry points inside target networks.

Research shows backdoor incidents stem primarily from Cobalt Strike operations [4]. The majority of backdoor activity stems from Cobalt Strike use. A spike in activity the October increase in backdoor activity matches a corresponding increase in RAT activity. Analysis suggests that this peak might to the release of version 4.9 of Cobalt Strike [4]. Transparency reveals that backdoors continue to present a major threat by delivering operators continuous unauthorized system access [4]. attackers with ongoing, unauthorized access to compromised systems. Their hiding technique and persistence Long-term cyberattack data by aches become happening because of these features or function. surveillance, or further malicious activities. The strategic placement of backdoors within software or the supply chain collapses lead attackers to place backdoors through systems. These attacks prove difficult to eliminate because of their position as an enduring obstacle to system security operations [4].

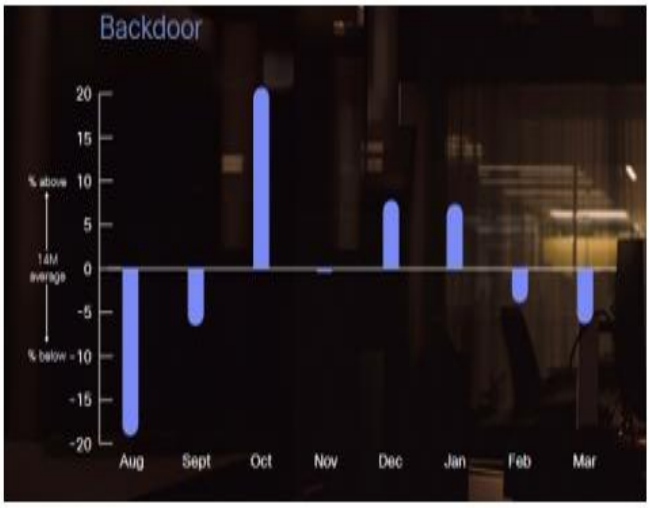

Fig 2: Chart showing the impact between 2023 Aug – 2024 Mar [4]

c) APT (Advanced Persistent Threats)

APT threats represent advanced and highly sophisticated attack methods. Special entities including organizations stand as the primary targets in specific threat operations. The perpetrators target captured states and nations to access their data or disturb their operational functions. APT threats succeed in staying undetected within networks because they persist for lengthy periods before detection [4]. Cybercriminals along with state-supported actors execute APTs with their financial backing sponsored groups.

The Russian Turla APT group actively produces threats under the name "TinyTurla-NG" (TTNG) through their threat authoring operations [4]. Research shows TinyTurla-NG shares identical characteristics with TinyTurla because both function as a tiny "last resort" backdoor inserted by Turla APT to replace other access methods [4]. When unauthorized mechanisms for system access on infected systems fail detection TinyTurla-NG remains behind as a backdoor [4].

c.1 Chart showing it impact

The classification showed 40 million blocks per month but demonstrated minimum activity fluctuations throughout the monitored time period. Members of this classification execute sophisticated cyberattacks using resources while devoting extensive time to their attacks [4]. APTs persist within the cyber threat landscape since their capability to conduct complex and discreet strikes contains strong financial and state backing from nation states and well-organized entities [4].

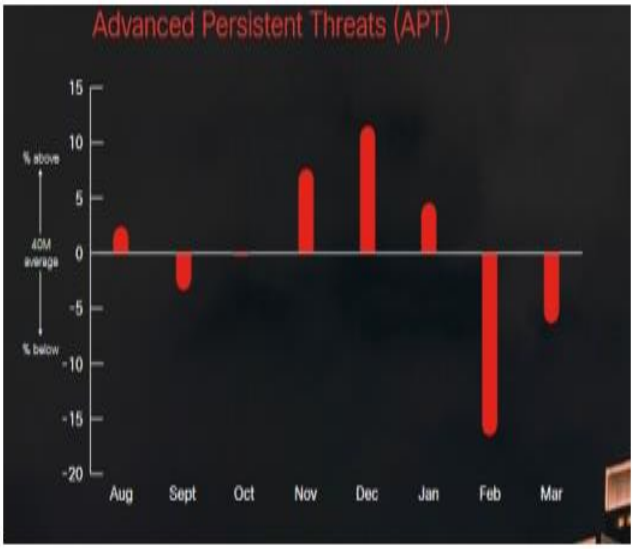

Fig 3: chart showing the impact between 2023 Aug – 2024 Mar [4]

APT threat actors maintain a long-term offensive posture toward espionage and IP theft while sustaining undisclosed network presence for months or years thus preserving a lasting platform for persistent attacks.at actors with resources, time, a dedication to carry out sophisticated attacks [4]. The prevalence of APTs exists because of their complex targeting methods combined with their secret operational style which receives state-level or sizable financial support. APS pose a long-term security threat because they focus on espionage and intellectual property theft as well as maintain their hidden presence in networks for extended periods which makes them a persistent threat in cybersecurity [4]

d) Supply chain attack

Supply chains represent attack targets for cyber-attacks that specifically exploit fragile components across industries such as finance, government and pharmaceuticals. Attackers access supply chain entities to modify both software and hardware while installing espionage components and malware. Supply chain networks experience security vulnerabilities since they connect many entities through complex networks of third-party systems that have weak integration points. Physical manipulation together with software intrusions serve as attack routes through which cybercriminals succeed in placing malware onto electronics. Major threats exist that endanger company information and manufacturing operations along with damaging business standings. Supply chain attacks grew more frequent due to globalization and decentralization became an industrial threat of serious magnitude.

Publicly available data lacks information about victim counts from either supply chain attacks or other cyber-attacks between August 2023 and March 2024. The number of victims affected depends on attack scale as well as reporting documentation shared by cybersecurity organizations. Supply chain attacks presents an ongoing upward trend in recent years [5]. Supply chain incidents continue to grow according to the 2023 Verizon Data Breach Investigations Report (DBIR) as they attack wide-ranging sectors across the globe [5]. Unprecedented information about supply chain attacks during the afore-mentioned period requires source materials from organized publications issued by cybersecurity firms such as FireEye alongside Symantec and CrowdStrike and Verizon. [5]

e) Cloud-threat

Cloud computing appeals heavily to cybercriminals and malicious actors because it continues to attract more organizations using its data storage and operational capabilities and processing capabilities [5]. Cloud threats take advantage of systemic flaws in cloud architecture designs and system configurations and service delivery models that allow attackers to breach vital cloud service and data secrecy and platform integrity and operational power [5]. Cloud computing environments constitute the primary reason for security challenges to emerge. Multiple infrastructure systems operated by cloud service customers can fall victim to an initial breach through their shared architecture model.

Cloud resources operate on demand which allows cybercriminals to make their attacks bigger and reach more users or systems quickly [5]. Cloud environments become vulnerable to attacks through weak supply chain aspects introduced by outside third-party vendors. The form of cloud threats depends both on the IaaS, PaaS and SaaS cloud service models and the security configurations that the cloud provider and users implement.

Cloud-based attackers specifically pursue cloud infrastructure weak points and unsettled software applications and dispersed data that organizations store inside the cloud through improper configuration options or inadequate security standards and unsecured application programming interfaces. [5] For 2023 intrusion rates in cloud environments surpassed the 2022 rates by 75% due to both cloud-aware (110% growth) and cloud-blind (60% growth) threats [5]. Cloud-conscious describes perpetrators who understand cloud workload vulnerabilities and exploit exclusive cloud characteristics to fulfill their malicious needs.

Symantec Loader investigations determined eCrime adversaries lead the way in cloud environment attacks since they performed 84% of intrusions compared to 16% conducted by intended intruders [5]. Traditional BGH adversaries under the name INDRIK SPIDER demonstrated increasing understanding of cloud computing throughout 2019. [5]

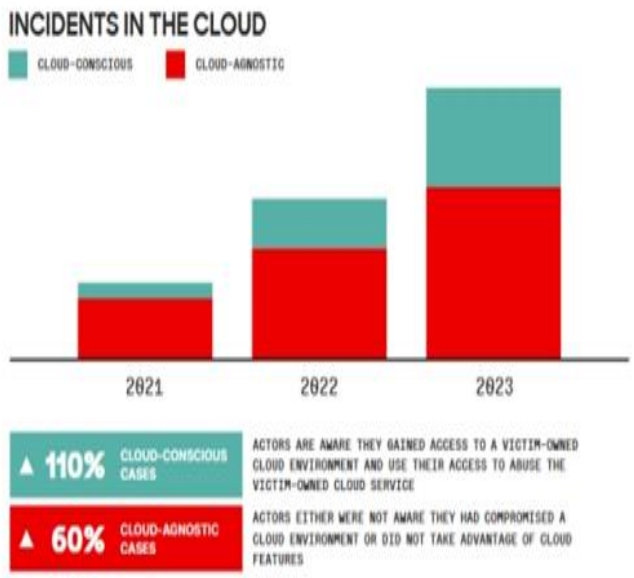

Fig 4: chart showing the impact between 2023 Aug – 2024 Mar [5]

5. Cyber Threat Empowered by Ai

a) AI-Powered Social Engineering

A hacker uses artificial intelligence to conduct extraordinary attacks on people by manipulating their disclosure of sensitive details and making them perform damaging security breaches or join illegal activities through AI-powered social engineering technologies. The main advantage AI provides in these attacks originates from its ability to work through massive datasets, which lets attackers deliver targeted tactics with compromised accuracy [7]. Very grateful to ML and NL processing alongside data extraction through scraping, AI systems can judge human behavior through collected social media activity along with communication patterns to build attacks with personalization that succeed in social engineering [7, 8]. Phishing emails together with text messages or voice calls that impersonate trusted sources like colleagues, managers, and service providers become possible because of this method.

AI tools enable attackers to produce emails with content that presents the same writing patterns as bosses while using live employment data, thus boosting the success rate of the social engineering scheme. The feature of AI tools to make deep-fake videos and voice copy allows attackers to form impressions of people whom the target really knows, such as relatives, colleagues, or friends [8]. The sophisticated impersonations made through these methods prove very authentic, so victims cannot easily tell what is real and what is fake in their communications.

An Automated attack operation, AI produce thousands of distinctive messages for individual targets, which automatically cuts down social engineering workloads. The learned adaptation capability of AI during social engineering makes this technique both self-learning and adaptable. The system improves its tactics through victim responses by modifying delivery messaging elements to maximize the success rate in real-time. When an attacker fails to extract sensitive info the first time, AI technology can rewrite the message with intensified language to pursue the victim with different tactics. These cyberattacks can be executed automatically and without human help through AI systems because AI technology provide both flexibility and scalability. Consequently, it becomes harder to detect such attacks and develop countermeasures [7, 8]. AI-powered social engineering attacks present a major threat to population and institutions because of their effectiveness, so people must learn to recognize these threats, and organizations need top-level cybersecurity defense to slow down or to stop these attacks. Creating effective defenses against AI-powered threats demands organizations to launch ongoing staff training sessions about identifying complex tactics and deploy systems capable of blocking and detecting such threats before damages occur.

b) AI Phishing attack

AI-controlled phishing operations emerged as one of the most dangerous cyber threats because these operating ways have become so deceptive that detection has become more head aching problem [20, 26]. Phishing attacks by AI is a particular case to be most considered. Classic phishing emails were often so easy to spot because of the generic content, poor grammar and awkward data-glomming which could be ebbed for. But now in AI-driven phishing this man-made threat to new length of sophistication.

Modern phishing attempts built by AI systems offer greater sophistication than those of previous years. The statement within ivy-covered frames signifies the time plus security risk reduction as PVC window frames yield maximum performance and contact opportunities. Through these systems they can reproduce writing approaches as well as scan and duplicate individual and company linguistic patterns to establish convincing impersonations.

AI systems create highly sophisticated simulation environments linked to human-related and precarious content thus resulting in higher user participation. AI systems maintain the ability to develop interactively through user responses for dynamic multi-run phishing campaigns that become tougher to remove. The cyber-criminal can manufacture and distribute numerous up to multiple hundreds of pretentious phishing messages through AI systems while putting minimal risk into execution to achieve substantial power elevation.

This amplified function has result lead to further an considerable rise in phishing attacks [9]. Over the past six months We have seen a 30% rise in business email compromise attempts, a rate similar to last year’s 200% rise in phishing attempts when that fourth quarter COVID [9]. These stats highlight a concerning trend: cybercrooks speed in during periods of turmoil and technological change; the take advantage of human psychology for their financial profit.

c) Data poisoning:

The vulnerability attacks the base structure of AI-operated systems particularly when deployed for security applications. As all AI systems need to

protect data from cyber threats need extensive datasets to discover normal routines and illegal behavior patterns. The models acquire their capacity to separate normal activities from security threats through the use of training data. Attacks on training datasets occur when malicious actors deliberately tamper with data through which AI undergoes its learning process and subsequently reduces its capacity to detect security threats properly [11]. The insertion of false data along with manipulatable examples which imitate regular network traffic could deceive AI systems into considering valid cyberattacks harmless and therefore hiding their existence.

The deception of AI through adversarial attacks leads to harmful activities that get falsely ignored because the AI system views them as typical network behavior. Attackers use adverse training examples that abuse AI learning system loopholes to generate minor data modifications that would make the system misinterpret data leading to wrong computations [11]. The degraded performance of the AI system would result in both benign threats being misclassified as hazardous conditions and extreme circumstances where dangerous activities would be treated as normal processes thereby allowing attackers to carry out their strategies without detection.

Data poisoning attacks against AI security systems represent an exceptional threat because these models provide protection to essential information networks [11]. Attackers who manage to poison the data system can control how AI operates by altering its decision capabilities which results in weakened security protocols and unknown intrusions along with weakened defense capabilities. The increasing integration of AI into cybersecurity requires complete protection of training data to maintain reliable secure systems which resist developing threats. [11]

d) Attacks on AI systems:

The intensity of dangers connected to AI increases substantially. Cyber attackers focus on the AI models by discovering weaknesses in both training algorithms along with data inputs to adjust the decision-making characteristics of AI systems which results in crucial malfunctions or complete system breakdowns [10]. An attacker can manipulate the data sensors utilize through altering camera pictures and radar system readings therefore making the vehicle AI system misinterpret environmental conditions [10]. The resulting unsafe driving conduct consists of mediocre ability to identify obstacles and pedestrians which sometimes generates accidents or collisions.

An extreme attack against AI control systems would allow perpetrators to operate the vehicle's AI functions by sending the system into hazardous steerage or forcing the disabling of essential safety components [10]. The optimization of power grid energy distribution together with responsive demand management is other tasks performed by AI systems in these networks.

Attackers exploit AI infrastructure weak points to bypass security procedures because AI models are considered independent learning decision systems [10]. The injection of harmful data into training datasets by attackers through data poisoning attacks enables them to force the AI system to produce wrong outcomes that contradict its initial objectives [11]. Critical infrastructure safety faces immediate threats from these attacks which represent growing risks during the implementation of AI technologies across different industrial sectors [11]. Preventive measures for AI-driven operations will become essential because growing complex AI software will receive control of essential operations. This need has emerged as a critical concern for governments alongside enterprises [11]. The accessibility of AI-driven systems to attackers poses threats that may result in disastrous outcomes because of this security problem being a high-priority area in the cybersecurity field [10-11].

Table 1. Shows the global impact of cyber threat over world in past and future.

Cyber Threat	Year Started	Description	Impact	Lessons Learned
WannaCry Ransomware Attack	2017	A ransomware attack that exploited Windows vulnerability (EternalBlue) to infect 200,000+ computers globally [17].	$4 billion in damage, affecting 150 countries [17].	Importance of patching vulnerabilities and securing outdated systems [17].
SolarWinds Supply Chain Attack	2020-2021	Hackers infiltrated SolarWinds' software updates, compromising over 33,000 organizations, including U.S. government agencies [5].	Estimated $100 billion in damages, major breaches in U.S. government and private sector organizations [5].	Need for Zero Trust Architecture (ZTA) and stronger supply chain security [5].
NotPetya Cyber Attack	2017	A malware attack targeting Ukrainian infrastructure, later spreading worldwide, disrupting global shipping companies [4].	$10 billion in losses, heavily impacting Ukraine's economy and causing widespread disruption globally [4].	Cyberattacks can serve as nation-state weapons in geopolitical conflicts [4].
Equifax Data Breach	2017	Hackers gained access to personal and financial data of 147 million Americans [11].	$700 million in fines, widespread identity theft and financial fraud [11].	Need for stronger data privacy regulations [11].
Colonial Pipeline Ransomware Attack	2021	A ransomware attack on the Colonial Pipeline caused significant fuel shortages in the U.S. and forced the company to pay a ransom [17].	U.S. fuel shortages, panic buying, $4.4 million paid in ransom [17].	Cybersecurity is critical for national infrastructure protection [17].
Pegasus Spyware Scandal	2016-Present	A spyware developed by NSO Group that targeted journalists, activists, and government officials, exploiting vulnerabilities in mobile phones [6].	Worldwide political fallout, espionage, and violation of human rights [6].	Need for stronger international laws against cyber surveillance abuse [6].
AI-Powered Social Engineering Attacks	Future (Emerging)	AI can create highly personalized phishing emails and deepfake impersonations, leading to financial fraud and misinformation [20, 26].	Massive financial fraud, political destabilization, misinformation, and election manipulation [20, 26].	The need to strengthen defenses against AI-powered manipulation and social engineering attacks [20, 26].
Autonomous Hacking Systems	Future (Emerging)	AI-driven malware can autonomously exploit vulnerabilities and coordinate attacks using botnets without human intervention [10].	Disabling critical infrastructure (power grids, water systems), escalation of cyber warfare [10].	Need for stronger defense mechanisms against AI-powered, automated cyberattacks [10].
AI-Powered Data Poisoning Attacks	Future (Emerging)	Attackers manipulate AI training datasets to make models malfunction, affecting decision-making processes like self-driving cars [11].	Malfunctioning AI systems, incorrect threat detection, global financial market disruptions [11].	The need for robust AI training and validation processes to prevent data poisoning attacks [11].

AI-Powered Ransomware	Future (Emerging)	AI can adapt ransomware in real-time to avoid detection, using advanced encryption techniques that make data recovery impossible [17].	Paralyzed hospitals, emergency services, and financial systems held hostage [17].	Need for AI-enhanced ransomware detection and prevention systems to safeguard critical sectors [17].
AI-Powered Cyber Warfare	Future (Emerging)	Autonomous AI cyber weapons could hack military defense systems, and AI-driven misinformation campaigns could manipulate public perception and elections [10, 11].	Increased geopolitical tensions, silent cyber warfare, manipulation of global markets through automated trading and misinformation [10, 11].	Global cooperation on AI-powered cybersecurity defense and international regulations against misuse [10, 11].

6. Conclusion

AI-based security technologies remain essential to fend off new threats that form in this current era [6]. The systems based on cyberwarfare AI function as the most advanced systems within cybersecurity domains. The maintenance people who control this technology possess significant power but unknown operators who use the system gain an even higher level of control. Part V of this presentation explains how Artificial Intelligence helps produce cyber-attacks, but technological advancements indicate ominous times since cyber-attacks become more complex and automated with adaptive capabilities. The digital community along with malware complexity now possesses autonomous capabilities to conduct attacks without needing their physical existence. AI-driven security threats are predicted to become bigger challenges in the upcoming day because they may surpass human-operated cyberattacks in size and speed [13, 24]. To fight against cyber threats deep learning-based security has become important because it enhances AI cybersecurity through better anomaly identification and predictive threat interventions [23]. The threats that feel like science fiction now persist at an increasing rate against human beings and companies as well as technological systems. As AI progresses attackers create increasingly sophisticated threats so organizations should create new cybersecurity defenses against the impending threats. AI protective measures need to become part of your organization's defense strategy together with supportive communication networks and research development toward future cybersecurity methods to fight artificial intelligence-based cyberwarfare threats. Our outcome would likely have ended tragically because of this negligent attitude if we examine the growing population concentrations in modern society.

Reference

1. https://www.nist.gov/cyberframework?hl=en-GB
2. https://www.cisa.gov/topics/cybersecurity-best-practices
3. https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats
4. learn-cloudsecurity.cisco.com/umbrella-library/cyber-threat-trends-report
5. kdpelmjpfafjppnhbloffcjpeomlnpah/https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf
6. https://darktrace.com/blog/why-artificial-intelligence-is-the-future-of-cybersecurity
7. https://www.sigmasolve.com/blog/the-future-of-ai-in-cybersecurity-emerging-technologies-and-trends/
8. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
9. https://right-hand.ai/blog/impact-of-ai-on-cyber-threat/
10. https://www.cybereason.com/blog/unlocking-the-potential-of-ai-in-cybersecurity-embracing-the-future-and-its-complexities
11. https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems#:~:text=Adversaries%20can%20d

eliberately%20confuse%20or,there's%20no%20foolproof%20defense%20that
12. Feng, Y., Li, M., & Zhang, X. (2021). AI-Powered DDoS Attacks: Challenges and Solutions. Journal of Cybersecurity Research, 16(3), 121-134.
13. Li, J., Yang, X., & Liu, Z. (2022). AI in Cyber Espionage: A New Era of Data Exfiltration. Cyber Intelligence Journal, 8(2), 45-59.
14. Liu, S., Zhang, T., & Wu, H. (2023). Polymorphic Malware and AI: A New Threat Landscape. International Journal of Cyber Security, 14(4), 78-93.
15. Rao, S., Patel, R., & Wang, J. (2020). Machine Learning in Evasion Techniques for Cybersecurity. AI & Security Review, 10(1), 67-80.
16. Sood, A., Gupta, P., & Kumar, R. (2022). Deepfakes and AI in Cybercrime: The Growing Threat of Voice Phishing. Journal of Digital Forensics, 4(2), 102-115.
17. Zheng, Y., Chen, T., & Li, J. (2020). AI-Powered Cyber Threats: A Review of Modern Challenges. Cybersecurity Advances, 7(1), 50-62.
18. Zhang, H., Li, Y., & Wei, L. (2022). AI in Ransomware: Evolving Strategies and Defenses. Cybersecurity Technologies Journal, 18(2), 56-72.
19. Chen, X., Wang, Y., & Liu, H. (2023). AI-Driven Cybersecurity: Opportunities and Challenges. Journal of Information Security, 19(1), 55-72.
20. Patel, R., & Sharma, K. (2023). The Role of Deep Learning in Cybersecurity. Cyber Intelligence Journal, 10(3), 80-97.
21. Anderson, M., & Lee, J. (2023). AI and Cyber Warfare: Future Threats. Defense Technology Review, 15(2), 112-130.
22. Brown, P., & Thompson, G. (2023). Cyber Threat Evolution in the AI Era. International Journal of Cybersecurity, 11(2), 45-62.
23. White, D., & Green, B. (2023). Phishing Attacks and AI-Based Defense Strategies. Cybercrime Studies Review, 8(4), 76-91.
24. Kumar, V., & Singh, R. (2023). Ransomware and AI: The Next Generation Threat. Cybersecurity Advances, 9(1), 34-50.
25. Nelson, A., & Parker, T. (2023). AI-Enhanced Botnets: Emerging Risks. Journal of Digital Security, 17(3), 88-104.
26. Williams, J., & Roberts, C. (2023). The Future of AI in Ethical Hacking. Cyber Threat Intelligence Journal, 12(2), 99-115.