



CYBER DEFENCE LAB



Offensive Security

Automated red teaming for cyber range-based training

Researcher: Robbe Louwet

Develop **automated red teaming** for a better organization of "Red-Blue Team" training sessions with repeatable red team performance and better **skill evaluation and certification**.



Autonomous Cyber Red Teaming System (ACRES)

Researcher: Elli Makdis Antoun

Develop a proprietary **fully automated cyber red teaming system** able to deploy an attack by sensing its way into a target network.



Self Learning Attack surface Explorer (SLATE)

Researcher: Raphaël Simon

Develop a self-learning agent based on **Deep Reinforcement Learning** for the goals of **vulnerability identification** in the scope of network **pen-testing** and hardening.



Development of intrusive Linux capacity

Researcher: Zacharia Mansouri

Study and develop **proprietary Linux malware** capabilities, focusing on Linux platforms, based on the **Cyber Kill Chain**.



Management of Security

Automated Methodology for Common Criteria Certification (AMC3)

Researcher: Ahmed Bokri

Design and prototype a **flexible certification methodology** and framework for product certification schemes such as the Common Criteria (CC).



Facial Recognition prevention (F-REC)

Researcher: Charles Beumier

Counter risks of AI-driven identification of army personnel by using accessories, web monitoring, and post-processing of images before uploads to social media platforms.



Semestres Thématiques - CyberExcellence

Researcher: Ioanna Gianni

Strengthen collaboration between Walloon universities, responding to **Belgian Defence issues** by demonstrating the validity of **CyberExcellence technologies** in real military environments.



Military Cloud

Advanced European platform and network for Cybersecurity training and exercises centers (ACTING)

Researcher: José Carrasquel Vera

Deliver an **organized and coordinated approach** to proactively improve efficiency of cyber defence training and exercises in the European Union, through **effective and efficient multi-sector collaboration**.



Intrusion Detection

Multi Agent for APT detection (MASFAD)

Researcher: Georgi Nikolov

Study Advanced Persistent Threat life cycle and behavior, develop a **proprietary tool based on anomaly and behavior-based analysis** focusing on the **detection of Command & Control** channels established by APTs.



AI4Cyber

Researcher: Yemen Rhouma

Study and **compare the latest advances in Artificial Intelligence techniques**, and apply them to implement or **enhance the protection of BEL Defence cyber assets**.



AI-based detection of APT persistence techniques

PhD Student: Khaled Rahal

Apply **Machine Learning** for the **detection and identification of APTs** and how they establish **Persistence** via **Scheduled Tasks** in Windows machines.



Software Supply Chain

Using blockchain to secure the software supply chain

Researcher: Arnaud Stoz

Bolster and strengthen the supply chain, to mitigate possible attacks on external dependencies through the use of the **blockchain technology**.



Software supply chain Attack and Defence (SOLACE)

Researcher: Enrico Migliorini

The project aims to **evaluate the limits of current tools** and security measures and develop new approaches to efficiently **detect supply chain vulnerabilities** through pen-testing and bolster automated library updates.

