PRESS RELEASE

FEBRUARY 11TH, 2025

Artificial Intelligence in Cybersecurity: Opportunities and Challenges

Artificial Intelligence (AI) is increasingly reshaping the cybersecurity landscape—it can both enhance defense mechanisms and introduce new threats. These topics were the focus of the third CyberAgent project seminar, “Artificial Intelligence (AI): Insights You Can't Miss,” which brought together international experts and practitioners to discuss AI's impact on cybersecurity.

The seminar was organized by Vilnius University in collaboration with its partners, and it was moderated by Jorė Bendinskaitė, Public Relations Specialist at Vilnius University Kaunas Faculty.

CyberAgent Project Overview

The seminar was opened by Renata Danielienė, the CyberAgent project manager, who demonstrated AI's capabilities by simulating technical difficulties and showcasing a recording of her digital twin. “AI can be a powerful tool for various purposes—from content generation and presentation delivery to enhancing

cybersecurity. Although AI is a widely discussed topic, the importance of human intelligence should not be overlooked. Today's presentation is being delivered not by my digital twin, but by the real Renata Danielienė!" she continued.

Renata Danielienė then presented the project's achievements and future plans. The project has already conducted audience needs assessments, developed training programs, and is preparing an eight-module training curriculum covering technical, risk management, analytical, and organizational topics in cybersecurity. She encouraged attendees to follow project updates regarding the pilot training sessions scheduled for early 2026.

AI Capabilities in Cybersecurity

Özgür Can Turna, a software security engineer at ISTEC Cybersecurity, began his presentation by emphasizing that cyberattacks are becoming more frequent and sophisticated. He highlighted how AI is transforming cybersecurity technologies, enabling real-time threat detection and mitigation, reducing human error, and automating repetitive tasks.

The speaker stressed that AI can be used for threat detection, fraud prevention, and endpoint protection. AI allows for proactive threat forecasting and attack prevention before they occur, efficiently managing large networks and data volumes while minimizing the need for manual intervention. Furthermore, AI systems continuously learn and improve, becoming more effective over time.

However, AI also presents various challenges. One of the main issues is false positives, where AI incorrectly identifies benign activities as threats. Another concern is cybercriminals leveraging AI to bypass security systems. Additionally, ethical concerns arise regarding privacy protection and AI oversight. Addressing these issues is crucial to ensuring the responsible and effective use of AI.

AI Threats to Cybersecurity

Gülhan Ertürk Akgül, CEO of ArVis Technology, agreed that AI can be used both for protection and for conducting cyberattacks. She noted that hackers are increasingly using AI to automate their attacks, adapt them to defensive systems, and circumvent traditional security measures.

She provided examples of cyberattacks where AI-enabled systems evolve and adapt to different situations, facilitating automated cyberattacks. The speaker listed several specific ways AI is utilized in cyberattacks.

AI can automate vulnerability scanning, enabling rapid and efficient detection of security flaws. It is also used to develop and manage botnets—networks of infected devices that conduct coordinated cyberattacks. AI-driven botnets can adapt to changing conditions and continuously refine their attack strategies. These botnets can launch large-scale attacks on multiple targets simultaneously, causing significant damage.

Additionally, AI can be employed for brute-force attacks, crafting convincing phishing schemes that mimic human behavior and text in real time, and creating deepfakes used for social engineering, fraud, identity theft, and even falsifying critical government decisions.

Machine Learning Algorithms in Cybersecurity

Associate Professor Emil Simion from National University of Science and Technology POLITEHNICA Bucharest (UNSTPB), Centre for Research and Training in Innovative Techniques of Applied Mathematics in Engineering (CiTi) & Advisor of Director of DNSC, in a joint work with Assistant Professor Ioana-Corina BOGDAN from Transilvania University of Brașov & CiTi proposed a presentation on how machine learning can strengthen cybersecurity, particularly in defending against ransomware attacks. Ransomware is malicious software that encrypts user files and demands ransom for decryption. Such attacks cause significant damage to organizations and are among the most dangerous cyber threats.

Traditional security measures, such as signature-based antivirus software, struggle to detect emerging threats. Machine learning plays a crucial role here, identifying suspicious behavior instead of merely relying on known malware signatures. A Mandiant report indicates that 91% of cyberattacks are not detected immediately and do not trigger alerts, emphasizing the need for proactive threat detection.

Machine learning employs various techniques, such as Random Forest and neural networks, to detect malware, including ransomware. These methods analyze data and behavior to distinguish normal activity from malicious actions, potentially reducing attack detection time significantly.

Despite its advantages, machine learning also poses security challenges. Cybercriminals can manipulate training data to prevent the detection of malware or generate false alerts. They may also attack machine learning models themselves, attempting to deceive or exploit their vulnerabilities. Additionally, many AI-driven security systems operate in cloud environments, making them susceptible to data breaches.

In the future, AI and quantum computing may introduce new challenges, such as vulnerabilities in existing encryption methods. The risks associated with self-replicating AI are also increasing, highlighting the need for stricter AI regulation.

Conclusions and Future Perspectives

During the seminar, experts agreed that AI can both strengthen cybersecurity and introduce new threats. It is essential not only to improve AI-driven security systems but also to ensure their ethical and responsible use.

The CyberAgent project plans to continue these discussions and organize more seminars for cybersecurity professionals.

For more information about upcoming events and project activities, visit the CyberAgent project website and social media channels.

Presentations:

CyberAgent Project Overview, Renata Danieliene

Opportunities: The Usage Areas of AI in Cybersecurity, Özgür Can Turna, Software Security Engineer at ISTEC Cybersecurity

Threats: How AI Could Pose a Danger to Cybersecurity, Gülhan Ertürk Akgül, CEO at ArVis Technology

Machine Learning Algorithms in Cybersecurity: Protecting Networks and Detecting Attacks, Emil Simion, Associate Professor at Politehnica University of Bucharest and Advisor to the Director of the National Cybersecurity Directorate

Videos of seminar speakers:

https://youtu.be/qrovnDA221k
https://youtu.be/41YghChAhq8
https://youtu.be/WVJ6ChTSlbk

For those interested in learning more about the research findings and upcoming events, visit the CyberAgent project website www.cyberagents.eu and social media.

The event was organized as part of the CyberAgent project, which aims not only to address key cybersecurity challenges but also to promote an inclusive environment where women can thrive and successfully establish themselves in this field.

Project coordinator: Kaunas Faculty of Vilnius University.

Project Leader Dr Renata Danielienė, Institute of Social Sciences and Applied Informatics. renata.danieliene@knf.vu.lt

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.