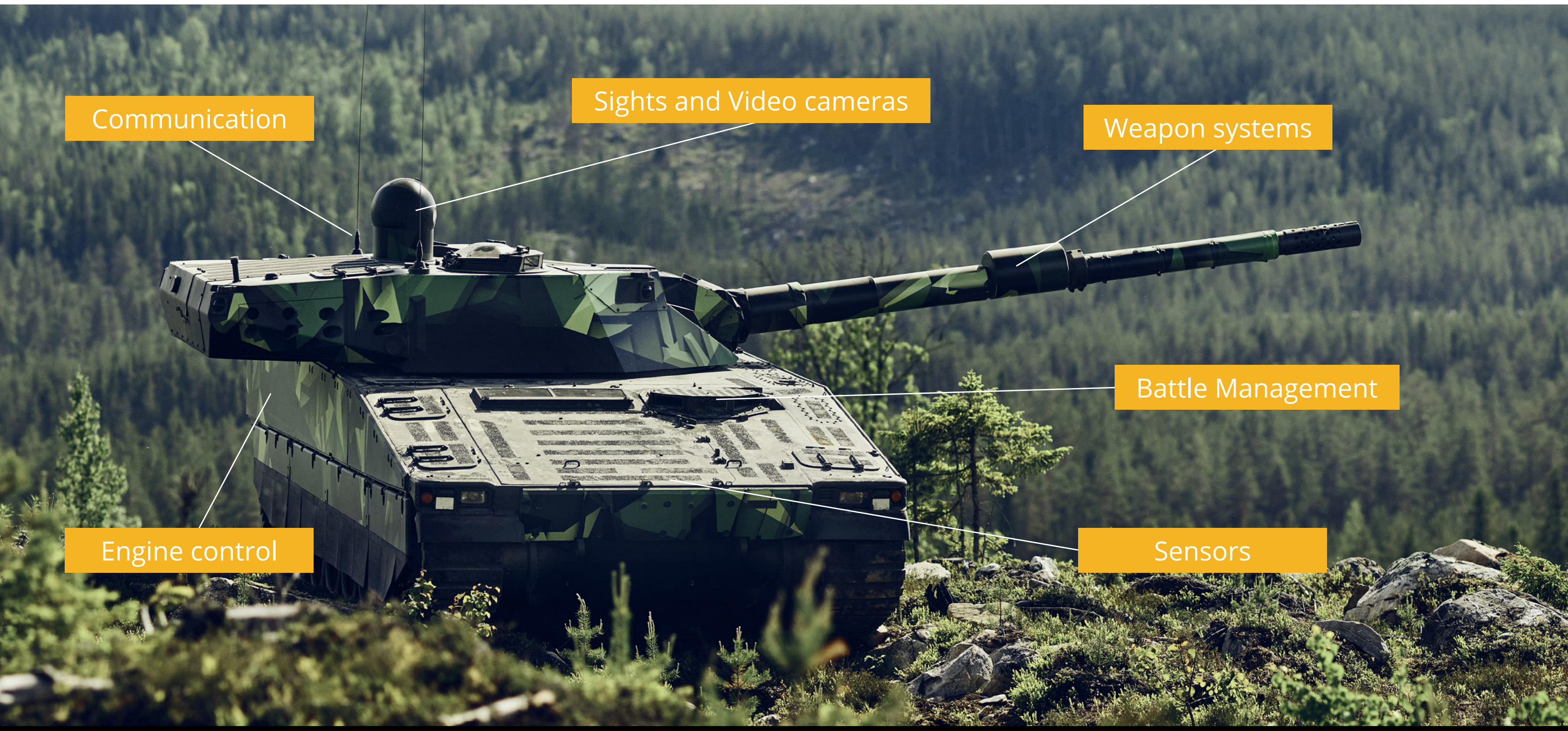
# CYBER ARMOUR

AI-powered cyber security
for military platforms

clavister®
CONNECT. PROTECT

# Urgent need of Cyber Defence

Defence and Security landscape has shifted in Europe and in the era of hybrid warfare, cyber security needs to be at the fore front.



Increased connectivity and digitization  makes military platforms more vulnerable.

**Military platforms and weapon systems are increasingly digital and connected.**

There is also greater interconnectivity between information technology (IT) and previously isolated operational technology (OT). OT powers the most critical and sensitive functions of major defense systems and weaponry, including fighter aircraft, combat vehicles, sea vessels, and artillery.

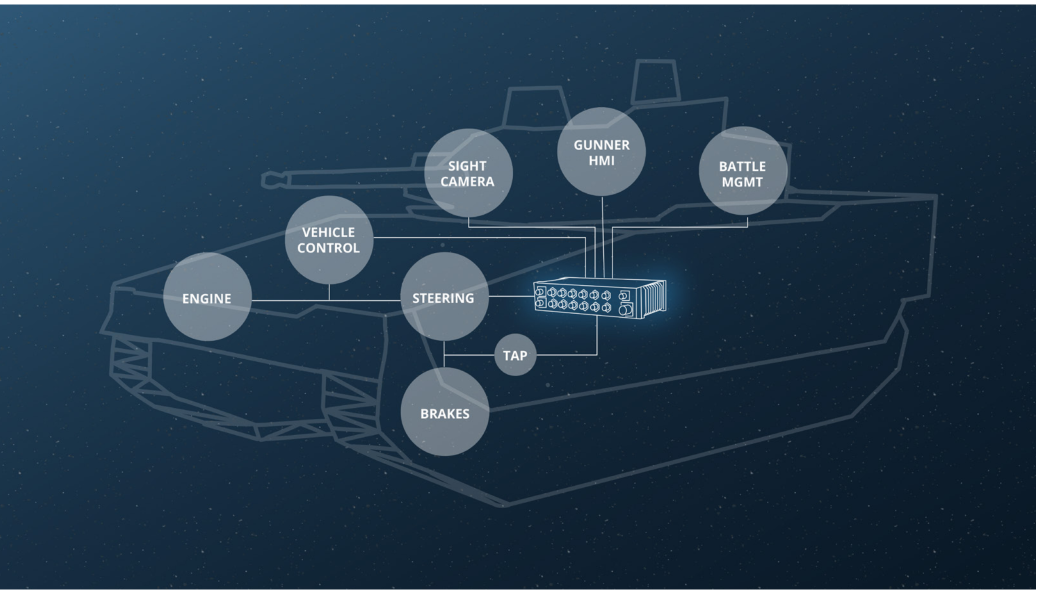
While IT security has improved tremendously, OT cybersecurity at the tactical edge is still in a nascent stage. As a result, cybersecurity solutions capable of defending the entire system have not kept pace.

Military platforms and weapon systems take years to develop and need to be protected for the entirety of their lifespan, which lasts 20-30 years in most cases. In the cybersecurity domain, the enemy can upgrade their cyber weapons every day, and we need solutions to be longer-lasting and relevant.

# Cyber Armour

### Military grade Cyber Resilience for European Defence

Part of Clavister's cyber security solutions for the defence industry, Cyber Armour is a ruggedised firewall product that fits into individual military platforms, like armoured vehicles, and provides active protection against cyberattacks. Cyber Armour can be embedded from start as part of vehicle design or introduced as part of upgrades and modernization programs as the hardware can be tailored and optimized for each military platform. Through software updates, it maintains a high level of cyber protection.



### Future-Proof  Protection with Artificial Intelligence (AI)

Cyber Armour comes with an option of adding an extremely efficient AI engine that not only provides protection, but detection and response ability also as the system models normal operational behavior to detect and fight against unknown cyber threats. AI allows military vehicles to continue to operate in the field and enhances vehicle's survivability.

### Advanced and flexible Cyber Security Gateway

Digital sub-systems are connected to the embedded Cyber Security Gateway which controls the internal communication flow to prevent and limit the impact of cyberattacks.

### Compliant to Military Standards

Cyber Armour can be customized according to specific customer requirements and according to military standards. It can be deployed as a ruggedized hardware appliance or deployed in a virtualized environment.

## AI-powered cyber security for military platforms

*Network Segmentation*

- Granular Firewall Policies
- VLAN segmentation

*Deep Inspection*

- Protocol Validation
- Application Control

*Quality-of-Service*

- Traffic Shaping
- Threshold Rules
- Link Monitoring
- Load Balancing
- High-availablllty Clusters

*Authentication and Encryption*

- 802.1 x Port Authentication
- IPsec and SSL VPN

*Maintenance*

- Secure Firmware Upgrade
- Logging

*AI-based Threat Detection*

- Intrusion Detection
- Communication Behavior
- Monitoring
  Anomaly Detection

# Defend the Defenders

CYBERSECURITY™
MADE IN EUROPE

## Trusted Europeancyber security vendor

Clavister is a leading European cybersecurity vendor with over 25 years of experience. Seated in Sweden, the company has customers—defence, government, telecoms, enterprise in more than 150 countries. Clavister provides unique security solutions to secure mission and business success. Clavister has been trusted with securing military platforms, including armoured vehicles, by several of the worlds leading defence companies and is in use by multiple NATO countries. The company is, since 2014, listed on Nasdaq First North.

SECURITY BY
SWEDEN

clavister®
CONNECT. PROTECT

COMMON CRITERIA
CERTIFIED
EAL4+

Sjögatan 6
891 60 Örnsköldsvik
Sweden