CYBERNETICA

Mission-critical cybersecurity for defence

Cybernetica

Cybernetica is an R&D-intensive, mission-critical system development company with over 25 years of expertise. Our technologies are deployed in more than 30 countries worldwide. Our expertise in the military domain builds on our capabilities to develop resilient information systems and our extensive expertise in advanced cryptography. Projects in collaboration with global industry leaders encompass cybersecurity solutions for military units and equipment in its everchanging dynamic environments.

"We are extremely proud of our decades-long journey. We are certain that with our values, our people, and our capabilities, we will continue to be the driving force in emerging technologies."

– Oliver Väärtnõu, CEO

Essential facts

Established in **1997**

Roots in academia **since 1960**

11% of employees **have a PhD**

Architects of e-Estonia, incl. **i-voting, X-Road, SplitKey**

Technologies exported to 30+ countries, incl. **USA, Japan, UAE Ukraine**

Global partners **NATO, European Commission, DARPA, EDF, USAFRL, ESA**

Integration is Key

In today's fast-paced world, staying ahead of potential threats is more crucial than ever. Situational awareness is achieved through the collection and sharing of information about a specific area, which in turn supports decision-making, prevents potential threats, and enhances safety, security, and efficiency.

With decades-long experience in the defence domain, Cybernetica's cybersecurity offering includes the following:

+ Cyber situational awareness
+ Entity behaviour analysis
+ Applied R&D

Cybersecurity in defence

"To understand the situation we need to be aware of what is actually going on in the systems."

You know which armour is best for your military equipment on the physical battlefield**, but can you be equally sure that it's sufficiently protected in the cyberspace?** Having your equipment connected to the network is paramount for swift operations – but the success highly depends on cybersecurity of your systems. Cybernetica is a dependable partner for establishing **cyber situational awareness** and **entity behaviour analysis.**

A large part of ensuring **cyber situational awareness** comes from understanding the system, the information it consumes and how the chosen information protecting measures function.

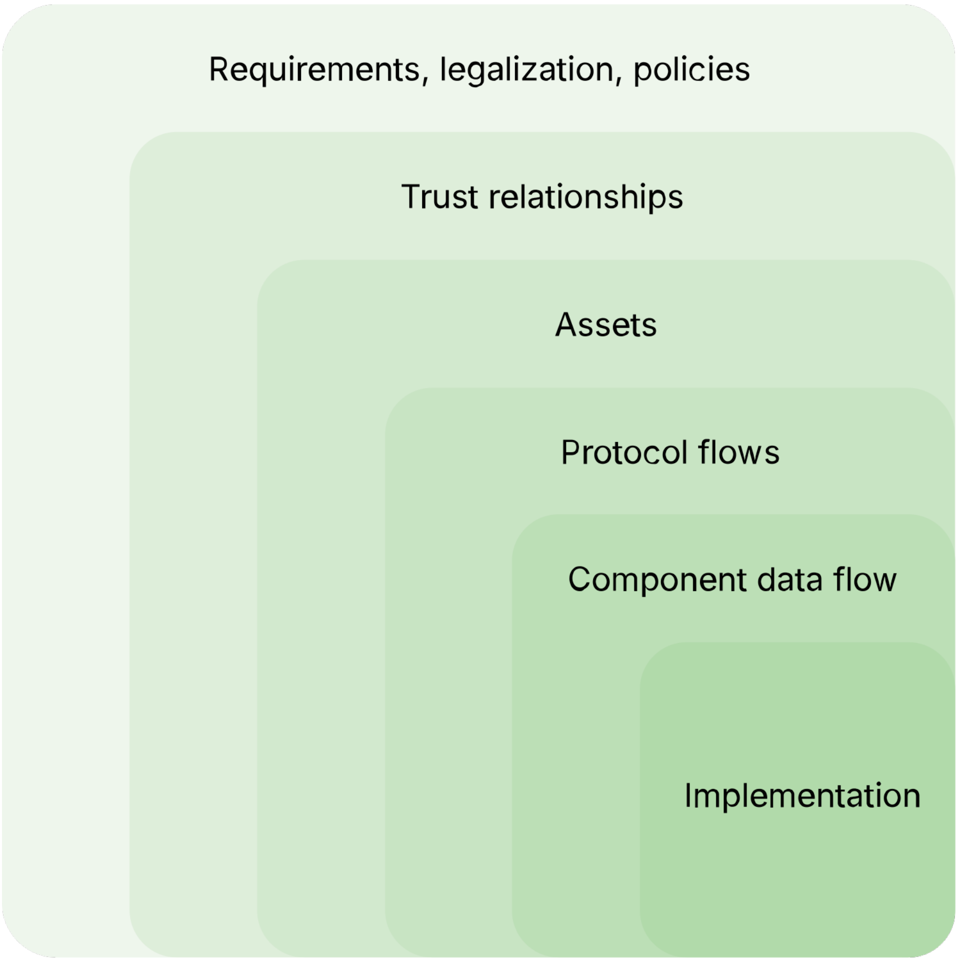
We help systematically identify and assess the elements such as:
+ system mission and processes,
+ assets,
+ threats,
+ vulnerabilities and risks.

While it's impossible to say what the next ransomware strains will look like, we recognise the behaviours attackers are using to execute attacks.

Behaviour-based security is a proactive approach to security in which all relevant activity in the systems and networks is monitored so that deviations from normal behaviour patterns can be identified and dealt with quickly. By monitoring data streams and comparing activity to baseline normal behaviour patterns, we can detect sophisticated and unpredictable threats faster.

We train, test and assess the experts, implemented systems and protective measures to create the ability to predict or anticipate the future states or events of the situation.

To protect a system, we need to understand all the layers - only then can we attain situational awareness.



Layers of protected system (Tarmo Oja)

Cybernetica helps analyse all the critical layers of the protected system enabling you to enhance your cyber situational awareness.

References

Cybersecurity projects in defence

Minerva / European Space Agency

Project duration: 3 years 5 months

We are building a local unsupervised machine learning enabled cybersecurity toolset that will assist an IT administrator or an auditing security analyst of an SME to rapidly comprehend complex local and external network activity and to effectively identify problem areas and suspicious behaviour.

Novel methods in machine learning model visualisation and entropy-based structural modelling of network behaviour will be the focus points of this technology de-risking activity.

Machine learning powered visualisation of the interactions and dependencies between network hosts in a mixed-use setting, i.e. employee personal traffic, business traffic, IoT devices, cloud services, helps local IT administrator to understand effectiveness of current network defences and address found issues with host based or perimeter based mitigations.

Visualisation of the interactions and dependencies between network hosts in a mixed-use setting, i.e. employee personal traffic, business traffic, IoT devices, cloud services, helps local IT administrator to understand efficiency of network defences and address found issues with host based or perimeter based mitigations.

FAMOUS & FAMOUS 2 / European Commission

Project duration: 5 years

The project “European Future Highly Mobile Augmented Armoured Systems” (FAMOUS) aims at maximising synergies, standardisation and interoperability capabilities of armoured vehicles to address highly demanding requirements while introducing innovative and promising new technologies and concepts. Several types of vehicles are targeted, such as future All-Terrain Vehicle (ATV), Light Armoured Vehicle (LAV) and Main Battle Tank (MBT) upgrades.

VORMSI / United States Air Force Research Laboratory

Project duration: 6 years

Estonia and United States have signed a Memorandum of Understanding to collaborate in the development of a security threat sharing and correlation system.

The project will be performed in collaboration between Cybernetica, United States Air Force Research Laboratory (USAFRL) and respective national entities that benefit from or are responsible for carrying out such information exchange. While the system will initially be used by Estonia and the United States, one of the requirements considered in the design is the capability to include additional allies in the information exchange.

The project aims to research, design and implement standards, processes, methods and rules for the exchange and processing of cybersecurity information between nations. Enabling information exchange and processing on various levels (from threats to ongoing attacks) between multiple nations with different relationships of trust and enabling different rules of information exchange dependent on the current cyber situation.

EUCINF / European Commission

Project duration: 3 years

EUCINF aims to create a comprehensive European library of adaptable software components that can be seamlessly integrated into Cyber and Information Warfare (CIW) systems. EUCINF will demonstrate its capabilities through the implementation of three operational CIW scenarios, aligning with the requirements from the Ministries of Defense as end-users, while adhering to legal regulations and societal expectations. These scenarios encompass information warfare attacks on friendly deployed forces, hybrid attacks falling below the threshold of conventional warfare, and military deception.

A key objective is to introduce and apply technologies and concepts previously not applied in the defence sector. This notably includes novel AI-enabled components for the collection, enrichment, categorisation and clustering of information as well as the detection of propaganda, mis- and disinformation that were trained and applied, so far, in the civil sector only, and whose potential for application in the military context shall now be evaluated. This includes methods to process audio, video, image and text data, to interlink and contextualise information and to support the detection and remediation of information warfare activities. Furthermore, tools for the extraction of cyber threat intelligence from log data, such as IP addresses, domains etc.

R&D for cybersecurity

We conduct scientific research for projects where theoretical results are applied in practical applications.

Our scientists collaborate closely with engineers, and as a result of such cooperation, several technologies have become indispensable parts of our daily lives. These technologies include trusted digital signatures, timestamping, internet voting, and secure multi-party computation.

Our offering for R&D capabilities includes:

World-class research
Close cooperation with institutes, centres of excellence, public and private sector partners in Europe, United States and Japan. Development of security and privacy standards.

Security-by-design
Risk-based design and architecture of systems with a very high level of security. Access control, authentication and authenticity, private, public and hybrid clouds.

Cryptography
In-depth research on public key infrastructure (PKI), cryptographic protocols, post-quantum cryptography with a focus on internet voting, identity, privacy.

AI and machine learning
Applications of AI and machine learning in cybersecurity and e-government. Privacy-preserving machine learning and artificial intelligence.

References

Helping military stay several steps ahead with applied R&D

ECYSAP / European Defence Industrial Development Programme

Project duration: 4 years 3 months

The main objective is to develop and implement of innovative theoretical foundations, methods and research prototypes integrated towards providing a European operational platform for enabling real-time Cyber Situational Awareness (CSA) with rapid-response defensive capabilities and decision-making support for military end-users.

An integrated and modular platform for national/European security purposes and military expeditionary operations will be developed, which shall become a real-time defensive system with cyber response capabilities, automated and deployable in areas of operations (national/European) interconnected between intelligent nodes.

The industrial consortium (including Cybernetica, Leonardo, Indra, Airbus) developing the platform is being led by the Spanish company Indra Sistemas. Cybernetica participates in design, R&D activities with main focus on visualisation of cyberspace and knowledge storage and management.

PROVENANCE / DARPA

Project duration: 4 years

Cybernetica was granted funding by DARPA (Defense Advanced Research Projects Agency, United States of America) under PROVENANCE project to bring value to communication between the public and private sector by creating techniques for constructing meaningful zero-knowledge proofs.

The goal is to improve government interactions with citizens, companies, and other governments by enabling them to confidentially handle sensitive data. The first key objective of PROVENANCE is to build proof structures that capture real-world settings, without unreasonable simplifications. This means developing new data encoding techniques and proof structures that make the verification of proof meaningful in the real world. A further goal is to select a proof system where the deployment fits the number of stakeholders and their trust. Once the proof structure and system are known, a tool is needed to translate the statement into the underlying cryptographic constructions.

Contact our team for more information:

Sander Valvas
Head of Cybersecurity Department
sander.valvas@cyber.ee

Marko Jõemets
Head of Cybersecurity Research and Development
marko.joemets@cyber.ee

cyber.ee/solutions/cybersecurity

cyber.ee/industries/defence