AI IN CYBERSECURITY: AN INSTRUMENT FOR DEFENSE AND ATTACK

Mykhaylo Gutsalyuk
Ph.D., Leading researcher at the Interagency Research Center combating organized crime under NSDC of Ukraine
ORCID ID: 0000-0003-4496-5173

The rapid development of the modern information society relies on robust cyber protection and effective measures against cybercrime [1]. However, cybercriminals continually evolve their tools and methods. They target cyberattacks at a variety of services, including banks, medical institutions, communications systems, and other critical infrastructure. For instance, in May 2021, the U.S.-based Colonial Pipeline company was attacked by the DarkSide ransomware group, which used a mix of traditional hacking techniques and artificial intelligence (AI) to penetrate the company's systems and encrypt its data [2].

The problem of the activities of organized cyber groups is especially relevant for Ukraine, which is a cyber training ground for Russian hackers. The Ukrainian energy system has already been subjected to powerful cyber-attacks in recent years. However, these days they are combined with massive shelling of energy facilities. All methods of disseminating disinformation aimed at creating panic among the population are also actively used, information and psychological manipulations and propaganda regarding the state of the energy sector are used.

In terms of emerging technologies, in 2024, cybersecurity researchers and practitioners observed a sharp rise in the use of Artificial Intelligence (AI) by cybercriminals to organize cyberattacks. The problem is accelerating rapidly.

Cybercriminals leverage AI to enhance the sophistication, scale, and efficiency of their attacks. In particular:

1. Phishing and Social Engineering:

- Deepfake Technology: AI-generated deepfake videos or audio can impersonate individuals, convincing victims to divulge sensitive information.
- Spear Phishing: AI can analyze a target's online presence and generate highly personalized phishing emails, increasing the likelihood of success.
- Malware and Ransomware:
- Polymorphic Malware: AI enables malware to evolve, changing its code or behavior to avoid detection by traditional antivirus software.
- Smart Ransomware: AI can optimize encryption strategies and identify high-value data for maximum impact.
- Automating and Scaling Attacks:
- AI-powered bots can scan networks, find vulnerabilities, and exploit them at a scale without human intervention.
- Tools like CAPTCHA-solving bots use machine learning to bypass security measures.

- Adversarial AI:
- Cybercriminals use adversarial machine learning to manipulate or corrupt the AI systems used in cybersecurity, causing them to misclassify threats or miss anomalies.
- Credential Theft:
- AI can be used to guess passwords through advanced brute force techniques, such as generating password patterns based on user behavior or previous breaches.
- Dark Web Intelligence:
- AI tools can monitor and analyze activity on the dark web to identify trends, new tools, or vulnerabilities that can be exploited.

At the same time, cybersecurity professionals are also using AI to protect information systems, especially in critical infrastructure facilities.

AI plays a vital role in enhancing cybersecurity by providing proactive and adaptive defenses against evolving threats:

1. Threat Detection and Response:
- Anomaly Detection: Machine learning algorithms can identify unusual patterns in network traffic, flagging potential threats in real-time.
- Behavioral Analysis: AI can model user behavior to detect insider threats or compromised accounts.
2. Automated Incident Response:
- AI-driven systems can isolate infected systems, block malicious traffic, or roll back unauthorized changes automatically.
3. Threat Intelligence:
- AI collects and analyzes global threat data to identify emerging attack vectors and patterns, enabling predictive threat mitigation.
4. Endpoint Protection:
- AI-based antivirus and endpoint detection systems use machine learning to recognize malware based on its behavior, even if it hasn't been encountered before.
5. Deception Technologies:
- AI can deploy decoys or honeypots that mimic real systems, tricking attackers and gathering intelligence about their methods.
6. Fraud Prevention:
- AI models analyze transactional and user data in real time to identify fraudulent activities, especially in financial systems.
7. Vulnerability Management:
- AI tools assess and prioritize vulnerabilities in an organization's systems, recommending fixes based on exploitation's likelihood and potential impact.
8. Predictive Analytics:
- By analyzing past attack data and current trends, AI helps predict future threats, allowing for preemptive action.

Despite the current practice of using AI in cybersecurity, certain challenges remain. Among them are:

- Arms Race: As defenders improve AI-driven solutions, attackers simultaneously innovate their methods.
- Bias and False Positives: Poorly trained AI models can lead to false positives or negatives, undermining trust in the system.
- Cost and Complexity: Advanced AI systems require significant development, deployment, and maintenance resources.
- Adversarial AI: Attackers can exploit vulnerabilities in AI models, such as poisoning datasets or fooling detection algorithms.

One of the most pressing concerns is the identification of AI-generated content. Artificially generated content enables attackers to create customized content with a much lower time investment. Deepfakes, private emails, and voicemails create great opportunities for phishing, which cybercriminals use for criminal purposes. For example, the CEO of a UK-based energy firm was conned out of US$243,000 by scammers using deepfake AI voice technology to impersonate the head of the firm's parent company [3].

Combining AI with traditional methods and human expertise is essential to stay ahead in the evolving battle against cybercrime. However, the dual-use nature of AI necessitates ethical frameworks and international collaboration to ensure its responsible use.

REFERENCES

1. Klymenko, Olga A.; Gutsalyuk, Mykhailo V.; Savchenko, Andrii V. Combating cybercrime as a prerequisite for the development of the digital society // JANUS.NET e-journal of International Relations, Vol. 11, N.º 1, Maio-Outubro 2020. Consultado [em linha] em data da última consulta URL: https://doi.org/10.26619/1647-7251.11.1.2
2. El ataque a Colonial Pipeline se originó con el robo de una sola contraseña URL: https://www.computerworld.es/article/2119818/el-ataque-a-colonial-pipeline-se-origino-con-el-robo-de-una-sola-contrasena.html
3. Catherine Stupp, "Fraudsters used AI to mimic CEO's voice in unusual cybercrime case," Wall Street Journal, August 30, 2019. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402