PHD THESIS ABSTRACT

"**INTERNET OF THINGS – Security and Military Applications**"

Author: Cpt.eng. **Marius-Ștefăniță PREDA**
Email: marius.preda@mta.ro, tel.: +40785257440
PhD supervisor: Prof. univ. emeritus phd. eng. **Victor-Valeriu PATRICIU**

This thesis explores the revolutionary potential of the Internet of Things (IoT) in reshaping modern warfare, a context where emerging and disruptive technologies like IoT are increasingly pertinent. The study focuses on the capacity of military IoT applications to significantly influence military tactics and strategy, as highlighted by recent conflicts such as the invasion of Ukraine by the Russian Federation. This context has not only demonstrated the relevance of military IoT applications but also the urgent need to adapt military strategies to integrate new technological capabilities.

IoT introduces significant complexities in terms of cybersecurity, given its ubiquitous nature and the convergence of physical and virtual elements. This results in an environment full of uncertainties, where cyber threats can quickly migrate between the physical and virtual realms. The defining features of IoT, such as heterogeneity and the large volume of data, exacerbate these challenges, necessitating innovative and effective security solutions.

A significant risk to national security, discussed in the thesis, is the use of IoT technologies by state and non-state actors to initiate attacks in cyberspace, with direct consequences on national security. The thesis advances by analyzing how IoT devices are integrated into critical infrastructures, such as energy and transportation sectors, highlighting the risks associated with their disruption. In the context of hybrid warfare, the combined use of kinetic and cyber operations is becoming more common, illustrated by coordinated cyberattacks preceding conventional military actions.

Thus, the issue of cybersecurity for IoT technologies with high potential for application in military operational environments is addressed in this thesis, focusing on three main research directions. The first direction concentrates on the security of IoT sensor networks - WSN, analyzing the RPL protocol and 6LoWPAN technology, identifying vulnerabilities and exploitation methods. The second direction addresses the analysis of IoT network traffic security, applying data analysis techniques to detect cyberattacks and establish normal network behavior. The third direction reviews existing IDS solutions for IoT, then proposing an innovative anomaly detection solution based on deep machine learning, highlighting the advancements and challenges in this field. The results obtained from this research effort significantly contribute to enhancing IoT security, offering innovative and effective solutions for various operational scenarios, including military ones.

Finally, the thesis addresses the need to integrate IoT with other disruptive technologies, such as artificial intelligence, 5G and Big Data, emphasizing how this fusion can enhance the responsiveness and adaptability of military forces in conflict scenarios. This blend of technologies facilitates a profound transformation within military operations, highlighting the importance of continuously adapting security strategies to technological evolutions.

This thesis provides a detailed and well-documented perspective on the crucial role of IoT in the context of modern warfare, offering a comprehensive analysis of the challenges and opportunities presented by this emerging technology from a cybersecurity perspective. By exploring the interaction between technology and military strategy, the work substantially contributes to the existing literature, proposing new directions for the development and implementation of IoT technologies for defensive and offensive purposes.