**Thesis title: Contribution to improving cyber-security in complex networks**
**PHD Student: Mihai BĂRBULESCU**
**PHD Coordinator: professor emeriti doctor engineer Sergiu Stelian ILIESCU**

## Abstract

Computer Science and Information Technology have grown in the last decades faster and uncontrolled than ever before. Together with the evolution in technology, the need for interconnected devices and uninterrupted communications became a vital part of our life. At the same time, with evolution, the security provocations are becoming more sophisticated and challenging to manage. As technology developed and become a critical element in our daily activities, there has been a need to add a different layer of security. A new concept was created to protect our computer systems, services, and networks from malicious activities that could impact in a negative way our lives. This new concept is known as **cybersecurity**.

This thesis presents methods of improving the cybersecurity posture of any organization in this new and evolved landscape. We will demonstrate that there is no silver bullet when it comes to a secure environment. There is a known fact that cybersecurity is about people, processes, and tools. The thesis introduces a new methodology to address big data issues by designing an architecture using open-source tools that can be used as a baseline for reference in future deployments.

We will provide ways for how machine learning use cases can help the Infosec practitioner to deal with repetitive tasks or well-defined incidents. Deep dive, we will propose a new software platform that can help bridge unconnected dots when it comes to operating tools in their silos.

Alongside the security tools, another important aspect is how we deal with incidents when having hybrid environments and complex networks. We will look from an incident management and response perspective and propose a methodology that can be used in day to day operations.
Considering the research and development of the cybersecurity area in different systems, we found methods than can be used to address present challenges.