PhD THESIS ABSTRACT
„MACHINE LEARNING IN CYBERSECURITY”

Author: **Constantin-Ilie NILĂ**
E-mail: constantin.nila@mta.ro, tel.: +40751 375 077
PhD supervisor: **Victor-Valeriu PATRICIU**, Professor Emeritus, Ph.D.

As artificial intelligence continues to evolve and integrate into various fields, propelled by rapid innovations, it's essential to consider the necessity for more robust and adaptive security systems. Cybersecurity solutions have become standard tools, now integral to any information technology and communications architecture. Covering a wide array of functionalities, from intrusion detection systems and malware classification to phishing detection methods and secure authentication, these systems stand to gain significantly from the advancements in machine learning.

This paper explores the integration of machine learning in cybersecurity, highlighting the shift from traditional security approaches to more dynamic and adaptive strategies. The proposed approaches reveal the challenges current predictive models face in real-time threat detection, emphasizing the importance of relevant and high-quality training datasets. A key aspect defined in the paper is the diverse application of machine learning techniques in the development process of cybersecurity solutions. This proactive approach is crucial in a landscape where reactive strategies are often insufficient against advanced persistent threats.

This research also analyzes the perspective in which security systems themselves are exposed to the risk of cyber-attacks, and how the successful implementation of privacy-preserving measures can make a significant contribution to future artificial intelligence systems and other data management systems. Balancing the sensitivity and specificity of models extends beyond security considerations, touching on ethical and privacy issues in the implementation of machine learning based cybersecurity solutions. As these systems often process and analyze sensitive personal and organizational data, ensuring data privacy and compliance with current regulations becomes crucial. This thesis supports various approaches that address these concerns, including differential privacy and homomorphic encryption, which allow data processing in an encrypted form.

Beyond technical aspects, the paper also addresses the importance of interdisciplinary collaboration in this field. The effective application of machine learning in cybersecurity requires a mix of expertise in computer science, data science, cybersecurity, and domain-specific knowledge. This interdisciplinary approach ensures alignment with practical scenarios and future cybersecurity requirements.