iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

# AI-POWERED CYBERCRIME: THE NEW FRONTIER OF DIGITAL THREATS

**Shoeb Ali Syed**
**University of the Cumberlands**

**ABSTRACT**

Cybersecurity is not an exception of the various fields that have been influenced by the advancement of artificial intelligence hence its evolution. Nevertheless, AI is also used by hackers for the increasing number, scale, and efficacy of their attacks. This paper therefore defines AI Cybercrime as automated phishing, AI malware, social engineering and cyber espionage, which are new form of threats that affect persons, organizations, and governments. This paper focuses on investigating AI-assisted cyber threats, knowledge and tools of an attacker, as well as defenses against threats and attacks. Applying threat detection systems with the help of artificial intelligence, ways and means of machine learning-based anomaly detection, and interaction between a human and an AI are discussed as some possible countermeasures. These small examples of AI applications in phishing, ransomware, and espionage have raised a call for robust and evolving cybersecurity measures. The results also state the fact that AI acts as a potential threat as well as having the capability to deal with threats effectively, thus requiring constant R&D in AI security.

**Keywords:**
AI-powered cybercrime, Machine learning in cybersecurity, AI-driven phishing attacks, Cybersecurity threat detection, AI-based cyber espionage

## 1. INTRODUCTION

### 1.1 Background

Artificial intelligence is a relatively new field that has grown and changed many industries to incorporate great automation, opportunities for analysis and optimization in various fields. AI technologies have helped improve leading sectors of the global economy such as health, finance, production and so on. Yet though it has lavished benefits, it introduced many new issues, the most important of which in the domain of cybersecurity. Now, AI is being used by attackers to plan, execute and optimize attacks, and to bypass security solutions. Through incorporation of artificial intelligence in cybercrime, crime has evolved to the current level where artificial intelligence is used in crime, highly scalable, intelligent and difficult to counter. Whereas the traditional cyber threats, AI cybercrime uses the capability of the machine learning system to make the phishing emails look very real, generate fake news for the purpose of ripping people off, to propagate the malware on the systems and make spying more sophisticated. Since AI technologies are becoming more and more sophisticated, so is the domain of cybercrimes and, therefore, it is high time to discuss the phenomena of and goals of AI cybercrimes. It is critical for the creation of effective countermeasures to guard against such threats as AI continues to advance.

### 1.2 Motivation

The importance of AI in the cybercrime domain is rooted in the fact that it creates more unalike threats to the digital environments. In general, the current protective methods and techniques used in cybersecurity, including rule-based methods and signed-based approaches, are not able to cope with AI based cyber threats that are constantly evolving. Artificial intelligence enhances the effectiveness of cyberattacks since it leads to real-time decisions by the attackers. Cybercriminals do use AI for current attacks and can create highly targeted and scalable attack vectors, for example, artificial intelligence spear phishing and automated hacking that can penetrate most of the contemporary security systems. On the same note, there is increasing authenticity of deepfake content by AI to compromise the credibility of verified information and identities. Through artificial intelligence, cyber threats such as exposure to sensitive data, financial crimes, and lack of reputation enhance considerably in organizations and individuals. Therefore cybersecurity, venture, and other regulatory authorities must extend their attention in the research and prevention of AI cyber-crime leading to mass causalities. Identification of these threats will enable formulation of appropriate counter measures that will address the dangers posed by terrorism and other attacks succeeding through AI.

### 1.3 Research Question

This work presents the problem, which stands as follows: how is AI is applied in cybercriminal activity, and what measures should be taken to prevent AI-based threats? In this regard, in responding to this question the study intends to explain the dynamics of AI cybercrime, how cybercriminals leverage AI in actualization of attacks, and how best they used AI to avoid identification. The study also looks at the possible measures that can be taken by the organizations as well as research in security to prevent these new-age threats. AI cybercrime is an exciting and dynamic field, which means that it is high time to familiarize with this subject to speak of the formation of effective preventative measures. Based on the findings obtained from analyzing AI-based cyber threats and risks, this research aims at filling the gap between the progress that has been made in the development of cybersecurity and the progression of smart and new AI- based threats. The findings will be of significance since they will provide a detailed approach of how the existing security measures can work hand in hand with AI measures to prevent AI-enhanced cybercrime.

### 1.4 Scope and Limitations

This study is centered on the following categories of AI-based cybercrimes, namely phishing attacks executed by AI, rampaging malware AI, social engineering, and AI hacktivism, and cyberespionage. It assesses how AI is used for evil purposes by hackers for carrying out unprecedented and tailored Cyber-attacks with little interactions. The paper also explores how the given type of AI is used to commit cybercrime, including machine learning-based attack automation, deepfake creation for fraud, and AI-assisted data theft. Also, the study considers various techniques such as AI-based threat identification systems and adversarial learning techniques to determine real-time anomalies. However, this study does not offer a real-time experiment and even the

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

countermeasures that may be implemented during operations. However, it leans on only theoretical and empirical literature, other case studies as well as the assistance from the experts to offer a detailed on the AI-Enabled Cybercrime systems. Although the paper is general in exposing all relative AI threats in cyber security, it does not exhaust all categories of AI when it comes to cybersecurity since the world develops new applications every other day. The findings also endeavor to provide the security researchers and planners with basic knowledge about the rise of new AI-related cybercrime to prevent the future attacks effectively.

## 2. LITERATURE REVIEW

### 2.1 Cybercrime

Cybercrime relates to activities perpetrated using information technology with an aim of offending individuals, organizations or a specific government. In the past, such threats comprised phishing, malware, ransomware, and the well-known DDoS assault. Earlier, hackers used only tech tools and features on machines as weapons in the battlefield; however, with the emergence of artificial intelligence (AI), which has predictive and generative functions, attackers may use them to upgrade their technical power. Today advanced AI cyber threat has become more versatile, flexible and efficient and is almost impossible to counter.

For instance, through AI, phishing attacks has escalated to the next level and thus businesses should prepare themselves. Machine-generated phishing e-mails may also effectively imitate the normal messages produced by people as they mimic the kinds of writing produced by the users. In a similar vein, malware and ransomware are capable of learning security measures by changing the code of the used algorithms. AI can also be used in botnet attack to attack large number of targets and drive out more traffic to{}". Such trends demonstrate that AI has taken cybercrime to another level where it is more challenging and enduring than before.

### 2.2 Artificial Intelligence (AI)

AI is a vast computing domain that is inclusive of ML, DL, and NLP processes through which machines have the capability of learning as well as interpreting the aspect of cognition relevant to human beings. AI programs are designed for real-time data processing, pattern recognition and data decision making that makes them appropriate in both cybersecurity and in the commission of cybercrime.

In defense, use of AI is adopted for functions such as threat identification, categorizing the behaviors, and responding to the threats. AI-driven security solutions are capable of the extrapolation of threats and risks, identification of disturbances and adverse events, as well as minimization of threats in real-time. Nonetheless, AI is also exploited by cybercriminals to automate processes such as attacks, avoidance of various measures, and other procedures related to malicious actions. For example, AI-based password cracking tools can assess hacked passwords and create most likely passwords with a high degree of accuracy. The NLP processing based chatbots are also being used in scams with the use of fake identities with the aim of extorting sensitive information from the gullible victims.

### 2.3 AI-Powered Cybercrime

In this case, cybercrime augmented by artificial intelligence is the use of the AI to the intensification of situ, speed, and flexibility of computer and internet-based crime. Cybercriminals employ AI in various ways, such as AI-driven malware, deepfake scams, and autonomous hacking systems. For example, deep fake creates fake audio and video presentation which make criminals impersonate the real people to perpetrate fraud and spread fake news.

AI and ransomware specifically are dangerous as the former can change its program code on their own. These are advanced threatening attacks that utilize even superior AI techniques on the sophistication of their coverage which makes it harder for traditional ways of security to impede them. Moreover, hackers use artificial intelligence techniques in social engineering attacks to study different large sets of data to make scams look more real for users and thus hard to detect.

According to the second source, another type of AI cybercrime is autonomous hacking. Examples of an AI hacking tool are the capability of autonomous hacking by putting together packages that can probe, penetrate and invade computer networks, and carry out various cybercrimes within a short span of time without being hindered by the standard human limitations such as time and energy. It makes the process of a breach faster and outpaces security teams, as they cannot efficiently manage such high speed and efficiency of hackers.

### 2.4 Existing Solutions

There are several AI-assisted security frameworks existing to tackle AI based cyber threats. Such are the IDS, anomaly detection, and the response generators that are associated with artificial intelligence technology. That is because, using artificial intelligence, security systems can monitor appearances in networks, recognize changes in their work characteristic, and in real-time establish possible threats.

The anomaly detection algorithms are pivotal important because of their ability to interpret large datasets and come up with the potential ill-natured behaviors. Further, automated response measures of the cybersecurity systems allow threats to be countered without any human intervention. That is why the use of AI as security measures contributed positively to the fight against cyber threats; however, they are not always capable of matching AI strategies that are still developing.

Though these have improved the security measures to protect the systems, due to the advancing AI based threats in the cyber world there is always a need for enhancement. Aided by a never-ending inspiration pool that is cybercriminals; the field of cybersecurity is ever evolving with the need for artificial intelligence in solving modern day hacking techniques.

## 3. TYPES OF AI-POWERED CYBERCRIME

### 3.1 AI-Generated Phishing Attacks

Phishing attacks in general, have been a critical issue since this kind of attacks have existed for many years now, however, due to the advancement in technology, especially the integration of artificial intelligence, the phishing attacks have become more prevalent and complex. However, the conventional form of phishing entails sending email or message with the intention of tricking the target into parting with personal information. However, AI phishing goes even further as it applies artificial intelligence and natural language processing to create vastly realistic messages that tend to look very much like business ones. These AI driven attacks can then use yearly, day, month, context of previous communication, style of writing in order to make the new communication more accurate. Finally, AI allows for mass emails to be used for phishing alongside changing the content of mass emails to link to the phishing emails based on the recipient's answers to give a better chance for success. It is also observed that voice phishing or vishing is also prevalent; with the use of voice synthesis, it has become easy to imitate people over the phone.

### 3.2 AI-Powered Malware and Ransomware

Malware and ransomware have, in the past employed set code and methodology which gives them a certain level of predictability and are thus easier to combat using signature-based analysis. However, with the emergence of AI-controlled malware it has become an issue of its own kind, as such programs are capable to modify and improve themselves based on cybersecurity counteractions. These make it possible to these malicious programs to analyze and learn the security measures that exist in a system and adapt themselves in real time as they launch their operations on the system. It is also possible to combine AI with the generation of new versions that an antivirus cannot detect using generative adversarial networks (GANs). In the ransomware attacks, the use of AI has made great progress in the encryption the best way to even encrypt the data to a level where decryption was impossible without the key from the attacker. Furthermore, AI can identify which systems to extort within the network and when would be the optimal time to do this since during the time of traffic load which is high or when files more vulnerable.

### 3.3 AI-Driven Social Engineering Attacks

This sort of attacks involves manipulation of the human mind to extract as much information as possible from victims. They have been improved more by AI in the sense that it is possible for cybercriminals to make human like responses that are contextually relevant. For example, AI-powered chatbots can converse credibly with the targets convincing them that they are talking to a representative of a company or a co-worker. Another powerful tool in this sphere is deep fake, which is a technology for creating fake audio and video based on Artificial Intelligence. Dark web scammers produce fake recordings of the leaders, politicians, or any other prominent personalities, including business magnates, and make people fall for it to get some money or leak important information. These manipulations make the techniques of social engineering much more effective and challenging to discover.

### 3.4 AI-Based Cyber Espionage

Cyber espionage it is a process of trespassing into the networks and systems of other, in other to gain classified or sensitive information that could be of politically, militarily or economically useful. With the help of AI, cyberspace espionage has become more efficient due to automation of the reconnaissance, identification of weaknesses and the actual attack. The automation of espionage tools makes it easier for the program to process large amounts of data, discover vulnerabilities within an organization's system and launch attacks on that system with little supervision. Governments and cybercriminal organizations use AI to perform reconnaissance, phishing attacks, and take advantage of vulnerabilities that are yet unknown to developers or vendors. Nevertheless, AI can imitate the creation of fake social media accounts and interact for an extended period in order to take as much information from a target individual. These features make AI as a tool for cyber espionage War an important factor to be considered by security and intelligence services at national and corporate level.

## 4. TECHNIQUES AND TOOLS USED IN AI-POWERED CYBERCRIME

### 4.1 Machine Learning (ML) Algorithms

Artificial intelligence is one of the essential components of the computerization and optimization of cyber-attacks. The utilization of Cybersecurity means that cybercriminals have been using the power of ML to process large datasets, recognize the nature of the security risks and improve the strategies that encompass them without requiring human input much. Self-learning malwares are developed using the similar features to gain capability to evolve on their own and hence, learn how to avoid common security detection methods. Also, the attackers apply sophistication of the algorithm to improve the password-cracking techniques by predicting the popular passwords in a precise manner.

| ML Technique | Function in Cybercrime |
|---|---|
| Supervised Learning | Enhances phishing email classification to bypass spam filters |
| Unsupervised Learning | Identifies system vulnerabilities by clustering weak security patterns |
| Reinforcement Learning | Adapts malware behavior to avoid detection |

***Table 1: Machine Learning Techniques in Cybercrime***

### 4.2 Natural Language Processing (NLP) Techniques

NLP makes it relatively easy for the attackers to create very efficient and elaborate message delivery and obvious scam messages. NLP and AI, today, enables the reproduction of realistic mailing, tweets, social network posts, even fakes voice calls and conversations impersonating individuals or organizations. It enables cybercriminals to avoid spam filters and get past peoples' initial disbelief with more successful phishing scams. Furthermore, AI chatbots can be engineered to have conversations with clients that essentially involve conning them, thereby getting private information from them.

### 4.3 Deep Learning (DL) Models

The cybersecurity threats benefit from DL because it makes the attacks more accurate, flexible, and stealthy. In DL technology, models are developed by feeding systems with vast amounts of data with an intent to learn patterns in regard to the security systems and to independently design and develop new strategies. CNN and RNN are the primary tools of hackers that enhance the malwares' capabilities, create more realistic deep fakes, and bypass security measures. For instance, generative adversarial networks (GANs) allow for the creation of very realistic image and videos which are in turn used in misinformation and identity theft cases.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

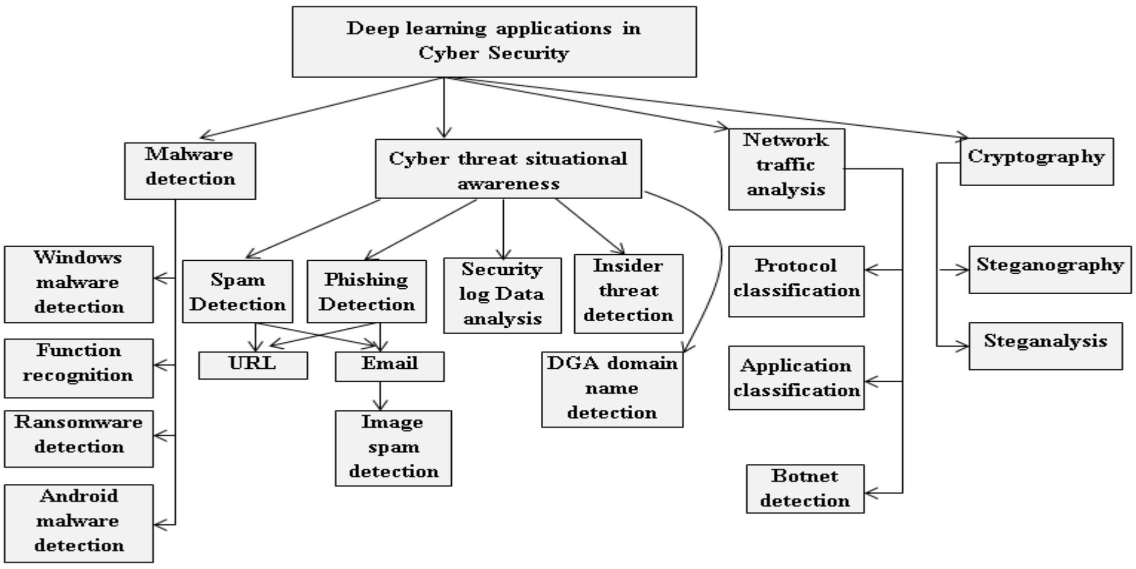

*Figure 1: Deep Learning in Cybercrime*

### 4.4 AI-Powered Exploit Kits

These are software tools that contain several tools designed to take advantage of any vulnerability that is ascertained in a particular computer network. Thus, AI-built exploit kits improve this process using analysis of system vulnerability and targeted attacks based on it. These kits possess the ability to run through the networks to identify software that have not been updated, insecure security settings, and exploitable vulnerabilities. Thus, when a target is found, an AI-driven system goes for an attack exploiting the vulnerability, thus making it easier for a hacker to invade.

In general, AI aids the work of cybercriminals, which is why cybersecurity shall work on the creation of AI-based tools for defense. The ongoing contest between new AI-enhanced threats and AI-assisted security solutions remains a general pattern of the development of threats.

## 5. DETECTION AND MITIGATION STRATEGIES

The more the AI threats increase, therefore, the more detection and counter strategies must also develop to be able to flexibly combat these threats. It has also been pointed out that the traditional security protection modalities are insufficient to protect organizations against AI-backed threats hence the need for AI-protected security features. The integration of threat detection systems, AI capacity, using machine learning approaches to detect anomalies, and using an automated incident response system along with human AI collaboration forms part of the contemporary security model.

### 5.1 AI-Powered Threat Detection Systems

Several AI based threat detection systems analyze the behavior and alert users of AI enabled cyber threats in real time. These systems work in the sense of analyzing the network traffic and logs, as well as the activities of the users to look for symptoms of malicious activities. It is an advanced security approach as compared to the traditional security based on signatures since it uses the capability of analyzing to predict and shield dangers before it attacks the system.

Another major beneficial effect of AI solution adoption in threat detection is that it possesses change agility. The cybercriminals often change their tactics and methods in order not to be detected with the help of usual rules. AI-based, on the other hand, rely on machine learning algorithms; the models are refined with the help of new threats identified all the time to increase the efficacy of threat detection.

### 5.2 Machine Learning-Based Anomaly Detection

In the presented context, the relevance of anomaly detection based on machine learning approaches is the ability to detect behaviors that signify cyberattacks initiated by AI technologies. A traditional security solution utilizes sequential analysers with specific rules by which prospective threats are identified; as for ML anomaly detection, no rules are used as activity variations from usual patterns are apropos.

Supervised learning models are trained on controlled datasets that contain samples of known threats so that they will be able to detect suspicious patterns. As for unsupervised models, they consider extensive data in the network without labeling them and are therefore useful in identification of new emerging attacks.

One of the most important use cases of ML-based anomaly detection is in the financial transaction security; customers' behavior is detected for any fraudulent transactions. For instance, an artificial intelligent system in the banking sector used for monitoring transactions can alert the user when there is an irregularity of spending by the account holder. Likewise, in corporate networks, there is the ability to use ML-based solutions in determining cases of unauthorized access and data exfiltration.

### 5.3 AI-Driven Incident Response Systems

Automated incident response is the use of artificial intelligence in cybersecurity to respond to threats to handle them and reduce loss. They incorporate artificial intelligence used in the decision-making process in relation to the attack simulation, identification of the optimal countermeasure, and the performance of the remedial measures.

For example, in the event of an AI-driven ransomware attack, an incident response system using AI can recognize the activities of file encryption in a computer system, stop it and replace the affected files and data with the backed-up ones soon after the attack erupts.

### 5.4 Human-AI Collaboration for Cybersecurity

Even though AI contributes to the protection against cyber threats, there are no substitutes for the analyst. When it comes to cybersecurity, the best top patterns combine professionals and solutions that apply artificial intelligence.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

The major problem in using AI in cybersecurity is that it is easy to generate false positives and at the same time, attackers can train the algorithms to act in a particular way. The second is targeted at using human analysts to provide a final check for the models and to handle alerts that cannot be handled by AI because of the context in which they are generated.

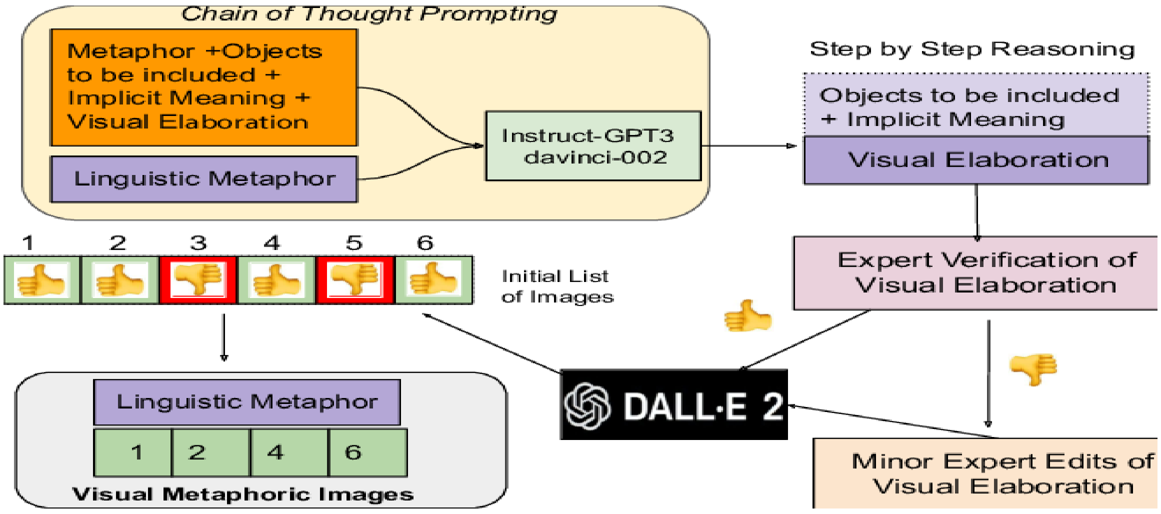
Chain of Thought Prompting
Metaphor +Objects to be included + Implicit Meaning + Visual Elaboration
Linguistic Metaphor
Instruct-GPT3 davinci-002
Step by Step Reasoning
Objects to be included + Implicit Meaning
Visual Elaboration
Expert Verification of Visual Elaboration
1 2 3 4 5 6
Initial List of Images
DALL·E 2
Minor Expert Edits of Visual Elaboration
Linguistic Metaphor
1 2 4 6
Visual Metaphoric Images

*Figure 2: Human-AI Collaboration Framework for Cybersecurity*

## 6. CASE STUDIES AND REAL-WORLD EXAMPLES

### 6.1 AI-Powered Phishing Attacks on Financial Institutions

The financial institutions are the most vulnerable to phishing attacks through AI because of the large volumes of customer information and transactions. The common type of phishing attempt is the use of multipurpose emails and messages aimed at pretending to be of a different organization or individual. However, AI uses NLP and machine learning techniques to create very convincing messages that are delivered individually to the targeted user.

For instance, in a recent case, an international bank faced this threat where the hackers used the strategies of sending the actual message like phishing emails that resemble the way the executives of the bank write. The AI was able to study emails, activities of the employee's and transaction history to prepare emails that would look genuine. Users as usual shared their login details, thus allowing unauthorized access of the customer's profile by the intruders. It is for this reason that organizations must turn to AI-based security systems, which can effectively identify such latest phishing scams.

To curb the cases of phishing that utilize AI, the financial institutions have deployed the systems that utilize AI in the identification of the unusual patterns in the emails. Furthermore, on how they can be mitigated, security knowledge of employees, and multi factor authentication are important in lowering the success rate of phishing scams.

### 6.2 AI-Driven Ransomware Attacks on Healthcare Organizations

The healthcare sector has become a lucrative area for the use of AI for ransomware attacks since many healthcare organizations have depend on digital platforms for patient data. AI helps ransomware emerge through live changes in approaches of operation, higher efficiency in gaining access and encryption of data.

A documented case of a health system giant falling victim to extortion ware using AI was performed through an identified weak area in their old web application software. This malware rapidly established and target patient record data mentioned above and bypass the existing security systems. The hackers demanded a large amount of money in bitcoins to unblock the information, and Caledonia Obama hospital had no option but to thaws off essential functions and postpone treatment.

They are using AI-based solutions for the prediction of the access pattern that the ransomware might use before it can deliver a payload. Other measures that help to reduce the harm caused by ransomware attacks include regular update of the software, deployment of the network segmentation, use of the endpoint detection and response (EDR) systems that employ artificial intelligence.

### 6.3 AI-Based Cyber Espionage on Government Agencies

Federal agencies are more vulnerable to cyber espionage attacks by artificial intelligence in attacks that are mounted by agents of other nations. That is why, today, based on artificial intelligence, opponents can carry out extensive data collection, organize effective reconnaissance and use modern malicious programs that can remain unnoticed for a long time.

One of the most striking examples is a government defense agency that was targeted with the help of AI cyber espionage. The hackers deployed AI malware, which was intelligent and configured to its environments, stole classified files, and sent them through an encrypted means. The AI-driven malware was active for months in carrying out its operation of stealing defense strategies and national security information.

To counter AI in espionage, the government authorities are using AI security systems that can detect threats in large amounts of data. Espionage threats can best be prevented and mitigated with help of the zero-trust security models, threat intelligence sharing and real-time AI-assisted monitoring.

| Case Study | Target Sector | Attack Method | Impact | Countermeasures |
|---|---|---|---|---|
| AI-Powered Phishing | Financial Institutions | AI-generated phishing emails | Credential theft, financial loss | AI-driven anomaly detection, MFA, employee training |
| AI-Driven Ransomware | Healthcare Organizations | AI-enhanced ransomware | Data encryption, service disruption | Predictive analytics, EDR systems, regular updates |
| AI-Based Cyber Espionage | Government Agencies | AI-automated malware | Classified data theft, intelligence breach | Zero-trust security, AI-assisted monitoring, threat intelligence sharing |

***Table 2: Summary of AI-Powered Cybercrime Case Studies***

## 7. CONCLUSION

### 7.1 Summary of Key Findings

With the help of AI, cybercrime became even more dangerous – increased in terms of complexity, ability to scale and harder to prevent. The AI-based threats are not how static like other cyber threats, which makes them almost impossible to be addressed by existing security solutions. This can be done through utilizing the natural language processing or artificial intelligence in coming up with some of the phishing messages which in form and content can easily look like they are from genuine senders. Likewise, AI malware/ransomware employ 'learning techniques to self-evolve and bypass the security systems' while AI social engineering attack the human mind on a much larger scale. In addition, the AI-based cyber spying has also been used in the past by organizations that are sponsored by different governments in the world and other cybercriminal groups to hack into secure networks and then steal authorized information. With an improvement in AI abilities, the cybersecurity threats must be addressed to ensure they can be dealt with sufficiently.

### 7.2 Contributions

This paper therefore aims at describing the advanced capabilities of cybercriminals by analysing the assets and methods utilised in AI cybercrime. By understanding the chances of artificial intelligence in the emergence of new threats such as AI based phishing, AI generated malware, based social engineering attacks and AI driven espionage, this paper aims at furthering the knowledge of the changes in the threat spectrum. Besides, the research focuses on the detection and prevention techniques and approaches such as artificial intelligence threat detection system, machine learning anomaly detection, artificial intelligence-driven incident response, and human computer interaction in cybersecurity. These are fine reference points on the advancement of more effective security measures in addressing AI-backed cyber threats.

### 7.3 Future Work

Current AI solutions in securing against AI cybercrime have some effectiveness, therefore further investigation is needed to enhance the security mechanism. Next research avenues should include improving AI defense capabilities, designing online threat identification strategies, and incorporating the government policies that relate to AI security threat. However, there is also a need for international cooperation and suitable guidelines as to how artificial intelligence can be used in the field of cybersecurity. Incorporating proactive work and sound policies, constant development of AI technology will require vigorous approaches to challenge such threats as AI cybercriminal.

## REFRENCE

[1] Shalaginov, A., Kotsiuba, I., & Iqbal, A. (2019, December). Cybercrime investigations in the era of smart applications: Way forward through big data. In *2019 IEEE International Conference on Big Data (Big Data)* (pp. 4309-4314). IEEE. https://doi.org/10.1109/BigData47090.2019.9006596

[2] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber-attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254

[3] Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv preprint arXiv:1502.03552*. https://doi.org/10.48550/arXiv.1502.03552

[4] Al-Jabban, M. O. (2021). AI-Powered Threat Detection in Cybersecurity Infrastructures. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(3), 1-8. https://doi.org/10.63282/00gwya15

[5] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), e1306. https://doi.org/10.1002/widm.1306

[6] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57-106. https://doi.org/10.1177/1548512920951275

[7] Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats: Research and Practice*, *4*(1), 1-38. https://doi.org/10.1145/3545574

[8] Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In *SoutheastCon 2017* (pp. 1-6). IEEE. https://doi.org/10.1109/SECON.2017.7925283

[9] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254

[10] Veprytska, O., & Kharchenko, V. (2022, December). AI powered attacks against AI powered protection: classification, scenarios and risk analysis. In *2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1-7). IEEE. https://doi.org/10.1109/DESSERT58054.2022.10018770

[11] Yeoh, P. (2019). Artificial intelligence: accelerator or panacea for financial crime?. *Journal of Financial Crime*, *26*(2), 634-646. https://doi.org/10.1108/JFC-08-2018-0077

[12] Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(3), e1394. https://doi.org/10.1002/wfs2.1394
[13] Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36-51). IGI Global. DOI: 10.4018/978-1-5225-9715-5.ch003
[14] Sewak, M., Sahay, S. K., & Rathore, H. (2021, October). Deep reinforcement learning for cybersecurity threat detection and protection: A review. In *International Conference On Secure Knowledge Management In Artificial Intelligence Era* (pp. 51-72). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-97532-6_4
[15] Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10*(5), 055-060. https://doi.org/10.53555/ephijse.v9i3.211
[16] Sornsuwit, P., & Jaiyen, S. (2019). A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting. *Applied Artificial Intelligence*, *33*(5), 462-482. https://doi.org/10.1080/08839514.2019.1582861
[17] Hassib, B., & Shires, J. (2022). Cybersecurity in the GCC: From economic development to geopolitical controversy. *Middle East Policy*, *29*(1), 90-103. https://doi.org/10.1111/mepo.12616
[18] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(5). https://ssrn.com/abstract=4323258
[19] Ranade, P., Piplai, A., Mittal, S., Joshi, A., & Finin, T. (2021, July). Generating fake cyber threat intelligence using transformer-based models. In *2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-9). IEEE. https://doi.org/10.1109/IJCNN52387.2021.9534192
[20] Ling, L., Gao, Z., Silas, M. A., Lee, I., & Le Doeuff, E. A. (2019). An AI-based, Multi-stage detection system of banking botnets. *arXiv preprint arXiv:1907.08276*. https://doi.org/10.48550/arXiv.1907.08276