CYBER & SECURITY SOLUTIONS

C3NTRIX

Leonardo Cyber Command & Control

LEONARDO

The growing use of the cyber domain for disinformation, sabotage, and low visibility intrusions has made cyberspace a key domain in the fight against hybrid threats. Adversaries increasingly blend criminal tactics with state sponsored operations. Their goals include targeting critical infrastructure, manipulating public opinion, and undermining national autonomy. They often remain below the threshold of open conflict.

In response to this rapidly evolving environment, defense organizations are investing heavily in innovative cyber command and control capabilities. Although some countries have achieved high level of maturity in joint, multi domain C2 cyber operations, overall visibility remains limited, and levels of capability vary widely.

This disparity underscores the need for interoperable, scalable solutions that can be tailored to different armed forces and operational requirements.

To meet these challenges, a next generation C2 cyber platform must deliver timely situational awareness of a constantly shifting threat landscape. It must also automate detection and analysis workflows to shorten reaction time and effectively manage events. It must enable rapid, coordinated responses to hybrid and below threshold attacks—even when attribution is unclear—and integrate cyber and kinetic operations to maintain tactical coherence across land, air, sea and digital domains.

Beyond immediate response, commanders require advanced decision support tools. These tools combine rapid risk assessment with dynamic Course of Action (CoA) planning. The platform should also support the design and execution of targeted offensive cyber operations—through modules for discovery, anonymization and action execution—while unifying previously fragmented capabilities into a single, modular architecture.

Ultimately, leveraging automation and data integration, a next generation C2 cyber system must secure strategic advantage. It also needs to synchronize multi domain campaigns and strengthen national resilience in an increasingly contested digital era.

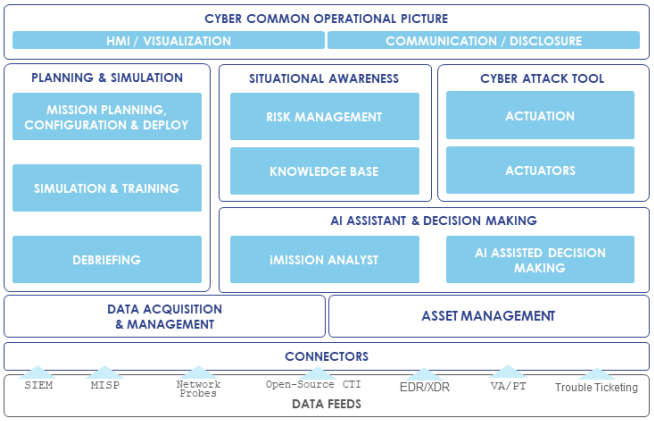
SHAPING THE FUTURE OF CYBER OPERATIONS

C3NTRIX is Leonardo's next-generation platform for cyber command and control that enables and orchestrates the planning, simulation, execution, and debriefing of cyber operations. Powered by AI-enhanced analytical capabilities, it supports the entire decision-making cycle — from defensive actions to active response — across all operational levels.

It offers a Cyber Common Operational Picture for an integrated view of the operational scenario and structured event management along the command chain. The platform supports risk assessment of both static and dynamic cyber threats to guide mitigation strategies. The AI assistant, iMission Analyst, helps define and identify the most effective CoAs, while asset monitoring detects Indicators of Compromise (IoCs) and anomalous behaviors to strengthen defense and operational readiness. Additionally, C3NTRIX includes a Cyber Attack Tool for orchestrating and executing proactive cyber operations.

LOGICAL MODEL

These features are based on an integrated and modular architecture that combines proprietary Leonardo products with commercial off-the-shelf solutions, delivering a flexible, modular solution for complex cyber operations.



MAIN FUNCTIONALITIES

C3NTRIX integrates all key capabilities into a single platform for cyber command and control, delivering comprehensive functionalities for managing, analyzing and executing missions in complex, multi-domain environments.

Cyber Common Operational Picture (COP)

→ Integrated visualization of the operational picture: scenarios, missions, assets, networks, geolocation and roles.
→ Structured management of alerts, notifications and information sharing across the command chain.

Planning & Simulation

→ Configuration and planning of missions with the definition of Courses of Action (CoA) and Enhanced Courses of Action (ECoA).
→ Simulation of missions and immersive training of personnel in realistic and controlled environments.
→ Post-mission analysis (debriefing) with feedback collection, configuration updates and automated report generation.

Situational Awareness

Network monitoring, vulnerability identification, and attack prediction to enhance critical infrastructure security and ensure mission success.

Actuation

Management and orchestration of offensive cyber operations across all phases of the cyber kill chain, from preparation to attack execution.

AI Assistant & Decision Making

→ Automated analysis of CoA and ECoA with predictive simulation and support to the operational mission cycle.
→ Decision support through prioritization, prediction and recalculation of Courses of Action.

Data Acquisition & Management

→ Collection and transformation of operational data through optimized and integrated ETL pipelines.
→ Scalable data management through storage, search, visualization and advanced processing on distributed architectures.

Asset Management

Continuous monitoring of availability and security, with automated discovery and centralized inventory of network assets.

Data Feeds

Integration of structured, unstructured, and threat intelligence feeds, including CTI, SIEM, EDR, ticketing, vulnerability and network probes.

KEY FEATURES

- → **Comprehensive coverage of both defensive and offensive cyber operations, with a unified view of physical and cyber domains.**
- → **Integration with multi-domain C2 systems,** with the ability to operate across all military levels: tactical, operational, and strategic.
- → **Simulation of operations and early evaluation of Course of Action effectiveness.**
- → **Reduced operational response times through the use of Artificial Intelligence.**
- → **Secure exchange of data, commands, and procedures between national, allied, and partner systems,** with compatibility with NATO and civil standards and third-party platforms.
- → **Data sovereignty ensured,** with the ability to build a proprietary knowledge base.
- → **Modular and scalable architecture,** integrating proprietary and commercial components, adaptable to specific operational objectives.
- → **Integration of tools for conducting offensive and defensive cyber operations.**

For more information:
cyberandsecurity@leonardo.com

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

LDO_IT25_01494 08-25

leonardo.com