LEONARDO CYBER & SECURITY SOLUTIONS

DEFENCE4FUTURE SUITE

LEONARDO

Digitalization and the resulting hyper-connectivity have significantly impacted the Defence sector, which is continuously adapting its processes and infrastructures to take full advantage of these technological opportunities, but, at the same time, has to prepare to deal with new threats to national security coming from the cyber space. Nowadays cyber-attacks rely on hybrid actions carried out by state-directed or state-supported actors designed to threat both physical and cyber assets remaining below the detection and attribution threshold.

Leonardo supports the increase of Defence capabilities and expertise needed to face cyber-physical risk acting as a:

- **system integrator**, proactively involving all national and international partners who can actively contribute to Defence programs;
- **technology provider**, designing and developing products, systems, services and solutions that contribute to the national and supranational digital sovereignty.

LEONARDO APPROACH TO CYBER-PHYSICAL RISKS

Leonardo provides a structured approach to security aimed at improving Defence capabilities across all domains. According to this paradigm, the cyber domain provides tools, skills and intelligence capabilities needed not only to conduct operations in the cyber space, but also to ensure operations continuity in the other domains.

Since the security of cyberspace is increasingly synergic with that of physical space, in order to effectively protect Defence infrastructural assets, it is essential to address these two issues in a parallel and coordinated manner. This is possible not only through platforms able to gather all data coming from on field fixed and mobile sensors, but also through control rooms integrating information from cyber and physical domains.
These control rooms integrate as well operational procedures, decision support processes, radio communications and leverages technologies for a superior situational awareness and informed decision making.

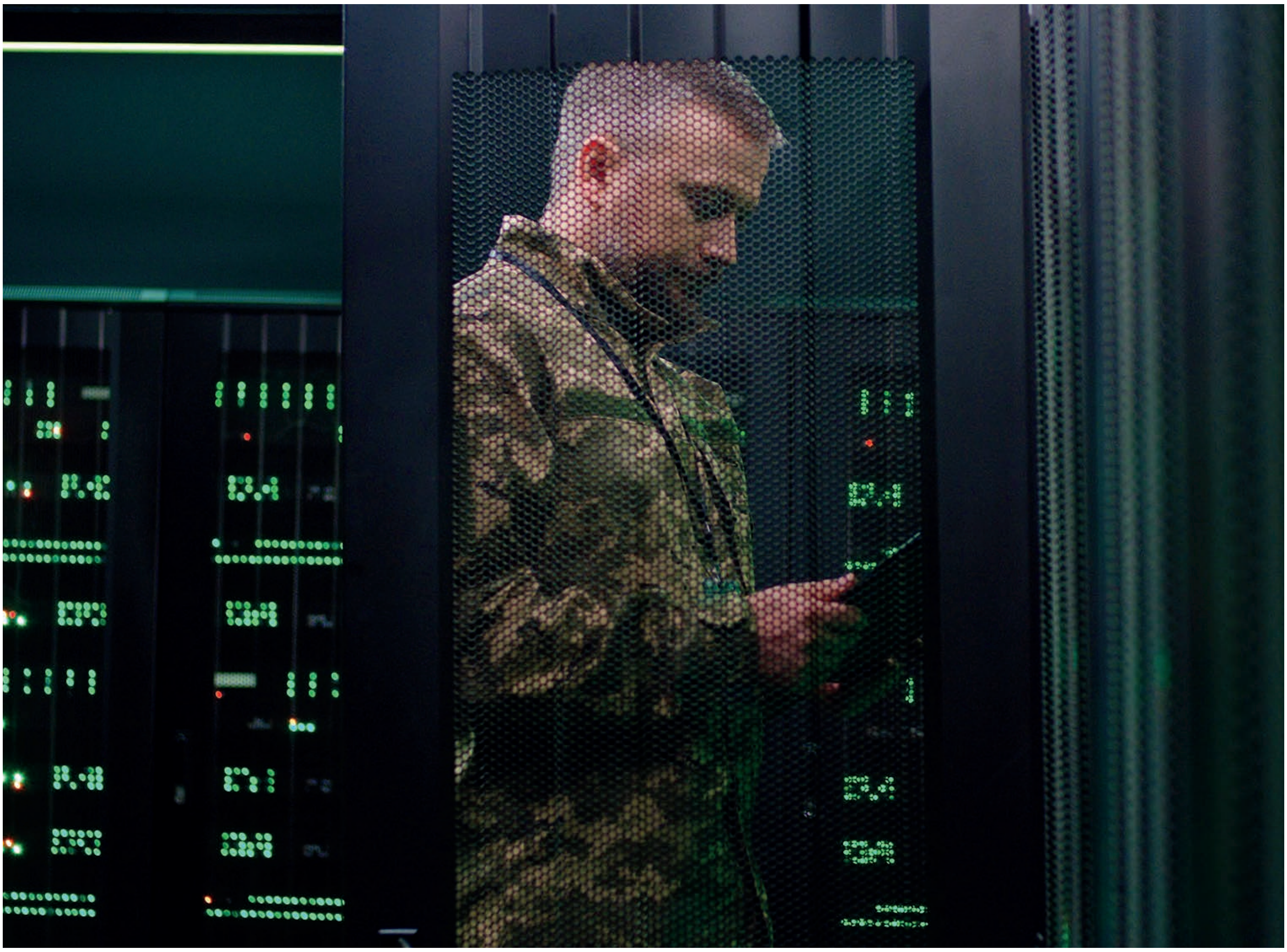
BENEFITS

- Continuous strengthening of the cyber resilience levels of the whole Defence infrastructural assets (military basis, ports and airports) through the adoption of innovative models and tools to be applied also to the supply chain.
- Decrease cyber-physical risks leveraging on a multi-domain and comprehensive situational awareness.
- Availability of valuable and actionable information which can be used to rapidly implement targeted prevention actions and policies.
- Timely implementation of cyber response and containment activities with local critical data management including remediation actions and malware analysis outcome.
- Improvement of personnel’s cyber defence and cyberwarfare skills through innovative modelling and simulation tools for automatic generation of highly complex training theatres (digital twins).

The identification of infrastructural assets, the quantification of the impact caused by their compromise, and the definition of guidelines to ensure their cyber resilience constitutes a particularly complex, but fundamental point to strengthen Defence information systems. It is a process that necessarily requires also the involvement of the entire Defence supply chain to adopt 'secure by design' policies throughout the development life cycle of military systems.

To support Defence in the verification of operational resilience and the definition of business continuity and disaster recovery plans, Leonardo's digital solutions provide:

- reproduction of realistic scenarios through virtualization techniques that allow to test the resilience of even extremely complex operative contexts or legacy technologies;
- cooperative, competitive and technology evaluation processes based on the integration with external virtual and physical environments;
- high reuse of the virtualized infrastructures and architectures for cyber testing and evaluation enabling a continuous effortless improvement cycle taking into account the dynamic structure of systems;
- support in operational resilience verification activities and the definition of business continuity and disaster recovery plans.



As for infrastructural communications, intended for uses other than high impact tactical contexts, Defence requires fully integrated solutions that are both reliable and robust, designed to operate in military basis, ports and airports, etc., also during critical situations.

Leonardo provides Defence with a complete communications packages addressing:

- Transport networks (both wired and wireless)
- Access to wired (LAN) and wireless networks
- PAGA/PABX
- Clock distribution
- Operational communications.

Mission Critical Communications

LTE/5G	LTE infrastructures **support data intensive applications**. Leonardo has a system integration approach providing third party infrastructure to supply extensive coverage, integration of commercial networks, hot spots (with tactical bubbles or network-in-a-box configuration).
TETRA	**Adaptanet®** is a complete modular, scalable and flexible family of **TETRA products**, satisfying requirements ranging from single-site to national networks. The s**ystem supports technology enhancements with full IP communications**, and is complemented by terminals dispatching solutions and service applications.
Network Integration	The **CSP (Communications Service Platform)** enables the integration of multi-technology networks with unified users and application management; it is at the heart of Leonardo **RIM (Italian acronym for Hybrid multi radio vector network)** supporting the progressive evolution from narrowband to broadband professional communications networks. CSP implements the LMR portion of **3GPP standard LMR –IWF (Interworking Function)** allowing the integration of 3GPP MCX applications.
Push-To-Talk over cellular	**Push to talk over cellular** is the way to provide professional services over broadband networks. Leonardo **CSP MCX platform** is a complete solution fully compliant with 3GPP standards enabling mission critical communications over LTE and 5G. **Designed to take advantage of broadband mission critical enhancement**, MCX can also be deployed as an OTT (Over-The-Top) application on an existing commercial network and provides a fully featured android client and a web based dispatcher.

Increasing the resilience of its infrastructures is critical for the Defence sector, so that it can anticipate, withstand and adapt to adverse conditions, stresses, attacks or compromises. Assuming that it is impossible to completely eliminate cyber-physical risks, it is indeed necessary to ensure that operations continue even in the face of a physical, cyber or hybrid attack. To do so, it is necessary to continuously monitor, process and analyse a huge amount of multi-domain data in order to extract, in a timely manner, concise, contextualised and immediately usable information to support decision-making processes and optimally cope with the new converging risks.

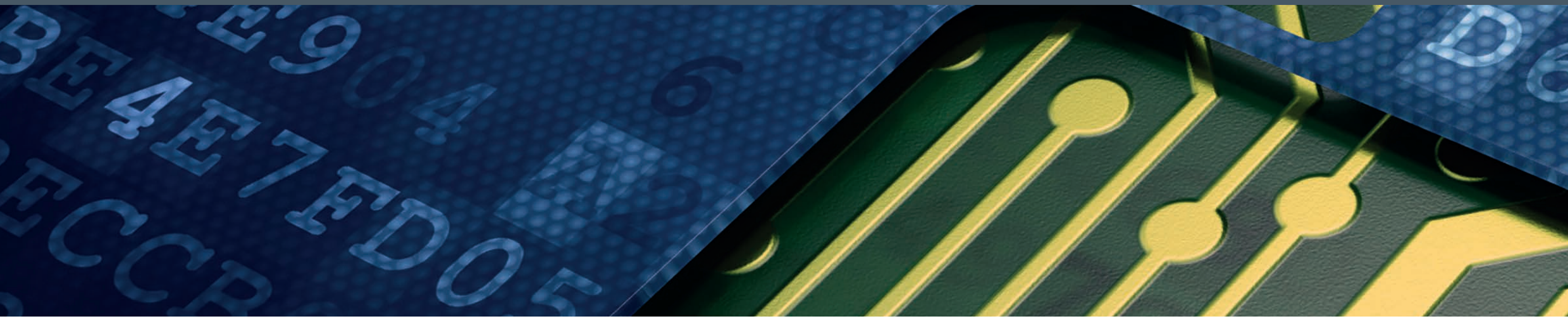
Leonardo's Integrated Control Centre is able to:

- integrate a large number of different sensors and subsystems to collect events and alarms both from physical and cyber domains;
- filter and correlate alarms through intelligent rule based engine;
- geographically represent the on-field scenario thanks to an effective and flexible GUI integrated with a powerful GIS;
- automate operations and guide operators in the analysis of the situation by following standard and emergency operating procedures;
- boost on-field squad coordination through the integration of Mission Critical Communication;
- track and record all events to enhance post event analysis, investigation and debriefing.

Global Monitoring

SC2	Physical Security management oriented platform **able to gather all data coming from on field fixed and mobile sensors** (PIDS, AC, Video Surveillance, UAVs), **correlate events** and **drive operators through the resolution of the incident** thanks to the automated workflow system (Orchestrator).
X-2030	A new model of control room system **based on system of systems paradigm**. **X-2030** integrates operational procedures, decision support processes, radio communications and **leverages technologies for a superior situational awareness and informed decision making**. Designed to integrate existing systems, provides an innovative user interface based on virtual assistant and natural language understanding.
GANIMEDE	A solution for the **audio and video analysis based on AI**, instantiable through different frameworks on different harware platforms and applicable on live or recorded streams. Leonardo Artificial Intelligence Labs can develop and train customized solutions. **Natively integrated in SC2 or X-2030 platforms**, Ganimede provides a set of API for applications in third party systems.

CYBER SECURITY & RESILIENCE: WHERE READINESS MATTERS



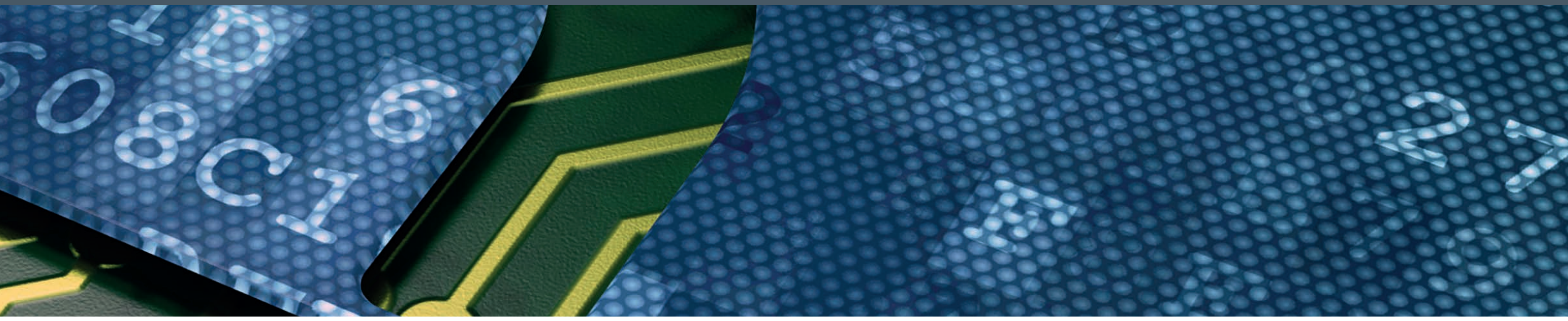
In the context of current geopolitical crises, cyber-attacks have often anticipated and supported the offensive and defensive strategies of adversaries through actions on the cyber domain that can cause significant impacts also on the real world. Such actions are particularly effective due to the difficulty of attribution, worsened by an increasingly blurred dividing line between states and non-state actors.

Leonardo can support Defence customers in the design, deployment, commissioning and management of cyber security and data protection services, platforms and solutions in order to defend and secure military IT/OT infrastructures to make them more resilient against new and highly complex cyber threats.
Leonardo offering includes:

- cyber security professionals and certified engineers, with specific skills for the implementation of secure by design infrastructures;
- effective prediction and identification of advanced threats and highly structured intelligence process management and orchestration;
- design and implementation of physical and logical infrastructures supporting high-classification projects;
- preparatory activities for obtaining certifications and homologations needed for classified information management;
- enhancement of situational awareness capabilities in cyber operations to support commanders in understanding and managing cyber risks;
- timely implementation of tailored detection rules and response actions through a proprietary EDR (Endpoint Protection & Response) solutions;
- local management of vulnerability data, response actions and malware analysis;
- access to multiple malware analysis tools from a single dashboard, optimizing COTS (Commercial Off-The-Shelf) usage costs.

Cyber Security & Resilience	
Design and Build services	Services based on a **proprietary approach and an established process for designing and building security management of on-prem infrastructures** (SOC, CERT, IOC).
Leonardo Engineering Assurance Profile for Cyber Resilience (LEAP4CR)	**Methodology based on NIST and MITRE frameworks**, developed to define the level **of Cyber of a new or already existing product/system/service**. It defines a comprehensive view of security ensuring effective security governance, while **allowing the association between resilience techniques and the ability to contain a given type of attack.**
Cyber Information Superiority (CIS) suite	Suite composed of a **combination of platforms providing threat intelligence, end point protection and malware analysis based upon Information Superiority concept** applied to the cyber domain. It aims to obtain valuable and actionable information which can be used to rapidly implement targeted prevention, response and containment actions.
Cyber Situational Awareness System (CSAS)	The system is **designed to keep security teams and commanders informed about what is happening in terms of their IT perimeter security status and support decision making**. It provides an **information centralizing platform** that aggregates and displays data through both high-level management views and technical-operational ones.

CYBER TRAINING: WHERE KNOWLEDGE MATTERS



Education and training activities play a key role in the prevention and early detection of new cyber threats. Cyber space operators dedicated to the protection of national strategic infrastructures must be able to promptly, rapidly, and cooperatively test and implement the actions necessary to contain threats and minimize their impacts. It's necessary to create a cultural network made up of integrated and shared security skills that help raise awareness of the new risks among all the parties playing a key role in guaranteeing the Countries' security. It is therefore essential to invest in training activities that, on one side, strengthen security knowledge in terms of technologies, processes and regulations, and on the other, develop the 'human factor', enhancing the ability to share context and interpret information, which is crucial to effectively manage crises arising from security attacks and incidents with large-scale impacts.

Leonardo supports Defence to enhance skills and capabilities needed to recognize and deal with the new cyber-physical risks that threaten Countries security through an advanced training centre providing:

- integrated and multilateral approach to global security issues that goes beyond the concept of delivering training content on specific topics;
- dedicated training ecosystem to exchange ideas, improve skills of cyber defence teams, propose and test new approaches and collect new requirements in the field of cyber protection;
- automatic generation and setup of complex training theatres and reusable exercise scenarios;
- context-driven training paths, implemented using proprietary training platforms based on the simulation of real operational contexts;
- interoperability with remote orchestrators, scenarios and native capabilities to share cyber gaming fields and be federated with other cyber ranges services;
- immersive training experience based on skills gained by Leonardo's security teams in critical domains.

Cyber Training	
Cyber & Security Academy	An innovative training centre to promote cyber security awareness increase competencies by means of a **complete training portfolio delivered by expert trainers leveraging advanced platforms for hands on exercises.**
Cyber Trainer	**Cloud-based platform to train and keep up to date both security professionals and non-expert users** managing the whole training process (training needs, formal learning, exercises, certification).
Cyber Range	Integrated environment for **immersive realistic simulations of cyber-attack and defence scenarios** and advanced simulation to **test the cyber resilience of military infrastructures**.

HIGHLIGHTS

- A tailored maturity model and innovative simulated test environments to assess the cyber security posture of Defence people, process and both existing and new technologies.
- Interoperable systems and solutions designed and developed to capitalize multi-domain heterogeneous information in order to obtain an operational advantage on the adversary.
- Proprietary platform enabling cyber security scenario-planning exercise in virtualized environment in order to prepare for inevitable cross ecosystem incidents.

ABOUT CYBER AND SECURITY SOLUTIONS DIVISION

With experience in information technology, communications, automation, physical and cyber security, Leonardo Cyber and Security Solutions Division generates synergies by joining its expertise to support enterprises, agencies, public safety, security and emergency organizations. Our offer includes solutions for the security and protection of critical infrastructures, transport infrastructures, major events and stadia, cyber security, integrated networks systems and secure communications that enable reliable and efficient information management.

Secure Cloud & Digital

Global Monitoring

Mission Critical Communications

Cyber Security & Resilience

For more information:
cyberandsecurity@leonardo.com

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

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorised in writing. We reserve the right to modify or revise all or part of this document without notice.

MM09151 06-23