CYBER & SECURITY SOLUTIONS

DEFENCE4FUTURE SOLUTIONS

LEONARDO

Il cyberspazio è ormai riconosciuto come un dominio operativo conteso, nel quale le azioni digitali possono produrre effetti significativi sul dominio fisico, sulle infrastrutture critiche e sulla continuità delle operazioni. Tali attività rientrano frequentemente in strategie ibride adottate da attori statali e non statali, che sfruttano deliberatamente la complessità dell'attribuzione e l'elevato livello di interdipendenza tra reti militari, infrastrutture civili e operatori privati. In questo contesto, la Difesa contemporanea trascende i domini tradizionali, integrando il cyberspazio e lo spazio quali domini permanentemente contesi, nei quali la resilienza, la continuità operativa e il mantenimento del controllo delle capacità digitali costituiscono requisiti fondamentali.

SOLUZIONI COMPLETE

Leonardo supporta la crescente esigenza di capacità di Difesa multidominio per far fronte ai rischi cyber-fisici, operando in qualità di:

- **fornitore tecnologico,** attraverso la progettazione e lo sviluppo di piattaforme, sistemi e soluzioni di livello Defence-grade, che contribuiscono alla sovranità digitale nazionale e sovranazionale;
- **system integrator**, coordinando partner nazionali e internazionali che concorrono a programmi di Difesa all'interno di ambienti operativi complessi e federati.

Leonardo adotta un approccio strutturato, orientato alla missione, alla sicurezza, volto al rafforzamento delle capacità di Difesa in tutti i domini. In tale paradigma, il dominio cibernetico fornisce strumenti, competenze e capacità di intelligence indispensabili non solo per la condotta della cyber defence, ma anche per garantire la continuità della missione negli altri domini.

I Joint Operations Centers avanzati rivestono un ruolo essenziale nell'integrazione delle informazioni provenienti dai domini cyber e fisici, delle procedure operative, dei processi di supporto decisionale e delle comunicazioni sicure. Grazie all'impiego di tecnologie avanzate, essi assicurano una situational awareness completa e multidominio e consentono processi decisionali tempestivi e informati in ambienti complessi e contesi.

In questo scenario, il defence cloud rappresenta un abilitatore operativo critico. Esso garantisce un'integrazione dei dati sicura, resiliente e in tempo reale attraverso i domini terrestre, marittimo, aereo, spaziale e cibernetico, a supporto della superiorità informativa. Collegando sensori, piattaforme e sistemi di comando e controllo, il cloud accelera i processi decisionali, migliora l'interoperabilità tra forze armate, alleati e rafforza la resilienza complessiva, fungendo da spina dorsale digitale delle operazioni multidominio.

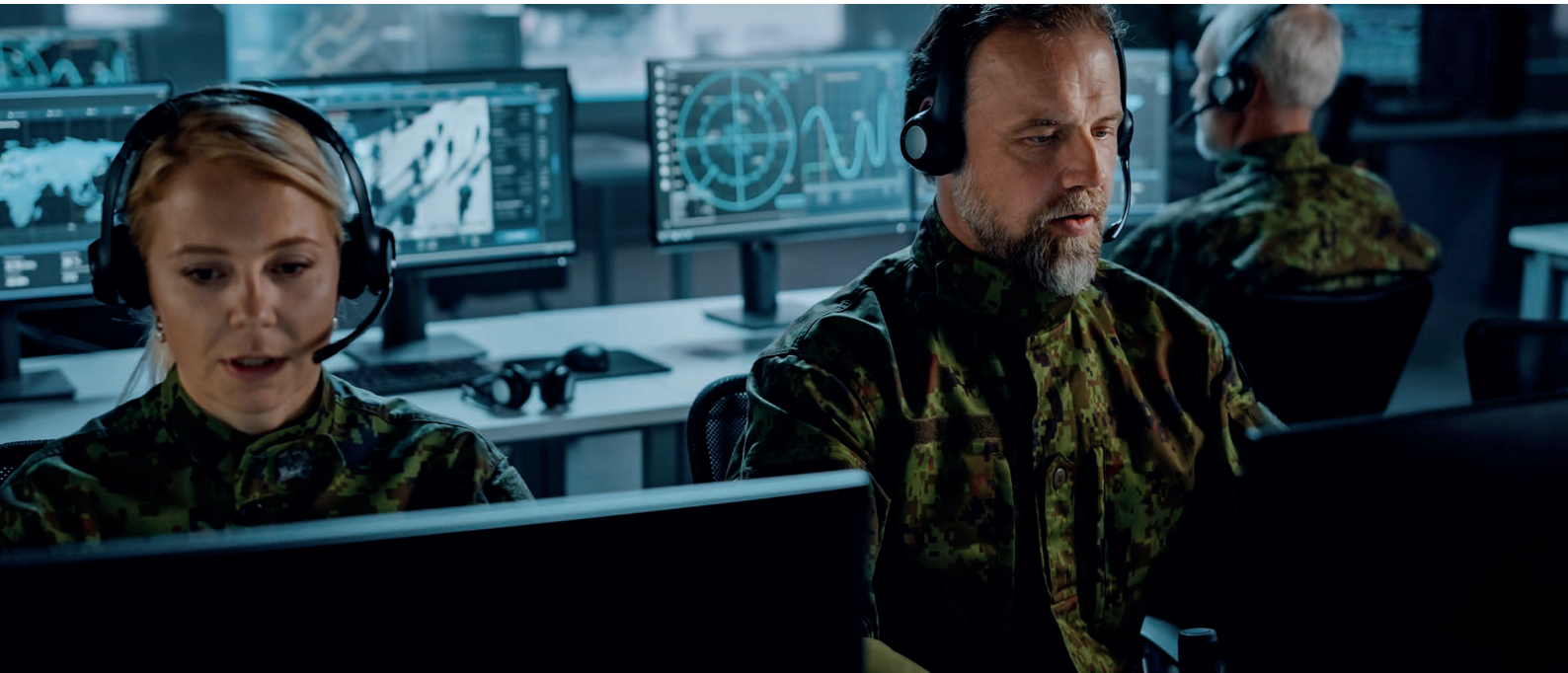
BENEFICI

- Rafforzamento continuo dei livelli di resilienza cibernetica delle infrastrutture di Difesa e degli asset mission-critical, mediante modelli e strumenti innovativi applicati anche agli ambienti operativi e lungo l'intera catena di fornitura della Difesa.
- Riduzione dei rischi cyber-fisici attraverso una situational awareness completa e multidominio, a supporto dei processi decisionali operativi.
- Disponibilità di informazioni affidabili, validate e immediatamente utilizzabili, al fine di consentire attività tempestive di prevenzione, risposta e supporto decisionale.
- Esecuzione tempestiva di azioni di risposta e contenimento cibernetico, incluse le attività di remediation, l'analisi del malware e la gestione locale dei dati operativi critici.
- Potenziamento delle competenze in ambito cyber defence e cyber operations attraverso strumenti avanzati di modellazione e simulazione, in grado di abilitare ambienti di addestramento realistici e l'impiego di digital twin.

SECURE DIGITAL: GLOBAL MONITORING & SICUREZZA

La sicurezza delle caserme, delle basi militari e dei quartieri generali operativi riveste un'importanza primaria, in quanto tali infrastrutture costituiscono nodi critici per il comando e controllo, nonché per la prontezza delle forze.
Garantirne la protezione richiede un monitoraggio continuo e la capacità di individuare e contrastare rapidamente potenziali minacce. L'applicazione dell'intelligenza artificiale alla video-analytics incrementa in modo significativo le capacità di early warning, consentendo il rilevamento automatizzato, in tempo reale, di comportamenti anomali, intrusioni e attività sospette.
Parallelamente, le capacità di massive data analytics basate su IA supportano le operazioni militari e il monitoraggio degli asset attraverso la correlazione di informazioni provenienti da fonti multiple, l'individuazione di pattern ricorrenti e la generazione di informazioni utilizzabili a fini operativi. Nel loro insieme, tali capacità rafforzano la situational awareness, migliorano la force protection e consentono un approccio più proattivo ed efficace alle operazioni di difesa.

genesiX	**genesiX** è la nuova piattaforma web di Leonardo che, nei diversi domini operativi, valorizza i dati e i sistemi disponibili al fine di generare informazione e garantire superiorità conoscitiva e decisionale. → Raccolta delle informazioni provenienti da fonti dati strutturate (database, archivi) e non strutturate (video, sensori, media). → Elaborazione, correlazione e analisi dei dati con il supporto dell'intelligenza artificiale, mediante dashboard e indicatori contestuali specifici. → Geolocalizzazione di tutte le informazioni su mappe multilivello (digital twin), gestione di eventi e risorse (sicurezza, operazioni, manutenzione) e supporto decisionale attraverso workflow procedurali. → Coordinamento delle operazioni sul campo tramite applicazioni mobili e sistemi di comunicazione (MC_linX).
Forge2Know	**Forge2Know** è una piattaforma di Big Data analytics progettata per l'ingestione, l'archiviazione e l'analisi di dati sia strutturati sia non strutturati, trasformandoli in informazioni utilizzabili a fini operativi. La piattaforma integra funzionalità avanzate di AI/ML, data governance ed elaborazione in tempo reale, scalabili su grandi volumi di dati, a supporto di processi decisionali basati sui dati (data-driven decision-making).



Le piattaforme di sicurezza di Leonardo sono progettate per fornire una Common Operational Picture (COP) a supporto delle funzioni di Comando e Controllo, della gestione della sicurezza, della situational awareness e della resilienza, creando un sistema integrato di safety e security per la protezione di caserme, basi militari, quartieri generali operativi, impianti e aree critiche da monitorare e controllare.

SC2	**SC2** è una soluzione PSIM (Physical Security Information Management) altamente flessibile, scalabile e affidabile, progettata per la gestione della sicurezza con un elevato livello di configurabilità e la capacità di realizzare un'architettura federata, in grado di collegare siti differenti. La soluzione consente di ottenere una situational awareness completa, integrando informazioni, risorse e allarmi, tutti gestibili e attivabili su una mappa geolocalizzata. La piattaforma supporta l'integrazione di sistemi di sicurezza di numerosi brand eterogenei e può essere ulteriormente potenziata mediante funzionalità di video analytics basate su intelligenza artificiale. SC2 integra decine di brand relativi a differenti sistemi di sicurezza. La soluzione offre inoltre capacità di comando e controllo di droni e robot, l'integrazione di body worn camera e sistemi di comunicazione vocale, al fine di coordinare in modo efficace le risorse operative sul campo.
Ganimede	**Ganimede** è il framework avanzato di Leonardo per la gestione di algoritmi basati su intelligenza artificiale dedicati all'analisi di sorgenti audio/video, sia in streaming live, sia registrate. Una singola piattaforma, dotata di oltre 20 algoritmi facilmente configurabili e applicabili a sorgenti video multi-brand già esistenti, con la possibilità di applicare più algoritmi contemporaneamente sullo stesso flusso video. Algoritmi sviluppati ed addestrati nei laboratori Leonardo specializzati in AI, con scalabilità progettuale fino a 10.000 telecamere e 20 algoritmi differenti. Nativamente integrato nelle piattaforme Leonardo, Ganimede fornisce interfacce dedicate per l'integrazione in sistemi di terze parti.

Un defense and combat cloud è un'infrastruttura digitale distribuita e sicura, progettata per supportare operazioni militari in tutti i domini. Consente la raccolta, la fusione e la diffusione dei dati in tempo reale provenienti da sensori, piattaforme e sistemi di comando e controllo. Progettato con elevata resilienza e robustezza cyber, garantisce la continuità operativa anche in ambienti contesi. L'architettura supporta interoperabilità, scalabilità e rapido dispiegamento delle applicazioni mission-critical. Sfruttando l'intelligenza artificiale e l'analisi avanzata dei dati, potenzia la superiorità decisionale e l'efficacia operativa

Secure Cloud	il **Defence cloud** è un'infrastruttura basata su cloud che garantisce accesso distribuito alle risorse e interconnessione tra diversi domini di sicurezza, con livelli di classificazione eterogenei, a supporto della conduzione delle operazioni, comprese le operazioni multidominio. E' articolato in: → **High-Classified Region (Private)** garantisce elevata affidabilità e continuità operativa, sfruttando la resilienza architetturale e servizi dedicati di disaster recovery. → **Low-Classified Region (Public\Hybrid)** basata su fornitori di cloud la cui sicurezza è assicurata tramite la cifratura dei dati "at rest", "in transit" e "in use". → **High-Ranking Edge Systems** soluzione trasportabile e dispiegabile in contesti operativi e tattici. La soluzione è supportata da: **MovinCloud** piattaforma per la gestione della governance, orchestrazione, provisioning, sicurezza e monitoraggio di cloud multidominio e multi-classifica. **Forge2Know**, piattaforma di Big Data e Analytics che trasforma i dati in insight strategici mediante algoritmi di intelligenza artificiale, a supporto dei processi e delle decisioni mission-critical.

COMUNICAZIONI CRITICHE

Le comunicazioni critiche costituiscono un abilitatore fondamentale per consentire alla Difesa di condurre operazioni in basi militari, unità navali, porti, aeroporti e altre infrastrutture strategiche, anche in contesti critici che richiedono soluzioni integrate di informazione e comunicazione affidabili, robuste e progettate per essere impiegate in ambienti mobili e in situazioni di emergenza.
Leonardo opera sia come fornitore tecnologico (TETRA, DMR, applicazioni broadband MCX e reti ibride) sia come system integrator, fornendo infrastrutture di comunicazione mission-critical chiavi in mano.

MCX (broadband)	**MC_linX** è la piattaforma di comunicazioni broadband mission-critical di nuova generazione, basata sullo standard 3GPP MCX, progettata per supportare servizi sicuri e in tempo reale di voce, dati e video per operatori di sicurezza, protezione civile e infrastrutture critiche. La soluzione include un'applicazione mobile client, un dispatcher web e strumenti di gestione, garantendo funzionalità push-to-talk, messaggistica multimediale, servizi di localizzazione e situational awareness in modalità seamless su reti LTE/4G/5G e WiFi.
TETRA / DMR (narrowbnd)	**Adaptanet** è una suite modulare e scalabile di prodotti TETRA, progettata per garatire comunicazioni sicure, cifrate, resilienti ad alte prestazioni. La soluzione abilita i servizi core essenziali per le comunicazioni voce e dati, oltre a un'ampia gamma di servizi supplementari e avanzati ed è articolata in: core network, stazioni radio base, terminali, sistema di gestione (Network Management System), dispatcher e molto altro. Le soluzioni **ECOS DMR** si caratterizzano per un elevato grado di scalabilità e flessibilità, che consente di fornire la configurazione più adatta alle specifiche esigenze del Cliente. La stessa stazione radio base può operare in **DMR Tier II**, con opzione **simulcast** e modalità **analogica FM** dinamica, oppure in **DMR Tier III**, in configurazione simulcast o cellulare.
Hybrid networks	La **Hybrid Network Platform** è una soluzione progettata per garantire un'infrastruttura integrata narrowband-broadband durevole, a supporto dell'evoluzione delle reti professionali. La core network fornisce funzioni di coordinamento e controllo per la rete integrata, oltre ai servizi core per i componenti **TETRA, DMR** e **MCX**.

CYBER SICUREZZA E RESILIENZA

Nell'attuale contesto geopolitico, il cyberspazio è diventato un dominio operativo pienamente conteso, in cui le azioni cibernetiche difensive e offensive anticipano, accompagnano e amplificano le operazioni militari in tutti i domini. Le attività cyber possono produrre effetti tangibili sul mondo fisico, incidendo su infrastrutture mission-critical, catene di comando e continuità operativa, mentre la difficoltà di attribuzione e la convergenza tra attori statali e non statali aumentano complessità e incertezza.
In questo contesto, la cyber resilienza rappresenta una capacità operativa cruciale, strettamente interconnessa con la capacità di condurre operazioni cibernetiche. Essa consente alle organizzazioni di Difesa di preservare la continuità della missione, mantenere la libertà di manovra e supportare la superiorità decisionale, operando anche in ambienti degradati, contesi o negati. Le capacità cyber difensive e offensive agiscono quindi in sinergia per proteggere, modellare e sostenere le operazioni nei domini terrestre, marittimo, aereo, spaziale e cibernetico.
Leonardo supporta i clienti della Difesa attraverso un approccio cyber orientato alla missione, basato su piattaforme avanzate, centri operativi federati e capacità intelligence-driven. Integrando monitoraggio continuo, abilitazione alle operazioni cyber, ambienti di addestramento realistici e threat intelligence proattiva, Leonardo rafforza la capacità di prevenire, resistere, rispondere e riprendersi da minacce cibernetiche complesse, supportando al contempo la pianificazione e l'esecuzione delle operazioni cyber lungo l'intero ciclo operativo.

Cyber Defence	**Global Cybersec Platform** è una piattaforma unificata di Cyber Defence che consente il controllo end-to-end del dominio cibernetico attraverso un ecosistema AI multi-agente. **Global Cybersec Center** è il centro di eccellenza cyber di Leonardo, che sfrutta la Global Cybersec Platform e opera attraverso un modello federato, garantendo la sovranità nazionale e l'autorità decisionale.
Cyber Operations	**C3NTRIX** è una piattaforma di C2 Cyber di nuova generazione che abilita e coordina la pianificazione, simulazione, esecuzione e debriefing delle operazioni cyber. Grazie ad analisi amplificate dall'intelligenza artificiale, supporta i processi decisionali, dalle azioni difensive fino alla risposta cyber attiva.
Cyber Backbone	→ **C-THINK** è una piattaforma di Cyber Threat Intelligence che supporta i team di analisti in ambienti altamente classificati, abilitando la previsione e la prevenzione delle minacce più probabili. → **LENS** è una piattaforma EDR innovativa e flessibile, basata su agenti e sonde distribuite, che consente il rilevamento precoce delle anomalie e l'esecuzione di azioni configurabili di risposta e contenimento.
Zero Trust	**Leonardo Zero Trust** è un ecosistema di livello Defence-grade basato su tecnologie europee, che copre tutte le fasi, dalla gestione degli accessi e delle autorizzazioni fino alla protezione dei dati in transito, at rest e in uso, a supporto delle operazioni in ambienti multidominio e multi classifica.
Cyber Simulation	**LX Range** è un Cyber Range che consente la simulazione di teatri ibridi federati altamente realistici, al fine di creare ambienti di addestramento avanzati per esperti cyber, testare la sicurezza cibernetica di prodotti e tecnologie e valutare la cyber resilience di infrastrutture complesse e distribuite.

HIGHLIGHTS

→ Un “maturity model” su misura e ambienti di simulazione innovativi e avanzati per valutare la postura di cyber resilienza del personale, dei processi e delle tecnologie, sia esistenti sia di nuova introduzione, nel contesto della Difesa.

→ Sistemi e soluzioni interoperabili, progettati e sviluppati per valorizzare informazioni eterogenee provenienti da diversi domini, al fine di ottenere un vantaggio operativo sull’avversario.

→ Un portafoglio integrato di piattaforme e soluzioni proprietarie che abilita operazioni cyber, resilienza, addestramento e supporto alla missione in ambienti realistici, virtualizzati e operativi, preparandosi a gestire incidenti complessi cross-domain e cross-ecosystem.

For more information:
cyberandsecurity@leonardo.com

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

mm09151-0126
January 2026 © Leonardo S.p.A.

leonardo.com