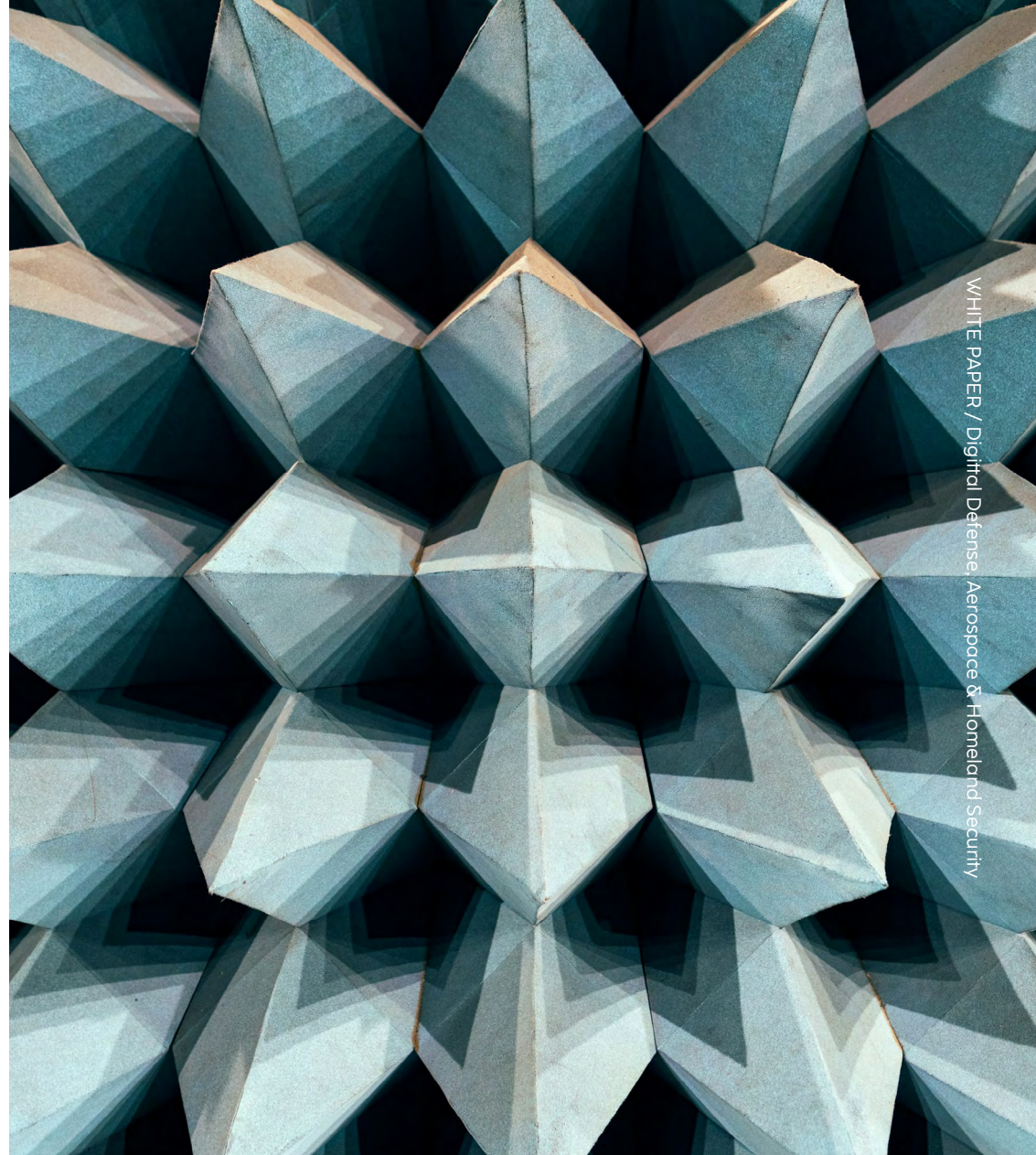




WHITE PAPER

# Digital Defense, Aerospace & Homeland Security





# Autori

## Massimiliano Camilli

Technical Manager  
Defense, Space &  
Homeland Security

ENGINEERING

[massimiliano.camilli@eng.it](mailto:massimiliano.camilli@eng.it)

in [Massimiliano Camilli](#)

## Chris Draska

VP of Sales for North  
America - Industries  
eXcellence

ENGINEERING

[chris.draska@eng.it](mailto:chris.draska@eng.it)

in [Chris Draska](#)

## Ernesto La Mattina

Head of AI & Advanced  
Analytics Research Unit

ENGINEERING

[ernesto.lamattina@eng.it](mailto:ernesto.lamattina@eng.it)

in [Ernesto La Mattina](#)

## Fabio Sala

VP of Industries  
eXcellence - USA

ENGINEERING

[fabio.sala@eng.it](mailto:fabio.sala@eng.it)

in [Fabio Sala](#)

## Giuseppe Vella

Head of Border  
and External Security  
Research Unit

ENGINEERING

[giuseppe.vella@eng.it](mailto:giuseppe.vella@eng.it)

in [Giuseppe Vella](#)



# Sommario

01 / <b>Trend, sfide e opportunità</b> .....	2
02 / <b>ENG per Digital Defense</b> .....	4
03 / <b>Defense</b> .....	8
04 / <b>Cybertech: sicurezza digitale per la difesa</b> .....	11
05 / <b>ENG Industries eXcellence: digital design, manufacturing &amp; supply chain solutions for A&amp;D</b> .....	12
06 / <b>Intelligence</b> .....	14
07 / <b>Maritime</b> .....	16
08 / <b>Space</b> .....	18
09 / <b>Homeland Security</b> .....	20
10 / <b>Qual è il futuro della Digital Defense?</b> .....	23



# Trend, sfide e opportunità

Trend, sfide e opportunità



## Negli ultimi anni assistiamo a minacce e fenomeni globali di diverso tipo che richiedono interventi significativi nella Difesa da parte dei governi.

Oltre che a livello territoriale, il campo di azione della Difesa si è allargato ad altri ambiti della società, fra i quali quello economico/finanziario, e soprattutto cibernetico. La scacchiera delle azioni difensive è cambiata, diventando più diffusa e multidimensionale.

Per far fronte all'evolversi dei conflitti e delle tecnologie, i dipartimenti di Difesa collaborano strettamente con il settore privato, garantendo l'utilizzo di tecnologie all'avanguardia per mitigare il rischio di obsolescenza. Tali dipartimenti devono quindi avviare alleanze con partner tecnologici in grado di fornire competenze e conoscenze complementari rispetto a quelle a loro disposizione. Nel fare questo, i governi non possono più affidarsi solo ai

loro fornitori tradizionali, le aziende del comparto Difesa, ma anche ad aziende del settore high-tech che godono, in assoluto, di un maggiore investimento nella ricerca.

Una cooperazione fra questi mondi non è solo auspicabile, ma necessaria per mettere a fattor comune le competenze di ognuno e governare la Trasformazione Digitale in un settore critico per nazioni e cittadini.

È proprio sul tema della cooperazione che emerge una seconda sfida: la collaborazione fra i dipartimenti di Difesa.

I vari rami non riescono a scambiare quei dati e informazioni necessari alla Trasformazione Digitale degli Enti. Inoltre, l'impiego di piattaforme digitali suscita forti resistenze interne ai dipartimenti per molteplici ragioni: innanzitutto per gli investimenti in termini di denaro e tempo richiesti (basti pensare alla formazione) e poi perché, affidandosi sempre più alla tecnologia, tutti gli apparati militari saranno sempre più interconnessi, aumentando l'esposizione nei confronti dei rischi cyber. Le sfide sono quindi molteplici e noi di ENG, con la nostra lunga esperienza a supporto dei governi, siamo pronti ad affrontarle con progetti di rilevanza strategica.



# ENG per la Digital Defense

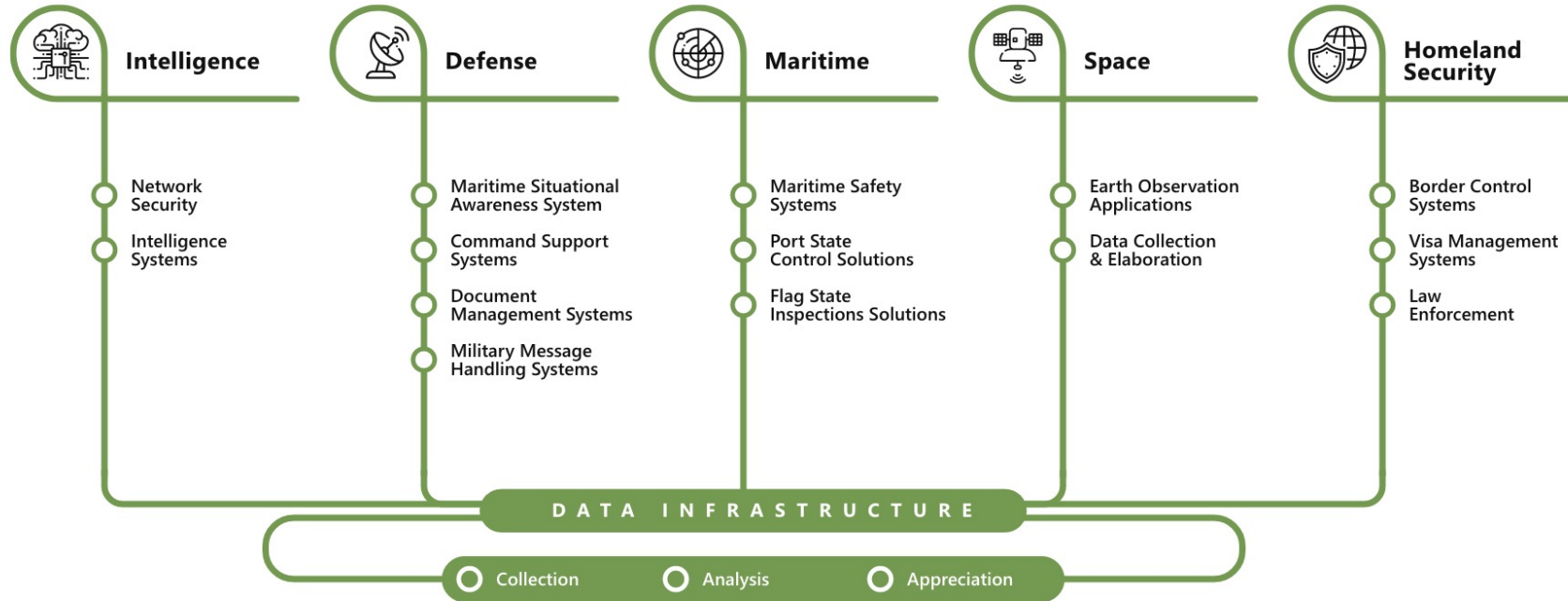
## WHITE PAPER / Digital Defense, Aerospace & Homeland Security

Operiamo nella Digital Defense, Aerospace & Homeland Security per **facilitare l'acquisizione, la gestione e la distribuzione sicura dei dati relativi alle operazioni militari e di sicurezza nazionale.**

Ci occupiamo inoltre del supporto logistico, legato al dominio terrestre, marittimo, aereo, spaziale e cibernetico. Supportiamo e affianchiamo le aziende in modo proattivo, posizionandoci come un partner tecnologico credibile e affidabile per le Istituzioni nazionali e internazionali che si occupano di Difesa e Sicurezza.

I nostri obiettivi in ambito Digital Defense, Aerospace e Homeland Security sono:

- **promuovere** il paradigma del Dual Use militare/civile, favorendo il riutilizzo delle competenze acquisite e delle soluzioni realizzate in entrambi i settori;
- **contribuire** proattivamente all'innovazione tecnica, tecnologica e di processo in domini di nicchia altamente specializzati;
- **supportare** gli utenti nel loro percorso di Trasformazione Digitale.



<b>ENABLING SERVICES</b>	Business & User Services	IT Consulting	Mobile Applications	UX & Service Design	Digital Communication & Strategy
	<b>ENABLING TECHNOLOGIES</b>				
	AI & Advanced Analytics	Cybersecurity	IoT	AR / MR / VR	



# Digital Defense, Aerospace & Homeland Security

Abilitiamo l'acquisizione, la gestione e la distribuzione sicura dei dati delle operazioni militari, della sicurezza nazionale e del supporto logistico in ambito marittimo, terrestre, aereo, spaziale e cibernetico.

**25+**

ANNI DI  
ESPERIENZA

**15+**

CLIENTI

**50+**

SPECIALISTI  
DI BUSINESS

**20+**

PROGETTI  
ATTIVI

**5+**

PROGETTI DI  
RICERCA ATTIVA

ADVISORY

MANAGED SERVICES

TECHNOLOGY & IMPLEMENTATION







## vDESK: un alto livello di sicurezza e flessibilità

Con la Trasformazione Digitale è cresciuto anche il senso di vulnerabilità da parte delle organizzazioni. Per rispondere alle loro esigenze di sicurezza, abbiamo innovato le nostre soluzioni puntando sempre alla massima protezione dei dati.

**vDESK** trasforma la tradizionale workstation in un **Digital Workplace**. È una piattaforma sicura e crittografata, integrata con altri sistemi IT dell'organizzazione. Permette di digitalizzare le attività lavorative, aumentando flessibilità e produttività, così da ridurre costi e tempi di fermo. Tramite un'unica dashboard vDESK permette di:

- profilare gli utenti in modo semplice e intuitivo
- utilizzare una serie di applicazioni integrate
- avere supporto da un assistente virtuale
- impostare avvisi e notifiche chiaramente visibili
- avere informazioni costantemente aggiornate.



# 03 Defense

Defense



Realizziamo e manteniamo una vasta tipologia di sistemi, che supportano gli utenti nelle attività operative e logistiche:

- sistemi di Supporto al Comando;
- sistemi di Maritime Situational Awareness e Sistemi dedicati all'Intelligence;
- sistemi per la Messaggistica Militare;
- sistemi di Gestione Documentale;
- sistemi a Supporto della Sanità Militare e soluzioni per l'Information/Cybersecurity.

La collaborazione tra il nostro team di esperti e il Centro di Competenza Engineering ECM (Enterprise Content Management) ha inoltre dato impulso all'implementazione di sistemi dedicati alla trattazione delle informazioni e in particolare alla **gestione documentale** e alla **messaggistica militare** (STANAG 4406).

Per quanto riguarda la prima, come ENG abbiamo sviluppato e curiamo la manutenzione del Sistema di Gestione Documentale e Protocollo Informatico che ogni

anno gestisce oltre 4 milioni di documenti e più di 17.000 utenti per lo Stato Maggiore della Difesa, Segredifesa e l'Esercito Italiano.

Per quanto attiene invece ai sistemi a supporto della **Sanità Militare**, come ENG siamo coinvolti nella reingegnerizzazione ed espansione funzionale del Sistema Informativo Sanitario dell'Amministrazione Difesa (SISAD).

Inoltre, ci stiamo occupando della realizzazione del Sistema Informativo Ospedaliero (SIO) che sarà adottato dall'Ospedale Militare del Celio.

Infine, nell'ambito del settore Difesa, limitatamente al mondo del **classificato**, ci occupiamo di Information/Cybersecurity relativamente ai seguenti aspetti:

- sicurezza delle applicazioni;
- sicurezza perimetrale di infrastrutture informatiche (Network Security Architecture, Vulnerability Assessment, Event and Log Management, End Point and Mobile Security, Data Loss Prevention, Advanced Persistent Threat);

- Cyber Threat Intelligence e sicurezza nello scambio di informazioni tra reti a diverso livello di classifica, sicurezza di infrastrutture critiche (sviluppo di sistemi di supporto alle decisioni e policy di prevenzione e/o intervento a seguito della valutazione, attraverso modellazione e simulazione dinamica, di impatti dovuti a incidenti e/o minacce su infrastrutture critiche interconnesse).

Inoltre, abbiamo collaborato direttamente anche con l'Agenzia Europea per la Difesa su due particolari temi: Strategic Technology Foresight e l'approvvigionamento di materiali e componenti per le industrie europee per la Difesa. Nell'ambito delle attività di Ricerca & Innovazione, coordiniamo due progetti europei complementari:

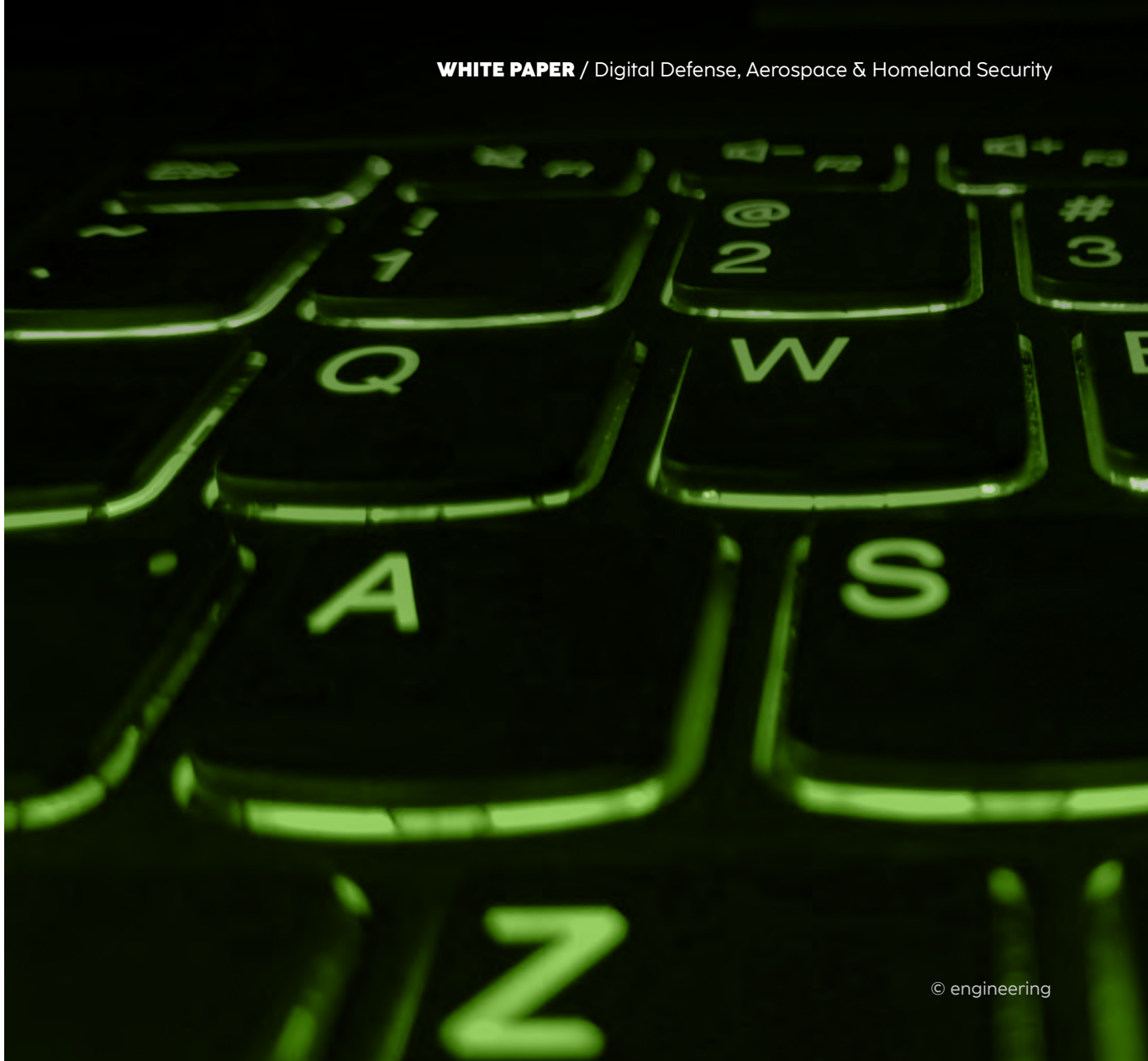
- **PYTHIA** (Predictive methodology for TecHnology Intelligence Analysis), finanziato nel contesto del programma Preparatory Action on Defense Research, con l'obiettivo di sviluppare una metodologia innovativa per effettuare previsioni tecnologiche strategiche nel contesto della Difesa, attraverso strumenti di Big Data Analytics e modelli previsionali. Il consorzio si caratterizza per un'ampia copertura



geografica, con partner di 6 diversi Paesi europei le cui organizzazioni sono Ministeri della Difesa, think tank specializzati in strategia e Difesa, provider e integratori di tecnologie.

- **SOLOMON** (Strategy-Oriented anaLysis Of the Market fORces in EU defeNse) che fornisce all'Unione Europea metodologie e strumenti per assicurare alle industrie di armamenti europei una filiera di produzione affidabile. L'obiettivo è ridurre al minimo la dipendenza tecnologica da Paesi extra-europei, legata ai regolamenti di restrizione ITAR e EAR, per definire le possibili roadmap per affrontare questi rischi.

Un altro progetto finanziato da DG\_DEFIS Unit A3 è **SEANICE** (Antisubmarine Warfare European Autonomous Networked Innovative And Collaborative Environment) che mira a studiare, sviluppare e impostare le basi per la fornitura di un avanzato sistema di difesa antisommergibile. Questo progetto, basato su uno scenario operativo, sfrutta nuove tecnologie all'avanguardia come la gestione dei dati, le tecnologie di comunicazione, l'Intelligenza Artificiale e un mix di asset, con e senza pilota, per svolgere nel migliore dei modi una missione ASW (Anti-Submarine Warfare).



# Cybertech: sicurezza digitale per la difesa



Cybertech, la società del Gruppo Engineering specializzata in soluzioni e servizi per la sicurezza informatica, ha consolidato negli ultimi anni la sua presenza nel settore della Difesa, Spazio e Sicurezza Nazionale, offrendo innovazioni per le principali istituzioni italiane del settore.

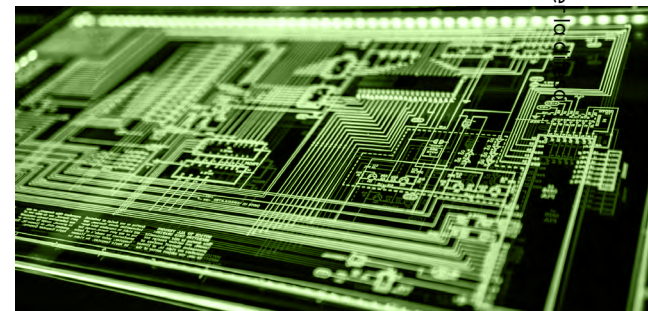
I nostri clienti continuano ad affidare ai nostri esperti una vasta gamma di servizi che coniugano una comprovata esperienza professionale, un'approfondita conoscenza del settore e tecnologie all'avanguardia, quali ad esempio:

- servizi per l'analisi forense, per estendere e sostanziare la capacità investigativa a fronte di incidenti di sicurezza informatici, indagando le attività svolte su ogni tipo di dispositivo (end-user devices, mobile devices, macchinari di rete o web);
- progettazione ed erogazione di servizi di protezione delle identità digitali, gestione e controllo degli accessi, per

assicurare il corretto uso da parte del personale autorizzato e prevenire eventuali intrusioni;

- servizi di monitoraggio continuo delle attività su reti e dispositivi al fine di garantire una protezione efficace e affidabile di tutti gli asset aziendali.

Con tecnologie innovative e pratiche avanzate, il nostro team continua a offrire soluzioni di sicurezza personalizzate per rispondere alle esigenze mutevoli dei nostri clienti, garantendo resilienza e prontezza nel panorama delle minacce odierno.





# ENG Industries eXcellence: digital design, manufacturing & supply chain solutions for A&D

Anche la nostra divisione globale **Industries eXcellence** è coinvolta in progetti di Digital Defense, Aerospace & Homeland Security. In questa fascia di mercato, la produzione è indirizzata direttamente alle agenzie governative e deve conformarsi a rigidi standard e regolamenti, soprattutto negli Stati Uniti, fra le maggiori potenze mondiali in termini di esercito, marina e aviazione. Il nostro team Engineering USA opera in questo settore da anni per fornire consulenza, soluzioni tecnologiche e servizi dedicati all'Industria 4.0 per il Dipartimento della Difesa USA.

Per quanto riguarda l'ambito tecnologico, gli appaltatori della Difesa, che producono aerei e navi per gli Stati Uniti, hanno l'esigenza di velocizzare i tempi di progettazione e produzione. Grazie alla nostra esperienza nel Digital Manufacturing, forniamo soluzioni verticali e servizi di system integration in grado di supportarli nel raggiungimento dei loro obiettivi,



nel rispetto dei rigorosi requisiti normativi. Il nostro gruppo dedicato alla Digital Industry è coinvolto nella realizzazione di sottomarini, sistemi radar, veicoli terrestri, aerei e cantieri navali per il governo degli Stati Uniti. Guidiamo la Trasformazione Digitale del manufacturing, forniamo e integriamo sistemi IT per gestire dati e processi produttivi e offriamo soluzioni per ottimizzare la riparazione degli asset.

Alcuni esempi:

- **supporto alle attività di standardizzazione aziendale** per la Marina degli Stati Uniti, con servizi di assistenza per velivoli (ricerca, progettazione, sviluppo e ingegneria dei sistemi, acquisizione, test e valutazione, formazione, riparazione e supporto tecnico e logistico in servizio). È stata implementata una soluzione per gestire i dati di produzione in un repository centralizzato,

consentendone l'utilizzo nei processi downstream. Creando un'unica fonte dati, il Cliente è stato in grado di ridurre il time-to-market e migliorare l'efficienza dei processi di riparazione della flotta.

- **supporto nella trasformazione verso l'Industry 4.0** per un'azienda americana leader nel settore della Difesa e dell'Aerospazio, attiva in quattro ambiti: sistemi aerospaziali, sistemi di missione, servizi tecnologici e sistemi di innovazione. È stato creato un Solution Maturity Model per accompagnare la trasformazione del Cliente verso la sua vision di Industry 4.0, con l'obiettivo di migliorare il processo decisionale basato sui dati, aumentare il vantaggio competitivo e l'automazione (in più siti di produzione), supportandolo nel passaggio alla closed loop production.

- **supporto nelle fasi di progettazione** di uno dei principali produttori di sottomarini per la Marina degli Stati Uniti da oltre 100 anni, nonché vincitore nel 2017 di un importante contratto con il governo statunitense per produrre la prossima generazione di sottomarini. È stata implementato il Siemens Next Generation Planning (NGP) – primo caso in Nord America – consentendo al Cliente di trasformare i dati di progettazione, sfruttando il 4th Generation Design, in un piano di produzione dettagliato. L'obiettivo era massimizzare le prestazioni e la scalabilità, per supportare l'assemblaggio di strutture complesse.
- **supporto all'ottimizzazione dei processi** per un importante produttore di navi commerciali, che ha vinto un contratto per supportare la produzione di navi per il governo degli Stati Uniti. Tecniche di simulazione degli

impianti di produzione sono state implementate per aiutare il Cliente ad aumentare l'efficienza dei processi di assemblaggio e produzione navale.

- **supporto alla progettazione di un cantiere** per una base navale statunitense e il quartier generale della flotta del Pacifico degli Stati Uniti. È stato avviato un progetto in cui verrà costruito un modello di simulazione avanzato dell'attuale base navale, per analizzare il layout e i processi in un ambiente virtuale, facilitando così una completa riprogettazione e ristrutturazione della base. Seguendo questo modello, si deciderà dove costruire nuovi edifici e quali rimuovere, se è necessario acquistare nuove attrezzature e quali servizi di riparazione eseguire per evitare blocchi, creando così un piano per la progettazione del futuro cantiere.

# 06 Intelligence

Da anni siamo presenti nel settore dell'Intelligence. Ci occupiamo dell'integrazione di sistemi e sensori per la **Signals Intelligence** (SIGINT) e l'**Acoustic Intelligence** (ACINT) e di sicurezza e logica delle reti e degli ambienti dedicati allo scambio delle informazioni che contraddistinguono questa comunità operativa.

Le nostre soluzioni favoriscono la raccolta, la valorizzazione, l'elaborazione e la condivisione dei dati acquisiti da diverse tipologie di sensori.

In questo settore siamo partner tecnologico di riferimento per le Agenzie Nazionali e anche della NATO. Abbiamo realizzato e manteniamo la piattaforma di raccolta e analisi delle intercettazioni e della banca dati degli emettitori, attraverso la quale è possibile derivare i dettagli e le caratteristiche dei singoli sensori. Sul MPV (Multi Purpose Vessel) della Marina Militare Italiana ci siamo occupati dell'integrazione dei sensori di bordo e della realizzazione del sottosistema per la connessione terra-bordo-terra, con particolare riferimento all'invio di specifici task, alla raccolta delle informazioni e al loro inoltro verso

le installazioni terrestri. Attualmente stiamo realizzando la nuova Banca Dati Nazionale degli Emittitori.

Collaboriamo con la Marina Militare Italiana nella realizzazione di diverse soluzioni innovative. Ad esempio, abbiamo realizzato un **DSS (Decision Support System)** per la classificazione di elementi rilevati in mare aperto, attraverso l'analisi del relativo segnale acquisito con sensori SONAR. Fondamentale è stata la piattaforma per l'individuazione e il tracciamento di bersagli rilevati, con l'ausilio di sensori del tipo SONAR bi-statici, in configurazione non collaborativa. Questa tecnologia permette ai sommergibili di non essere individuati durante l'acquisizione delle informazioni relative all'ambiente circostante in modalità passiva, evitando l'emissione dei segnali dai SONAR di bordo.

Per la Componente Anfibia Nazionale stiamo realizzando degli **UAV (Underwater Automated Vehicles)** per la ricognizione delle acque prospicienti una spiaggia di sbarco, in grado di operare nelle shallow waters e nella surf zone (da 10 metri a 50 centimetri di profondità).





Per la messa in sicurezza di reti, ambienti e sistemi dedicati allo scambio di informazioni sensibili, ci siamo occupati del supporto all'omologazione di sicurezza (tutela del segreto di Stato), progettando e implementando le misure necessarie allo scopo: security risk assessment, vulnerability assesment, hardening dei sistemi, ecc.

Inoltre, abbiamo realizzato diodi software (Information Exchange Gateway) per l'interconnessione di reti e sistemi informatici di più Stati (Communication and Information System e/o Command Control and Information System). Utilizzati per molteplici scopi (operazioni congiunte, coalizioni, esercitazioni) e con diversi domini di sicurezza, hanno garantito la completa interoperabilità, il rispetto di specifici requisiti di sicurezza e il flusso dei dati senza soluzione di continuità.

Siamo uno dei partner tecnologici di riferimento nell'ambito dei progetti internazionali CAESAR e MAJIC per l'acquisizione, la memorizzazione, l'elaborazione e la condivisione di informazione ISR (Intelligence, Surveillance e Reconnaissance).





# 07 Maritime

Maritime

Come ENG abbiamo iniziato a occuparci di sorveglianza marittima circa 20 anni fa, gestendo le attività inerenti al sistema di supporto al comando della Marina Militare Italiana: Maritime Command Control and Information System – Italia. L'adozione delle Direttive Europee relative al monitoraggio del traffico marittimo mercantile da parte degli Stati Membri ha innescato un circolo virtuoso con progetti in ambito UE attraverso il riutilizzo delle esperienze maturate in ambito militare, come SafeSeaNet/STIRES per la European Maritime Safety Agency – EMSA, Consolidated European Reporting System/Single Vessel Database per la Maritime and Coastguard Agency UK – MCA.

In particolare, ci siamo occupati di sistemi per la sicurezza marittima attraverso il controllo del traffico marittimo mercantile, il supporto alle ispezioni volte alla verifica dei requisiti di sicurezza (safety) a bordo delle Unità Navali mercantili che arrivano presso un porto europeo o che appartengono a un determinato registro navale (Port State Control e Flag State Inspection).

Come ENG ci siamo inoltre occupati della realizzazione di sistemi di supporto alle attività portuali orientati all'implementazione della Direttiva Europea 2010/65/UE, che introduce il concetto di Interfaccia Unica.



Queste realizzazioni sono state fondamentali per progetti di ricerca europei (FP7 e H2020) sul tema della sorveglianza marittima e delle frontiere, come ad esempio PERSEUS, BlueMassMed, SAGRES, PROMERC, EUCISE-2020, ALFA, MARISA ed EFFECTOR.

- ALFA (Advanced Low Flying Aircrafts detection and tracking) analizza le problematiche, il modus operandi e i contesti operativi dei centri spagnoli di controllo SIVE (Sistema Integrado de Vigilancia Exterior spagnolo) e SIVICC (Sistema Integrado de Vigilância, Comando e Controllo), addetti anche al monitoraggio di attività illecite legate al traffico di droga che si sviluppa tra il Marocco e le coste dell'Europa Occidentale, principalmente Spagna e Portogallo. A partire dal contesto operativo, abbiamo sviluppato una serie di requisiti implementati in un'interfaccia unificata GIS, che rappresenta i velivoli leggeri coinvolti in traffici illeciti, identificati da sensori elettroottici, antenne a radio frequenza passive e radar, e classificati dal sistema ALFA come minacce da monitorare.
- MARISA (Maritime Integrated Surveillance Awareness) fornisce una gestione integrata delle informazioni provenienti dai diversi sistemi informatici dei Ministeri

della Difesa dei Paesi dell'UE coinvolti nell'iniziativa. La gestione di Big Data generati dalle marine militari che hanno aderito al progetto consente l'integrazione fra i diversi sistemi informatici e l'aggregazione in un solo punto centralizzato di tutte le informazioni derivanti dalle varie componenti sensoristiche (per esempio satelliti, radar, sistemi di previsioni meteorologiche). Integrare questi dati ai sistemi di rilevamento di imbarcazioni in mare consente, infine, di generare alert in maniera tempestiva e rilevare fenomeni criminali, quali il contrabbando di merci, il trasporto di migranti o la pesca illegale.

- [EFFECTOR](#) (An End to end Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical OpeRations) è un progetto di ricerca che punta a migliorare le capacità dei sistemi di sorveglianza marittima e di condivisione dei dati a livello tattico e strategico introducendo soluzioni applicate per una maggiore sicurezza delle frontiere. EFFECTOR implementa una piattaforma data lake multilivello per l'interoperabilità end-to-end, lo sfruttamento dei dati e per lo scambio di immagini di consapevolezza situazionale avanzata a diversi livelli con la rete CISE (Common Information Sharing

Environment) e EUROSUR (Sistema europeo di sorveglianza delle frontiere) gestito da FRONTEX. Nello specifico, uno degli obiettivi principali è diffondere le informazioni generate dai nodi CISE con il framework EUROSUR. Noi del Gruppo Engineering, con il supporto del consorzio EFFECTOR, abbiamo guidato lo sviluppo di un adattatore CISE per consentire a FRONTEX di scambiare informazioni con i nodi CISE durante le sperimentazioni del progetto EFFECTOR.

Le esperienze acquisite in ambito civile ci hanno permesso di espandere le funzioni dei sistemi militari, ad esempio, nella realizzazione del sistema di MSA (Maritime Situational Awareness) della Marina Militare Italiana SMART e dei sistemi interministeriali per il monitoraggio del dominio marittimo in Italia e all'estero (DIISM, MARS e NEREUS).

La nostra offerta Maritime comprende anche i sistemi per la gestione logistica integrata di un porto (Port Management System), con particolare riferimento alle attività di import, export e transhipment delle merci.

ENG rappresenta quindi un punto di riferimento europeo per l'implementazione di soluzioni inerenti la MDA (Maritime Domain Awareness).



# 08 Space

Space

Nel dominio Space le nostre soluzioni si concentrano sull'**Osservazione della Terra**. In questo ambito abbiamo sviluppato la piattaforma [SIMONA](#) (Satellite assets Integration for Maritime situatiON Awareness) per il controllo delle coste e la sicurezza della navigazione. Attraverso l'integrazione di diversi assetti satellitari, SIMONA implementa una serie di servizi in grado di potenziare la Guardia Costiera e la Marina Militare Italiana nelle attività di sorveglianza marittima e di supportare la Guardia Costiera nelle Operazioni SAR (Search and Rescue) di ricerca e salvataggio, grazie all'acquisizione di informazioni non fruibili con gli assetti tradizionali. I servizi implementati riguardano:

- **arricchimento dello scenario operativo** per superare i limiti di copertura degli attuali dispositivi (AIS, radar) attraverso l'utilizzo di due assetti satellitari, l'Osservazione della Terra e la comunicazione satellitare. L'Osservazione della Terra è stata sfruttata acquisendo immagini satellitari SAR sottoposte a un processo di analisi visuale (denominato ship detection), con il quale vengono identificate le imbarcazioni presenti nell'area. Oltre a identificare le navi, l'algoritmo implementato è in grado di calcolare la dimensione dell'imbarcazione

e, attraverso l'analisi della scia, di stimare la rotta e la velocità dell'imbarcazione. La seconda fonte di informazioni è costituita dai radar di bordo di unità navali cooperanti, veri e propri sensori remotizzati che concorrono alla situazione individuata con i dati provenienti dai sensori posti a terra.

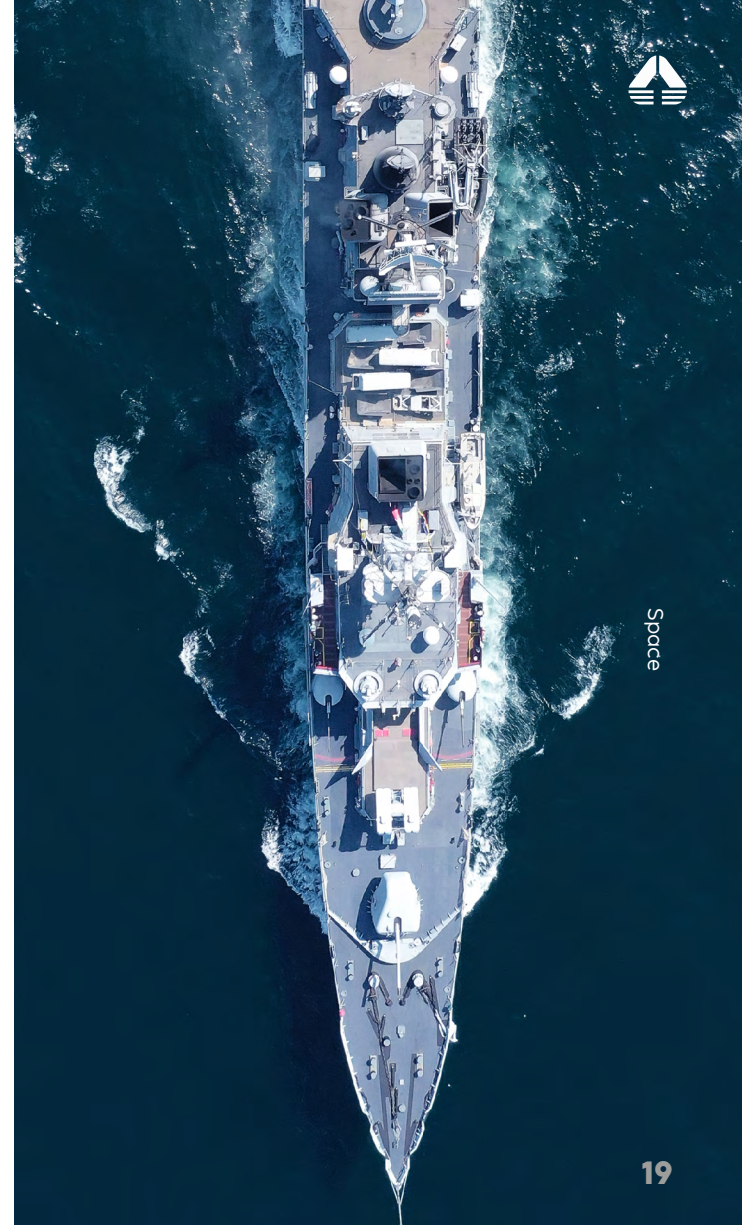
- **assistenza delle operazioni eseguite in mare** per una navigazione sicura. Il servizio è basato su due diversi componenti: un'app per smartphone (Android e IOS) con la quale richiamare i servizi SIMONA durante la navigazione, utilizzando la connettività telefonica 3G/4G e un dispositivo denominato SATCOMBOX per le comunicazioni satellitari attraverso la rete ORBCOMM. Analogamente alle scatole nere delle autovetture, questo dispositivo ha al suo interno altre due componenti molto importanti: un GPS per la geolocalizzazione e un Bluetooth, grazie al quale lo smartphone si connette all'apparato sfruttando la connessione satellitare per accedere ai servizi SIMONA, anche in assenza di copertura della rete telefonica, come può avvenire quando ci si allontana dalla costa.

Sempre nel settore Space abbiamo maturato un'importante esperienza nella gestione, conservazione ed elaborazione

di grosse moli di dati, prodotte dai sensori collocati su un gran numero di costellazioni satellitari e, per ASI (Agenzia Spaziale Italiana) come ENG ci siamo recentemente occupati di dimostrare la capacità del sistema GALILEO di soddisfare i requisiti indicati dalle normative IMO per l'introduzione del World Wide Radio Navigation System (WWRNS) nelle diverse operazioni portuali, attraverso lo studio e l'implementazione prototipale di un sistema centralizzato di allerta ed allarme. Nell'ambito di questo progetto, il segnale AIS è stato utilizzato per la trasmissione di informazioni complementari per l'ottimizzazione delle prestazioni e per migliorare gli aspetti decisionali aumentando la sicurezza della navigazione all'interno dei porti e nelle acque foranee.

Inoltre, per ESA (European Space Agency) ci stiamo occupando di garantire due importanti servizi, essenziali per il lavoro quotidiano dell'Agenzia: il Workplace Management e il Service Desk.

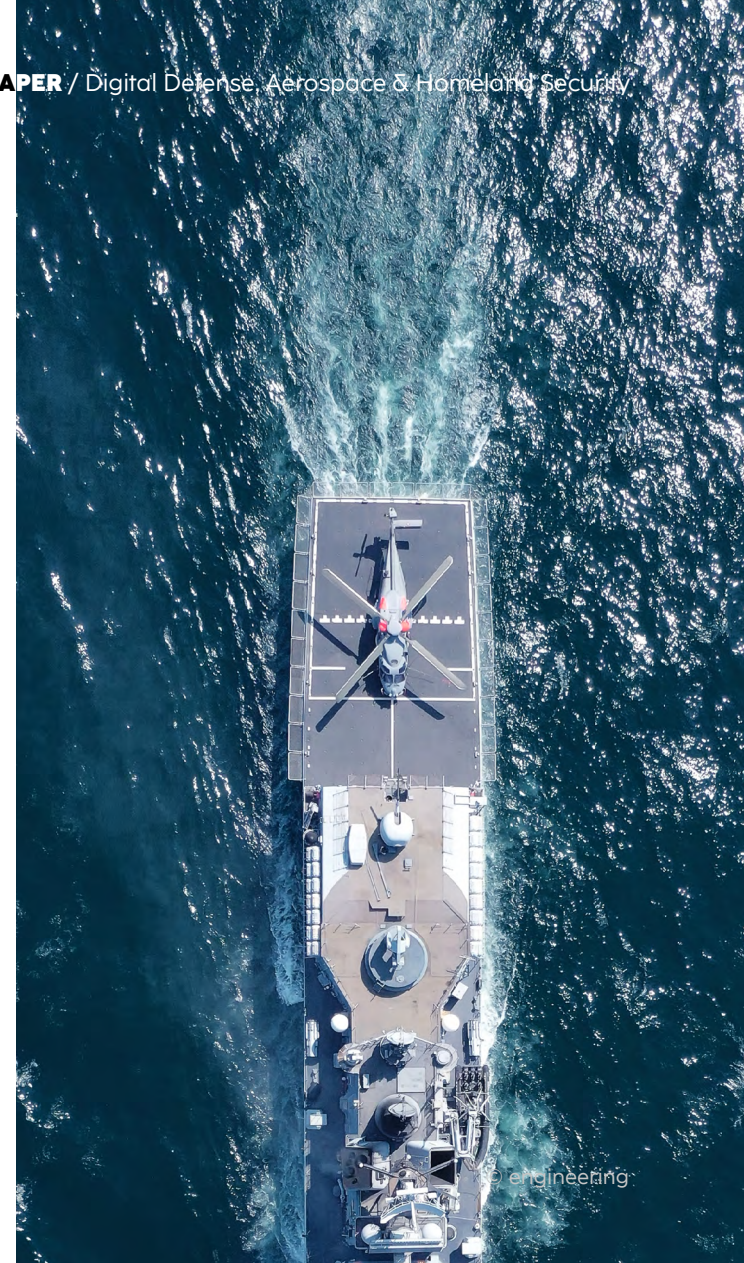
Infine, la nostra azienda è stata accreditata dalla Presidenza del Consiglio dei Ministri per la partecipazione alle gare bandite dalla European Global Navigation Satellite Systems Agency (GSA) inerenti al Galileo Public Regulated System (PRS).



# Homeland Security

Nell'area dell'Homeland Security collaboriamo con il Ministero dell'Interno italiano su due diversi temi: il primo riguarda la gestione e il rilascio dei visti, il secondo è relativo al controllo delle frontiere marittime. Nel corso del consiglio di Laeken alla fine del 2001, il Consiglio Europeo ha dato incarico alla Commissione di creare un sistema centralizzato per la gestione dei visti per favorire la cooperazione, la sicurezza e i controlli nell'area Schengen. Da questi presupposti è nato il progetto VIS (Visa Information System). Come ENG siamo stati coinvolti nel progetto fin dal suo inizio, sia dal Ministero degli Esteri che dal Ministero dell'Interno, per progettare e realizzare la componente italiana riguardante il rilascio dei visti e il loro controllo in frontiera e sul territorio, secondo quanto stabilito dal Regolamento (CE) n. 767/2008 del Parlamento e dal Consiglio Europeo e dal codice visti. In particolare, il Sistema Informativo I-VIS consente:

- controllo dei visti in frontiera tramite l'interrogazione del database centrale C-VIS, attraverso il raffronto biometrico;
- emissione di visti in frontiera, anche con l'acquisizione di dati biometrici e l'interrogazione dei database AFIS, SIS II, SDI, N-VIS e C-VIS;
- comunicazione elettronica, tramite portale delle agenzie marittime, dei dati dei marittimi richiedenti il visto.





I servizi del sistema I-VIS sono utilizzati anche dagli Uffici Immigrazione delle questure per l'attività di controllo dei visti sul territorio nazionale. Per il monitoraggio delle frontiere marittime, invece, abbiamo realizzato e manteniamo l'assetto nazionale deputato al controllo e alla gestione dell'immigrazione clandestina via mare, il National Coordination Center, Sistema integrato di TLC per l'attività di controllo dell'immigrazione clandestina SIA. Il SIA è stato realizzato per supportare gli organi preposti al monitoraggio del fenomeno immigrazione clandestina via mare, acquisendo attraverso interfacce con sistemi esterni i seguenti dati:

- messaggi della serie AIS (Automatic Identification System);
- messaggi VMS (Vessel Monitoring System);
- dati VTS (Vessel Traffic System);
- messaggi "contact" della serie OTH – Gold (Over The Horizon – Gold);
- messaggi relativi a "eventi di immigrazione clandestina" in formato XM;
- "eventi di immigrazione clandestina", "eventi SAR", inseriti attraverso l'interfaccia WEB del sistema SIA

- file di tipo multimediale.

I dati acquisiti vengono elaborati dal sistema attraverso i moduli CRM e BI per la generazione di report e statistiche. Il SIA, inoltre, permette la presentazione della situazione corrente (traffico marittimo, eventi di immigrazione clandestina, operazioni SAR, ecc.) su cartografia di riferimento (CM93/3).

Nel contesto della Homeland Security abbiamo maturato negli anni una vasta esperienza, partecipando e coordinando numerosi progetti nazionali ed europei, volti a esplorare, secondo un approccio multidisciplinare, il dominio della sicurezza pubblica. Il fine ultimo consiste nel supportare le forze dell'ordine ad adeguare le tecnologie impiegate in ambito investigativo e di intelligence alle sfide emergenti nel contrasto al crimine organizzato e al terrorismo.

Frutto di questa intensa attività di ricerca è [ATLANTIS](#) (AI-based platform for LAW enforcement intelligence and Investigation), piattaforma tecnologica dotata di servizi avanzati e basati su Intelligenza Artificiale, progettati per la ricerca, l'acquisizione e l'analisi di dati eterogenei provenienti da internet, inclusi il Deep Web e le Dark Net. La piattaforma permette l'estrapolazione aggregata di informazioni, consentendo il loro utilizzo per fini di intelligence o per la ricostruzione di eventi criminali, la formulazione di ipotesi investigative e la raccolta

di prove utilizzabili per fini giudiziari.

Le funzionalità della piattaforma si sono evolute e perfezionate nel tempo grazie alle esperienze maturate nei progetti di ricerca e al momento comprendono:

- **gestione collaborativa delle attività investigative:** facendo leva su tecnologie avanzate di Machine Learning e Intelligenza Artificiale, la piattaforma supporta le forze dell'ordine a combattere terrorismo e cybercrime (progetto [AIDA](#) - Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies). Un'interessante verticalizzazione sul dominio del traffico illegale di droghe e armi è stata affrontata in [ANITA](#) - Advanced tools for fighting online Illegal Trafficking. Partendo dall'esperienza di ANITA, il progetto [ARIEN](#) - Artificial Intelligence in fighting illicit drugs production and trafficking sta ulteriormente sviluppando la piattaforma per migliorare l'attività investigativa sul traffico internazionale di droghe e supportare l'analisi fenomenologica e la Drug Intelligence.
- **applicazione delle funzionalità alle investigazioni di Intelligence di tipo OSINT** (Open Source Intelligence), con particolare riguardo alle attività di contrasto della propaganda terroristica online, della radicalizzazione e del training delle cellule terroristiche jihadiste,



spesso veicolata da contenuti audio-video diffusi sia sul Surface Web che sul Deep Web (progetto DANTE – Detecting and ANalysing TERRORist-related online contents and financing activities).

- **gestione automatica di eventi di sicurezza estrapolati da archivi video** (progetto [SURVANT](#) – SURveillance Video Archives iNvestigation assisTant).
- applicazione delle funzionalità a casi d'uso e scenari operativi diversi con l'implementazione del concetto di **Community Policing** volto a promuovere e facilitare la collaborazione tra forze dell'ordine e cittadini, anche mediante tecniche di gaming (progetti TRILLION – TRusted, Cltizen-LEA colLaboratIon over sOcial Networks, SmarT SENSE – Strumenti e metodologie per Smart sECure urbaN SystEm ed APPRAISE – fAcilitating Public & Private secuRity operAtors to mitigate terrorism Scenarios against soft targEts ).
- evoluzione dei tool a supporto delle investigazioni di digital forensic e intelligence ([STARLIGHT](#) – Sustainable Autonomy and Resilience for LEAs using AI against High Priority Threats).

Grazie alla piattaforma ad ATLANTIS, le forze dell'ordine possono ottenere:

- riduzione significativa dei tempi di indagine tramite l'integrazione delle fasi di investigazione (acquisizione risorse, indizi e prove, esportazione delle ipotesi investigative secondo formati standard per la fase di prosecution)
- riduzione del tempo dedicato alle ricerche manuali su internet
- supporto per l'analisi automatica di contenuti testuali
- suggerimento automatico di indizi, prove e risorse utili alle indagini
- ampliamento degli strumenti investigativi grazie alla semplicità d'integrazione di nuovi servizi o di servizi già in uso presso le forze dell'ordine.

L'attività di ricerca sulla Homeland Security sta anche contribuendo a risolvere l'annoso problema della carenza di dataset utili ad addestrare gli algoritmi di Machine Learning e Artificial Intelligence nell'ambito della sicurezza dei cittadini.

Su questa tematica, il progetto [LAGO](#) (Lessen Data Access and Governance Obstacles) si sta occupando di definire l'architettura di riferimento per la realizzazione di un affidabile **EU Research Data Ecosystem**.





# 10 Qual è il futuro della Digital Defense?

Qual è il futuro della Digital Defense?

**La Digital Transformation sta creando numerose opportunità per il settore, aprendo nuovi fronti digitali che si intersecheranno con le sfide sul campo – terra, aria e mare – dove il tema centrale riguarderà la protezione e la gestione del dato, attraverso tecnologie come IoT, AI e Cybersecurity.**

Un'informazione completa, precisa e in tempo reale si traduce in superiorità strategica, logistica, tattica e di intelligence perché consente di prendere decisioni e adottare strategie più efficaci. La Cybersecurity quindi sarà sempre più centrale per la strategia di Difesa di ogni nazione, volta a garantire la massima protezione dei cittadini, passando da un assetto reattivo ad uno più proattivo, diventando sempre più autonoma e self-evolving, identificando vulnerabilità nascoste e bloccando attacchi in maniera preventiva.

In questo scenario, la ricerca e l'innovazione tecnologica, supportate da idonee politiche d'investimento e da una governance efficace, saranno fondamentali per affrontare le sfide degli operatori del settore. Il successo di queste attività, però, non può prescindere dalla collaborazione tra Istituzioni e partner tecnologici innovativi, affidabili e competenti, in grado di accelerare il processo di evoluzione delle organizzazioni della Difesa, consentendole di stare al passo con i continui mutamenti tecnologici.

Noi di ENG ci poniamo come partner strategico per

accompagnare governi, istituzioni e rispettivi fornitori in questo percorso evolutivo e per accelerare lo sviluppo di nuove soluzioni e tecnologie.

Crediamo nella necessità di partnership con aziende che siano basate sulla fiducia e sulle competenze tecniche, ma anche e soprattutto di processo. Portiamo avanti questo percorso secondo l'approccio del Dual Use militare/civile, che sarà sempre più centrale per il settore.

Nel contesto storico in cui viviamo e per i prossimi anni il riutilizzo e la condivisione delle competenze acquisite e delle soluzioni realizzate in entrambi i settori saranno essenziali. Dal punto di vista strategico, lo strumento militare agirà sempre più spesso in concorso con le autorità civili per il presidio del territorio, supportandole durante il verificarsi di disastri naturali.

Inoltre, dal punto di vista dell'operatività e della salvaguardia degli investimenti, poter contare su sistemi che sono "multi-purpose by design" significherà, di fatto, aumentare la resilienza di un intero sistema Paese, ottimizzando al tempo stesso le risorse impiegate.



Qual è il futuro della Digital Defense?



@ [www.eng.it](http://www.eng.it)

**in** Engineering Group

**@** @LifeAtEngineering

**X** @EngineeringSpa