CYBER & SECURITY SOLUTIONS

CYBERSEC DEFENCE SUITE

In strategy. In mission. In theatre.

LEONARDO

Today Defence forces operate across highly contested, multi-domain environments where digital architectures are increasingly exposed even under hostile, degraded, or disconnected conditions.

Defence systems deployed on land, at sea, in the air and in space rely on a distributed mesh of sensors, mission equipment, and command networks.

Connectivity enhances operational effectiveness but also expands the attack surface available to hostile actors. Adversaries exploit degraded communications, limited trust among tactical nodes, legacy hardware constraints, and the physical vulnerability of deployed assets. Hybrid threats employ coordinated cyber and kinetic actions, often enabled by malicious AI, to disrupt command chains and degrade operational tempo.

Armed Forces require reinforced cyber capabilities to maintain the security posture of systems — including armoured vehicles, land systems, vessels, and satellites — throughout the mission lifecycle, preserving cyber mission assurance despite evolving cyber threat vectors.

The challenge is no longer to protect individual systems as isolated assets, but to preserve the operational continuity of an interconnected digital mission environment, where a disruption to one node can affect the effectiveness of the entire mission chain.

Therefore, such environments require cyber defence capabilities that can operate consistently across several assets belonging to different domains, classification levels and mission conditions.

The priority is shifting from securing individual components to protecting the broader system-of-systems, ensuring continuity of operations, safe maintenance, and rapid recovery under contested conditions and in multi-domain contexts.

A COMPLETE, ORCHESTRATED CYBER DEFENCE ECOSYSTEM DELIVERING MISSION-LEVEL ASSURANCE

Maintaining decisive advantage in the cyber domain requires a transition from isolated defensive measures to integrated cyber mission assurance capabilities.

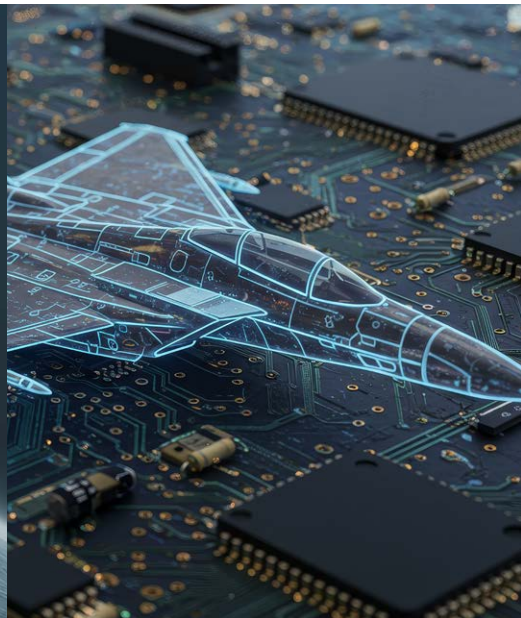
Leonardo's Cybersec Defence Suite introduces a unified, adaptive approach to provide complete situational awareness ensuring systems remain protected, observable, and trusted across all mission phases.

Unlike standalone security components, it provides a coherent protection chain that combines Leonardo's global cyber knowledge and awareness through the Global Cybersec Platform, tactical coordination through the Tactical Cybersec Platform, and autonomous field enforcement through the Cyber Cells.

This federated model transforms cyber defence from fragmented tools to a unified, orchestrated capability embedded across the mission-critical lifecycle.

At the core of Leonardo's Cybersec Defence Suite, there is the concept of cyber mission assurance: guaranteeing the integrity, availability, and trustworthiness of mission-critical systems against continuously evolving cyber threats.

By consolidating strategic intelligence, tactical synchronisation, and local enforcement into a coherent, federated architecture, the Cybersec Defence Suite enables defence forces to operate with confidence in highly dynamic and degraded environments.



THE TECHNOLOGICAL FOUNDATION

Leonardo's Cybersec Defence Suite is an integrated cyber defence architecture that translates the global cyber threat knowledge base into tactical coordination and autonomous edge enforcement, ensuring that deployed systems (e.g. armoured vehicles, land systems, vessels, and satellites) remain continuously protected, trusted, and operational throughout the mission lifecycle.

It combines three mutually reinforcing layers — the Global Cybersec Platform, the Tactical Cybersec Platform and Cyber Cell — to **deliver a continuous defence chain from the strategic level to edge systems.**

Designed for native integration with Leonardo systems and mission architectures, it reduces integration effort while strengthening the cyber readiness of deployed systems.

The Cybersec Defence Suite can interface with cyber Command & Control and kinetic-domain C2 systems, supporting a shared multi-domain command-and-control

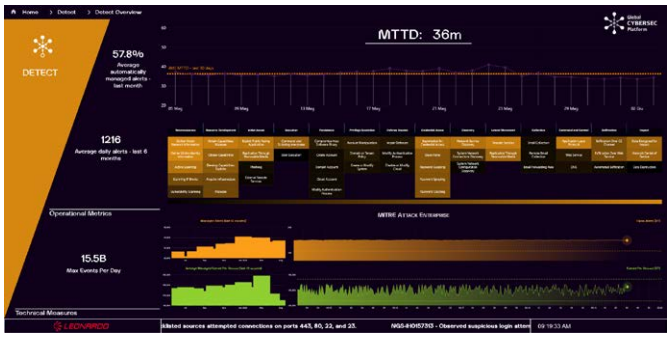
GLOBAL CYBERSEC PLATFORM

A high-capacity cyber defence platform to guarantee end-to-end management of the cyber domain. Built on **multi-agentic AI and Zero Trust principles**, it provides cutting-edge capabilties structured according to NIST CSF 2.0 functions. The Global Cybersec Platform key functions include:

- **Cyber Threat Prediction & Emulation** to anticipate and pre-empt adversary actions.
- **Deep Cyber Observability** to transform weak signals into actionable insights.
- **Cyber Respond & Recovery** to support mission continuity even under severe disruption.

Delivered through **sovereign deployment models,** managed security feeds or dedicated service configurations, it acts as the authoritative source of cyber knowledge for the entire ecosystem.

Its knowledge base is transformed into actionable policies, advanced detection capabilities and integrity baselines that can be distributed down to tactical and edge levels.



Global Cybersec Platform - Detect Smart View

TACTICAL CYBERSEC PLATFORM

Deployed at the logistic bases as the operational bridge between the strategic cyber layer and deployed systems, managing multiple Cyber Cells, securing maintenance cycles, and ensuring synchronization with the Global Cybersec Platform in both connected and disconnected mission profiles.

Tactical Cybersec Platform

The Tactical Cybersec Platform's capabilities include:

- **Secure execution and logging** of maintenance activities.
- **Cyber Observability of tactical and on-board telemetry,** mapped against global threat to identify advanced cyber anomalies
- **Distribution of updated policies, and integrity baselines** to all connected Cyber Cells

Its federated design supports fleet-wide situational awareness and consistent enforcement of security posture. By aggregating data from multiple Cyber Cells and redistributing updates according with knowledge base evolution, the Tactical Cybersec Platform federates deployed systems into a coordinated and constantly updated cyber defence framework.

CYBER CELL

A ruggedized edge component that provides autonomous cyber protection for systems operating in contested or disconnected environments.
Local capabilities include:

- **Local Identity:** enforces authorized access and ensures accountability of actions performed on the protected system.
- **Local Integrity:** verifies software, firmware, configurations, and file systems against trusted baselines.
- **Local Observability:** correlates on-board telemetry, logs, metrics and events to detect threats and anomalies.
- **Firewalling**: secures critical trust boundaries by policing network traffic and blocking malicious injection vectors, especially during ground maintenance and software upload cycles.

Cyber Cell

Tactical Cybersec Platform – Main Dashboard

LOGICAL MODEL

The Cybersec Defence Suite adopts a federated, system-of-systems architecture designed for Defence operations.

The Global Cybersec Platform operates at the Force's remote strategic coordination centre, providing authoritative cyber-intelligence, global threat awareness, and continuous enforcement feeds to tactical deployments while acting a central pane of glass that federally aggregates overall cyber defence capabilities.

At the logistic base, the **Tactical Cybersec Platform acts as the operational link between the strategic layer and the field and on-board deployed assets**, ensuring secure maintenance, data consolidation, and controlled distribution of updated policies and models.

On the ground, at sea, in the air or in space, **multiple Cyber Cells are installed on distributed systems** — tanks, ships, aircraft, satellites or unmanned systems — forming the protected edge of the ecosystem **locally observing and enforcing cyber defence capabilities.**

Each Cyber Cell autonomously enforces cyber posture during missions, regardless of connectivity conditions, while feeding operational data back into the tactical and strategic layers.

This model ensures that **updated knowledge base flows top-down and is enforced at the edge**, while operational telemetry flows bottom-up, maintaining a continuously aligned and updated security posture across the system.

OPERATING MODES

Leonardo's Cybersec Defence Suite provides a federated chain of strategic, tactical, and edge elements designed to ensure coherent **cyber mission assurance** across the full mission lifecycle.

ASYNCHRONOUS MODE

Designed for fully isolated missions, such as land or air systems operating in degraded or disconnected conditions, this mode ensures that **systems remain protected and observable even when fully disconnected** from the tactical layer.

The Cyber Cell collects and analyses logs locally. pon return to base, it synchronizes with the Tactical Cybersec Platform, uploading cyber data from the mission while downloading cumulative updates from the knowledge base.

SYNCHRONOUS MODE

Typical for naval or fixed installations or other operational contexts with sustained communications.

Multiple Cyber Cells transmit data in real time to the Tactical Cybersec Platform, enabling correlation across Cyber Cells and immediate application of updated policies or mitigation actions.

In both modes, the Tactical Cybersec Platform remains federated with the Global Cybersec Platform, ensuring that knowledge base updates continuously flows downward, while mission telemetry flows upward for broader operational assessment.

USE CASES

LAND

Deployed across armoured vehicles and land systems operating in isolation or degraded communications, the Cybersec Defence Suite ensures **secure maintenance cycles, integrity verification, and detection of on-board cyber anomalies.**

The Cyber Cell supports the entire mission profile:

- → **before field operations** it receives updated policies and integrity baselines;
- → **during field operations** it autonomously performs local cyber observability, enforces firewalling, identity control and integrity monitoring;
- → **after field operations** it synchronises mission logs with the Tactical Cybersec Platform, enabling the Command to analyse incidents, discover silent threats, and issue updated countermeasures.

For large land formations, the Tactical Cybersec Platform correlates data from multiple vehicles to identify coordinated attack patterns, lateral movement attempts, or recurring adversarial TTPs, strengthening fleet-level resilience.

SEA

The Cybersec Defence Suite **supports vessels with on-board Tactical Cybersec Platform and Cyber Cells local continuous connectivity, enabling correlation of cyber events and rapid distribution of updated policies** across multiple network zones.

Ships typically operate with local sustained communications, allowing the Tactical Cybersec Platform to maintain a real-time operational picture of all connected on-board Cyber Cells.

Cross-correlation highlights multi-vector attacks targeting different segments of the ship, allowing rapid enforcement of new detection models, rules or containment actions.

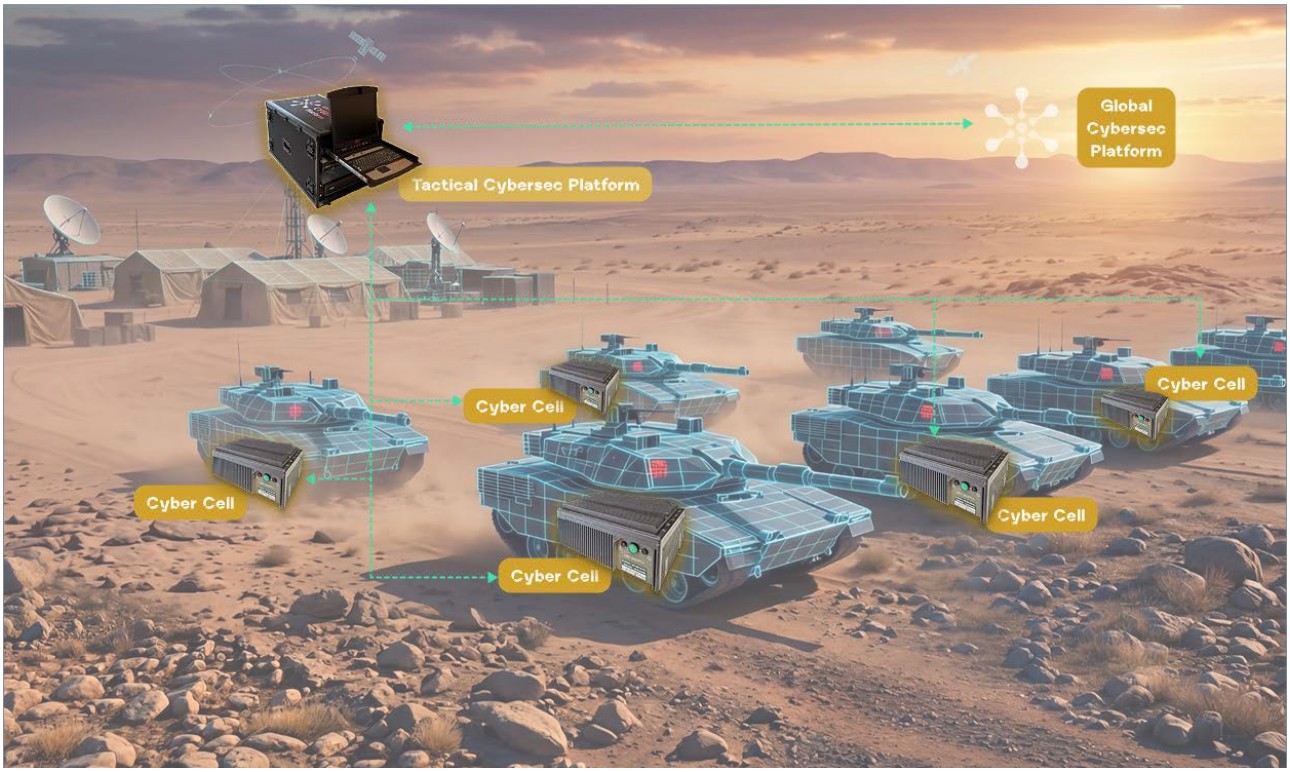
During maintenance alongside, **Cyber Cells verify the integrity of configuration updates and ensure that only authenticated and validated software is introduced** on board, mitigating risks coming from supply-chain compromise or insider activity.

AIR

The Cybersec Defence Suite protects avionics and mission equipment through telemetry observability, identity control, integrity assurance, and controlled maintenance workflows. To counter intermittent or contested in-flight communications, the **Cyber Cell preserves trusted execution throughout the sortie by securely logging all telemetry;** the ground-based Tactical Cybersec Platform performs the offline, post-flight verification —ingesting stored logs to reconstruct the mission's threat timeline and quickly re-verify the aircraft's security posture.

SPACE

The Cybersec Defence Suite ensures continuity and trustworthiness of space assets exposed to advanced threats. Cyber Cells deployed on ground control and payload support segments enforce identity and integrity checks, while synchronisation with the Global Cybersec Platform supplies updated defence models tailored to space-focused adversaries. **Tactical-level correlation strengthens protection of command sequences and uplink channels, safeguarding mission continuity and operational sovereignty.**



Example of deployment on land systems

KEY VALUES

STRATEGIC-TO-FIELD CYBER DEFENCE

A unified Cyber Defence architecture combining strategic, tactical, and edge components into a coherent operational framework.

MULTI-DOMAIN READY

Designed for land, air, naval and space domains, ensuring a federated approach and consistent protection for joint and combined operations at any classification level.

FEDERATED SYSTEM-OF-SYSTEMS

Strategic nodes continuously update the Tactical Cybersec Platform, which aggregates and federates deployed units to enable cyber defence at fleet level.

NEVER TRUST, ALWAYS VERIFY

A native Zero Trust foundation enforcing continuous authentication, dynamic authorization, and runtime integrity checks across deployed systems.

END-TO-END CYBER OBSERVABILITY

A single, continuous detection chain spanning deployed asset-sand operational phases — from operations to maintenance to recovery.

GLOBAL THREAT KNOWLEDGE AT THE EDGE

Strategic threat knowledge from Leonardo's Global Cybersec Centre turns into actionable detection, protection, and enforcement at tactical and field levels.

CYBER CAPABILITIES BEYOND PRODUCTS

Not a collection of disconnected tools, but a unified cyber defence ecosystem delivering mission-level assurance through an orchestrated, end-to-end architecture.

NATIVE INTEGRATION WITH LEONARDO ECOSYSTEM

Seamlessly embedded into Leonardo products, systems and architectures, reducing integration overhead and strengthening system cyber readiness.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

LDO_UK26_01931 06-26

leonardo.com