24. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Tsurko V. E.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Shaputko A. V. – Lecturer, Master of Arts (Philology)

This paper examines the influence of the neural network on cybersecurity. Their combination (artificial intelligence and cybersecurity) has many different aspects of application. The use of machine learning methods is naturally common, but the tasks and results achieved to date are completely different.

Today the role of artificial intelligence in any field of activity is significant. Many are concerned about the security of deploying this technology, as almost no one understands the encryption of user data or the company's neural network.

Cybersecurity is the protection of digital data, networks, and devices from unauthorised access, attacks and information leaks. The digital world is becoming more complex every year, and cyber threats are becoming more sophisticated. Hackers use advanced attack techniques that require new solutions to detect and prevent them. Artificial intelligence plays a key role in today's cybersecurity allowing us analyse huge amounts of data, detect anomalies and block suspicious activity in real time.

Cybersecurity tasks include preventing and detecting attacks, investigating and analysing threats, and training and modeling systems. Attack prevention is an effort to reduce the number of vulnerabilities contained in software [1].

Deep learning is also actively used in the area of android malware detection [2]. This paper outlines a system developed through funding provided by the Chinese government's grant for key technological advancements. One study presents a comprehensive comparative analysis of deep learning models for detecting malicious applications. The research demonstrates that the proposed deep learning architectures outperform classical machine learning methods in terms of accuracy and efficiency in identifying malware. The authors also address data bias and propose a hybrid approach that combines static, dynamic, and visual analysis methods for malicious code detection [3]. All such works have practical applications; for instance, Microsoft 365 Defender leverages deep learning algorithms to enhance its capability to identify and mitigate threats effectively [4].

Attack detection involves identifying suspicious behaviour and reporting it as it occurs. The goal is to respond attacks quickly, including determining the magnitude of attack, closing the entrances for attackers and eliminating vulnerabilities (backdoors, etc.) that could be exploited by the attacker.

Obviously, searching for unknown attack patterns can potentially lead to a large number of false positives [5]. The generally accepted opinion is that the main problem with detecting suspicious activity is precisely to find the right balance between ensuring sufficient coverage by seeking accurate security warnings and the number of false alarms.

The following areas can be highlighted regarding the use of machine learning for attack warnings:

1) priority setting for warnings of potential attacks [6];

2) recognising multiple hacking attempts over time that are part of larger and longer-term hacking campaigns [7];

3) detection of malicious software activity, both within the computer and in the network [8];

4) the identification of a malicious software stream being deployed through a particular organisation. These are so-called Living off the Land (LotL) attacks – cyber attacks in which the attacker uses legitimate software in the organisation to perform an attacking action [9];

5) identifying automated approaches to mitigate the consequences of attacks when rapid response is required to prevent the spread of an attack. For example, an automated system can disable network connection and block the device if a sequence of warnings is found which is recognised as being associated with ransomware activities [10].

Artificial intelligence techniques are also used in high-level threat analysis. Among other things, neural networks are used for cyber-hacking, including for the evaluation of existing security systems. The term offensive AI is associated with carrying out attacks. Figure 1 provides an overview of the attack vectors using machine learning systems on the MITRE threat matrix (Adversarial Tactics, Techniques, and Common Knowledge) – open database of cyber tactics, techniques, and procedures (TTP), developed by MITRE. It helps cybersecurity professionals analyse the cyber threats, develop protection strategies and identify threats.

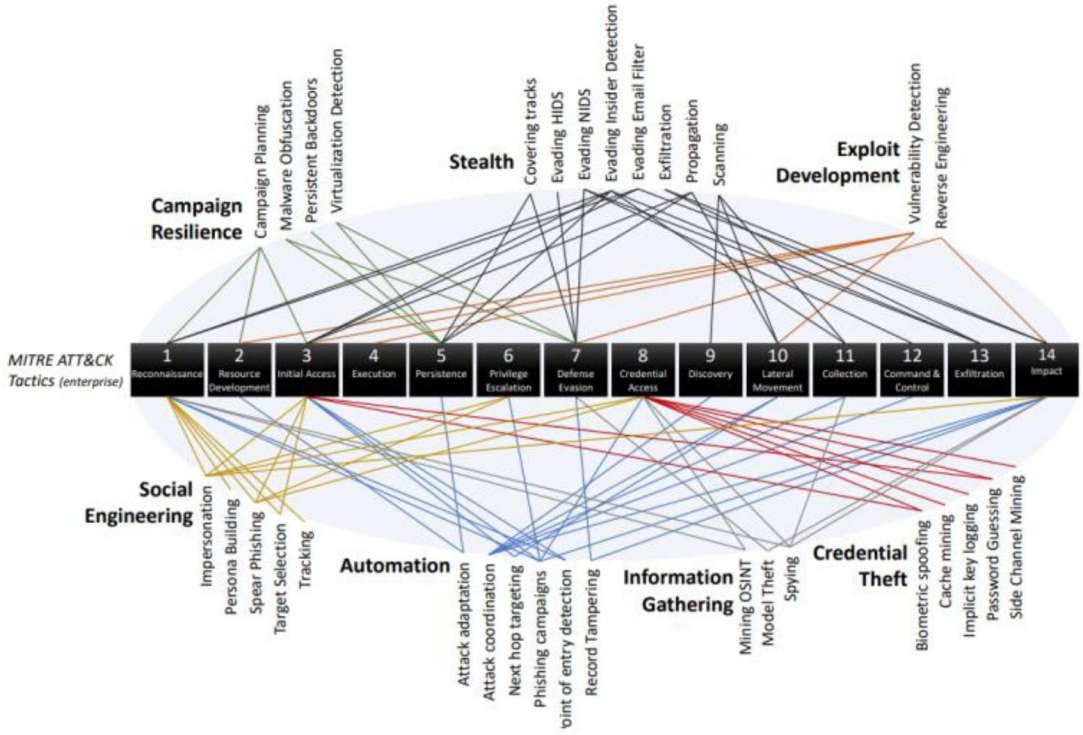

Figure 1. Machine learning in cyber attacks. Areas of attacks using AI

We can look at the tools that protect against cyber threats without using artificial intelligence. Product categories include:

1) intrusion detection and prevention systems (IDPS). Basic algorithms for network traffic analysis, detection of anomalies and detection evidence of unauthorised access. These systems can recognise both known and previously unknown attacks;

2) solutions for threat analysis and management. MITRE ATT&CK tools are used to identify links between different cyber incidents and patterns. Such solutions help analysts to react even faster to threats and take effective action;

3) malware protection systems. These products use machine learning technologies, including deep learning, to classify and identify malicious objects. They are able to detect even complex, encrypted and polymorphic types of malware.

At present, there are numerous diverse solutions for safeguarding against cyber threats. Many cyber attacks need to be identified and classified to train artificial intelligence to recognise them. Only after these steps the neural network can effectively protect any system from such threats. In conclusion, artificial intelligence has been quite successful with some cybersecurity challenges. However, it cannot solve all the problems: unpredictable attacks appear every year. Cybersecurity professionals will be in demand and not replaced by artificial intelligence.

References:

1. Kouliaridis, V., Kambourakis, G. A comprehensive survey on machine learning techniques for android malware detection / V. Kouliaridis, G. Kambourakis. – Information 12.5. – 2021. – 185 p.

2. Yuan, Z., et al. Droid-sec: deep learning in android malware detection / Z. Yuan, et al. – Proceedings of the 2014 ACM conference on SIGCOMM. – 2014.

3. Vinayakumar, R., et al. Robust intelligent malware detection using deep learning / R. Vinayakumar, et al. – IEEE Access 7. – 2019. – P. 46717-46738.

4. Using fuzzy hashing and deep learning to counter malware detection evasion techniques / Microsoft. – Mode of access: https://www.microsoft.com/security/blog/2021/07/27/coming-through-the-fuzz-using-fuzzy-hashing-and-deep-learning-to-counter-malware-detection-evasion-techniques/. – Date of access: 09.03.2025.

5. Shenfield, A., Day, D., Ayesh, A. Intelligent intrusion detection systems using artificial neural networks / A. Shenfield, D. Day, A. Ayesh. – Iot Express 4.2. – 2018. – P. 95-99.

6. Applications for artificial intelligence in Department of Defense cyber missions / Microsoft. – Mode of access: https://blogs.microsoft.com/on-the-issues/2022/05/03/artificialintelligence-department-of-defense-cyber-missions/. – Date of access: 11.03.2025.

7. Mishra, P., et al. A detailed investigation and analysis of using machine learning techniques for intrusion detection / P. Mishra, et al. – IEEE Communications Surveys & Tutorials 21.1. – 2018. – P. 686-728.

8. Alsaheel, A., et al. ATLAS: A sequence-based learning approach for attack investigation / A. Alsaheel, et al. – 30th USENIX Security Symposium (USENIX Security 21). – 2021. – 19 p.

9. Ongun, T., et al. Living-Off-The-Land Command Detection Using Active Learning / T. Ongun, et al. – 24th International Symposium on Research in Attacks, Intrusions and Defenses. – 2021. – 14 p.

10. Kok, S., et al. Ransomware, threat and detection techniques: A review / S. Kok, et al. – Int. J. Comput. Sci. Netw. Secur 19.2. – 2019. – 136 p.