Clavister Cyber Security Solutions for Defence

Defend the Defenders

clavister®
CONNECT . PROTECT

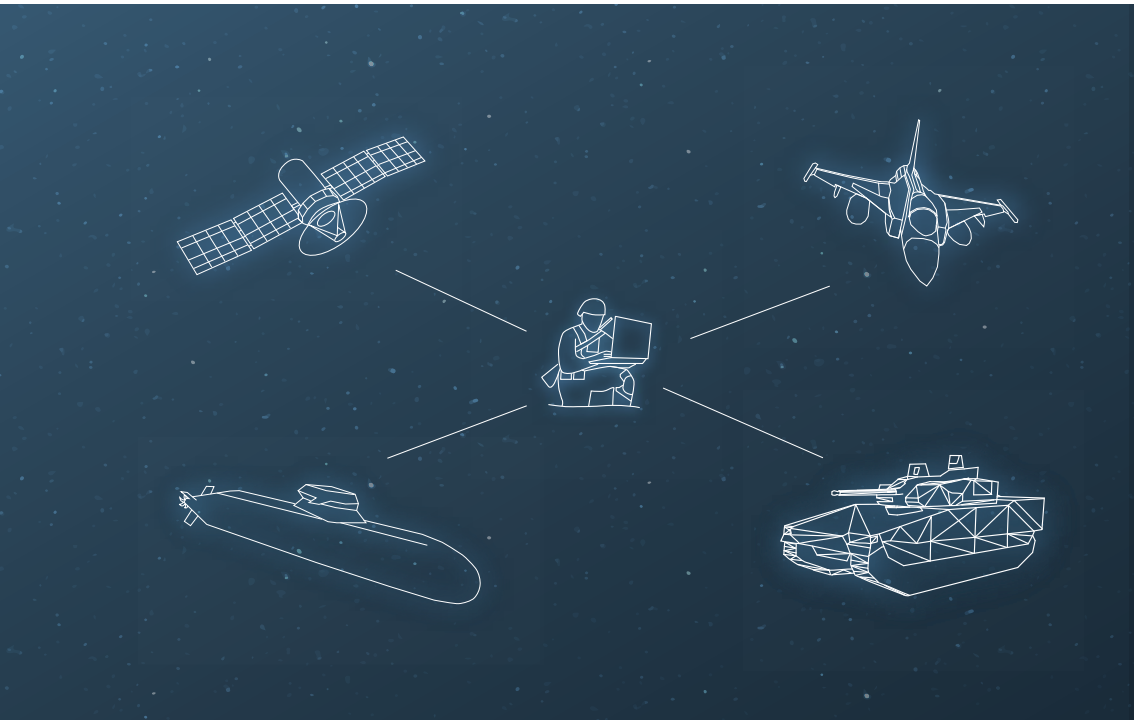
Cyber Threats Are Increasing in Intensity and Impact

Digitalisation is no longer a buzzword but has seeped deep down into defence innovation. Not only individual military platforms, vehicles and systems are getting digitalised but there is ever increasing connectivity and integration between different domains, creating a 'system of systems'. Cyber is now widely recognised as the fifth operational domain besides land, sea, air, and space. Strong cyber, intelligence, surveillance and reconnaissance (CSIR) capabilities will determine defence superiority and provide competitive advantage over adversaries.

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

Securing 'System of Systems'

In the context of defence, a System of Systems (SoS) refers to a complex and integrated network of various defence systems, platforms, sensors, and technologies that work collaboratively to enhance national security and military capabilities. The interconnected nature of SoS can create vulnerabilities that attackers may exploit. Therefore, ensuring the cybersecurity of a SoS requires a comprehensive approach that includes secure architecture design, continuous monitoring, threat detection, and incident response across the entire interconnected environment. Defending a SoS involves securing not just individual components, but also the interactions and interfaces between them. Different cyber security solutions and capabilities are needed to ensure the security of overall SoS.



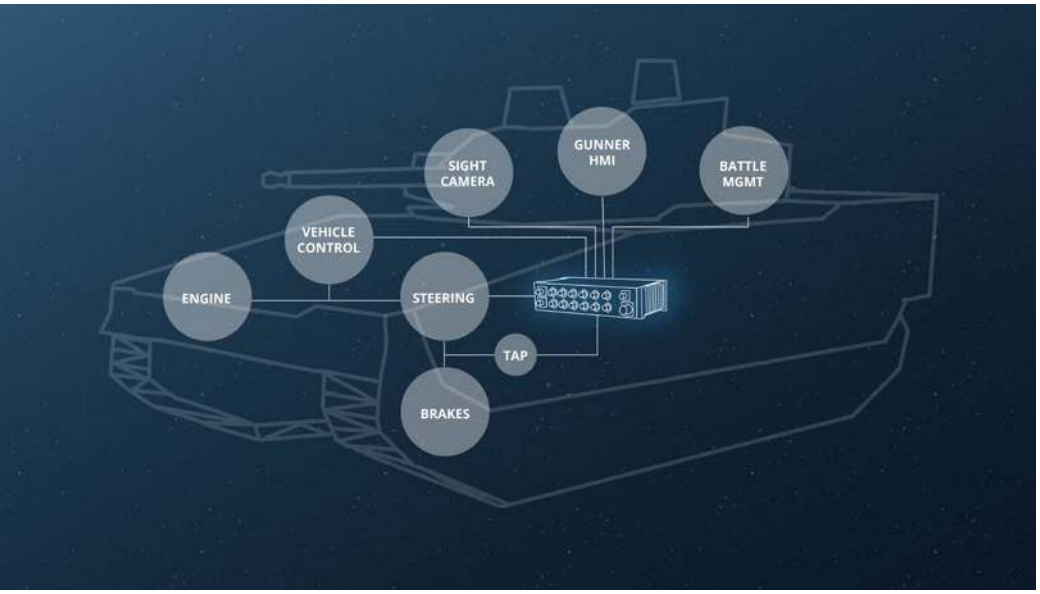
Clavister cyber security solutions

- Cyber Armour for military vehicles
- AI-powered cyber security
- Customised, ruggedized military firewalls
- Cyber security as a service
- Identity and Access Management
- Security for tactical communications

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 abilities as well, since 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 Cybersecurity Gateway

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

Compliant to Military Standards

Cyber Armour can be customised according to specific customer requirements and according to military standards. It can be deployed as a ruggedised hardware appliance or deployed in a virtualised 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-availabllity 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

"Digitalisation has accelerated significantly in the last 10 years. A modern combat vehicle is a node in a network and a sensor station. With all this increased connectivity, cyber security needs to be at the forefront of any organisation's priorities. This is what we have been doing with Clavister and we are proud to say that CV90 is one the most secure IFVs on the market today."

AI Advantage

Enhance Your Cyber Security with PASAD, a Software Deliverable with Detection and Response Capability, Independently Integrable with Any Military System

Autonomous defence

systems require real-time analysis and decision-making, which need to be cyber-hacking or jamming proof to maintain the integrity of these systems

Speed is key

on the digital battlefield decisions needs to be made within fractions of a second

Detection and response

capability is needed at the tactical edge where computer resources are scarce

The answer lies in empowering traditional cyber security products with advanced Artificial Intelligence (AI) technologies.

Clavister PASAD, a unique AI and machine-learning technology, optimised for machine-to-machine communication, developed from years of novel field research

PASAD Advantage

- Enabling autonomy by providing data assurance and integrity
- Continuous real-time analysis for instant detection and response
- Whole solution deployed at the tactical edge and completely portable
- Flexible and protocol agnostic technology, can be integrated with a wide range of defence platforms

Working with Swedish Military Procurement Agency (FMV) on a research project, Clavister has developed a cutting-edge jamming-detection AI technology that can successfully detect, with negligible latency, numerous real-world interference cases, including ones where the interference effect is hardly noticeable on specialized equipment such as spectrum analysers.

The technology is extremely lightweight making it possible to train AI models on various signals on-device, without the need to export sensitive data to off-site locations for training. Furthermore, the technology is agnostic to signal configurations, requires very little data to train, and can detect the onset of an active jamming attempt in less than 200 milliseconds.

Military grade Network Security

Standard security products cannot function reliably in harsh conditions on the battlefield. Clavister offers ruggedised, non-ruggedised network security hardware and software for virtual deployment, serving your exact requirements.

We offer NATO-compliant, ruggedised security gateways, switches and Next-Generation Firewalls (NGFWs) for the most harsh environments. Developed in Europe and Common Criteria Certified (EAL4+)

- Ruggedised firewalls for tactical deployment in the harshest environments meeting relevant military standards such as MIL-STD-810G, MIL-STD-461G, MIL-STD-1275E
- Virtual firewalls for deployment in data centres, tactical servers or as an integrated part of a Clavister partner product (support for KVM, VMWare, Hyper V)
- Custom hardware to meet specific customer needs in terms of capacity, certification, and compliance

Cyber Security As a Service

At Clavister, we have been working with defence organisations to augment their IT teams with the required cyber security expertise to fill the skill gaps. Our trained cyber security professionals can work as extension of in-house IT and cybersecurity teams, providing a range of 'scalable' capabilities:

- Cyber security risk assessment
- Implementation of cyber security design for specific military programs
- Provision of ongoing cyber security advisory services for specific military programs
- Cyber security awareness training to educate employees on cyber threats and best practices to prevent cyber attacks

Example of a cyber security risk assessment

Scope

- Initia workshop
- Architecture assessment
  - C2, Weapon systems, ...
- Risk analysis
  - Identify focus areas
- Use Case definition
  - Cybersecurity use cases required for protection

Delivery

- Lead cybersecurity expert
- Pool of Cybersecurity experts provide detailed knowledge in different areas
- NDA and security classified resources

Results

- Focus areas for Cybersecrutity work
- Cybersecurity architecture assessment
- Plan för implementation for Cybersecurity use cases

Workshop → Data gathering → Analysis → Report + Presentation

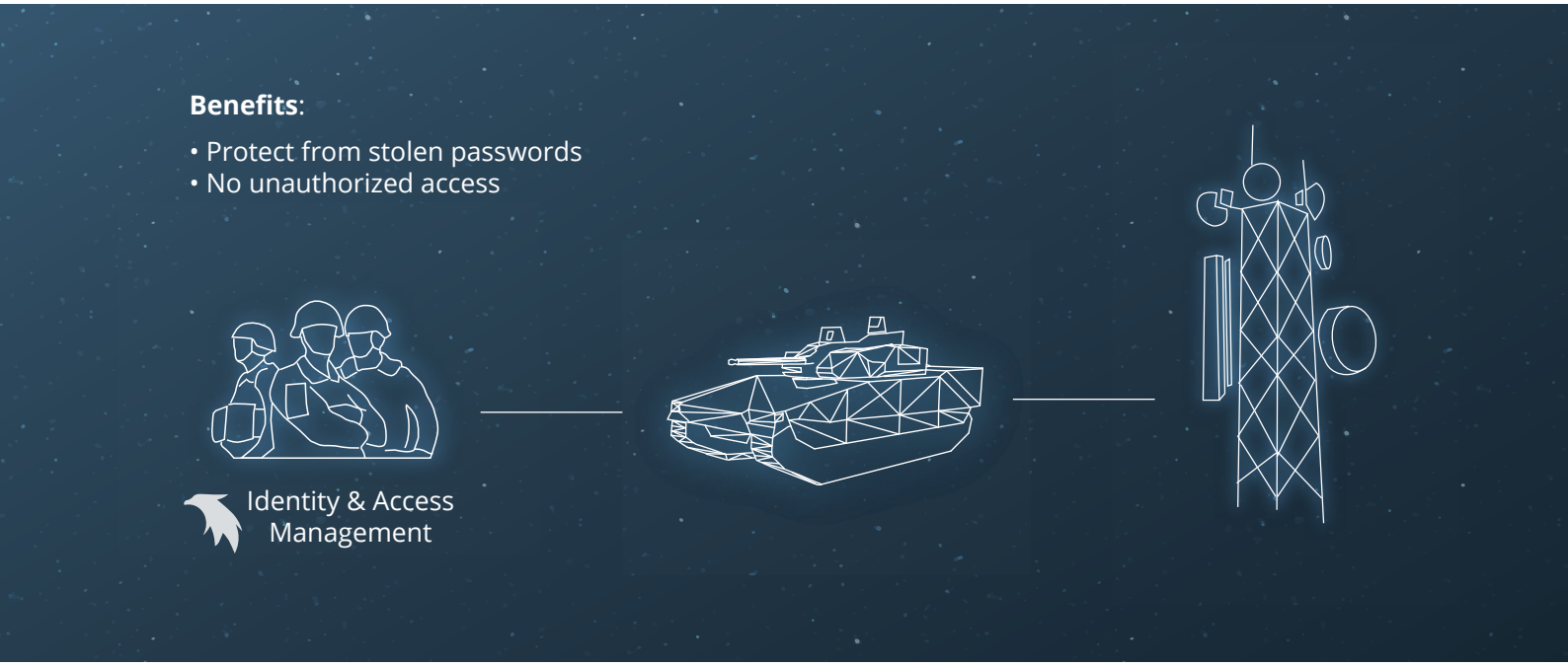
Identity & Access Management

Clavister's Identity & Access Management (IAM) solution with Multi Factor Authentication (MFA) enables the use of smartcards or biometric validation to protect the identity and improve the security of mission data.

The Clavister solution can provide a common proxy for means of authentication, ultimately enhancing service operations and mission readiness. Clavister's authentication solution provides:

- Integration with existing systems
- Enhanced login security controls
- Support for cybersecurity accreditation and authorization

The Clavister IAM solution is being evaluated by the U.S. Marine Corps and is also used by millions of people to access European government services every day.



Security for Tactical Communication - 5G and Satellite

Tactical communication using LTE or 5G networks is utilizing commercial standards and are only secure if implemented correctly. Clavister provides advanced 5G security based on partnerships with companies such as Nokia and many years of experience in telecommunications. The Clavister NetShield telecom firewall is specifically designed to protect LTE and 5G networks.

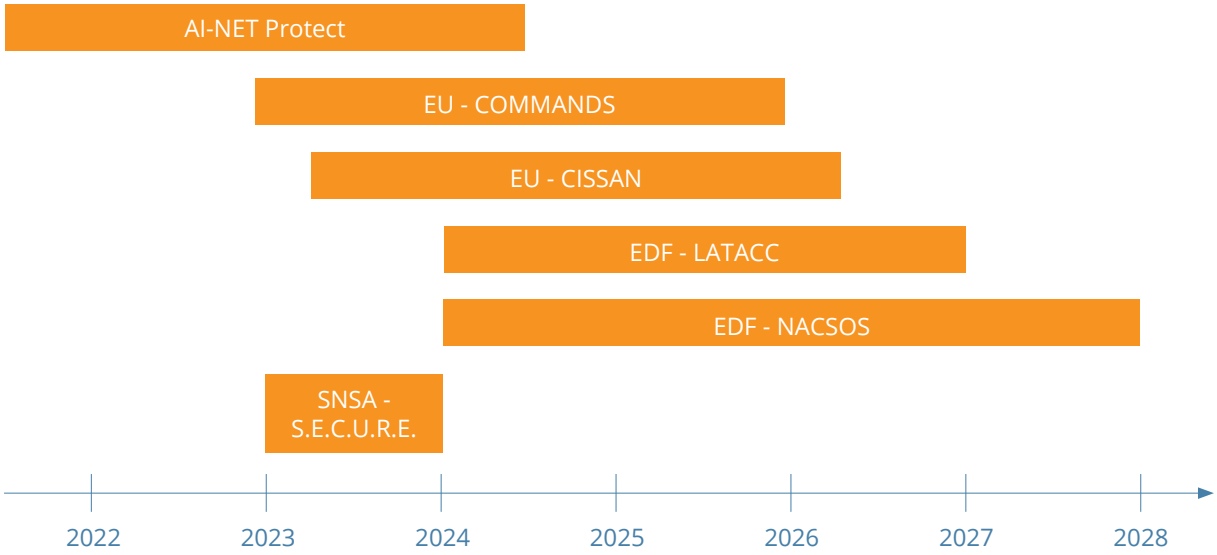
Clavister is also securing military satellite communication, which brings end-to-end protection, also including the satellite uplink from a tactical 5G network.

Clavister also delivers cybersecurity software for integration into other vendors' tactical communication products such as routers, communication servers and software defined radios.

Cyber Security Made in Europe

We are seeing seismic shifts in global power and geopolitical dynamics. In these scenarios, it's a key priority for Europe to have digital and technology sovereignty, including cybersecurity. Founded and headquartered in Sweden, Clavister brings the best of European innovation and cybersecurity technology service to critical infrastructure and the defence sector. We are actively collaborating with other vendors to grow the European cyber security ecosystem. We are proud to be part of various European cybersecurity research consortiums, working to make Europe a safer place.

European Research Programs



EDF - 'LATACC'
In 2023, Clavister secured its place as part of EDF's 'LAnd TActical Collaborative Combat (LATACC)' project. LATACC will improve armed forces' collaborative warfare capabilities. Clavister is providing cybersecurity expertise and working with leading defence contractors like Thales, Leonardo, SAAB and MBDA as part of this consortium.

EDF - COMMANDS
COMMANDS aims to deliver the European ground forces a System of Systems able to provide a trustworthy and effective cooperation between different manned and unmanned assets. In 2022, Clavister became a proud member of the consortium and has provided cyber expertise since.

Swedish Space Agency - SECURE
SECURE (Space Edge Computing with Unassailable and Robust Enforcement) is conducted together with Pandion AI. The project aims to establish guidelines and best practices for integrating cybersecurity in space infrastructure, especially regarding proactive threat detection and its autonomous response in satellite communication..

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