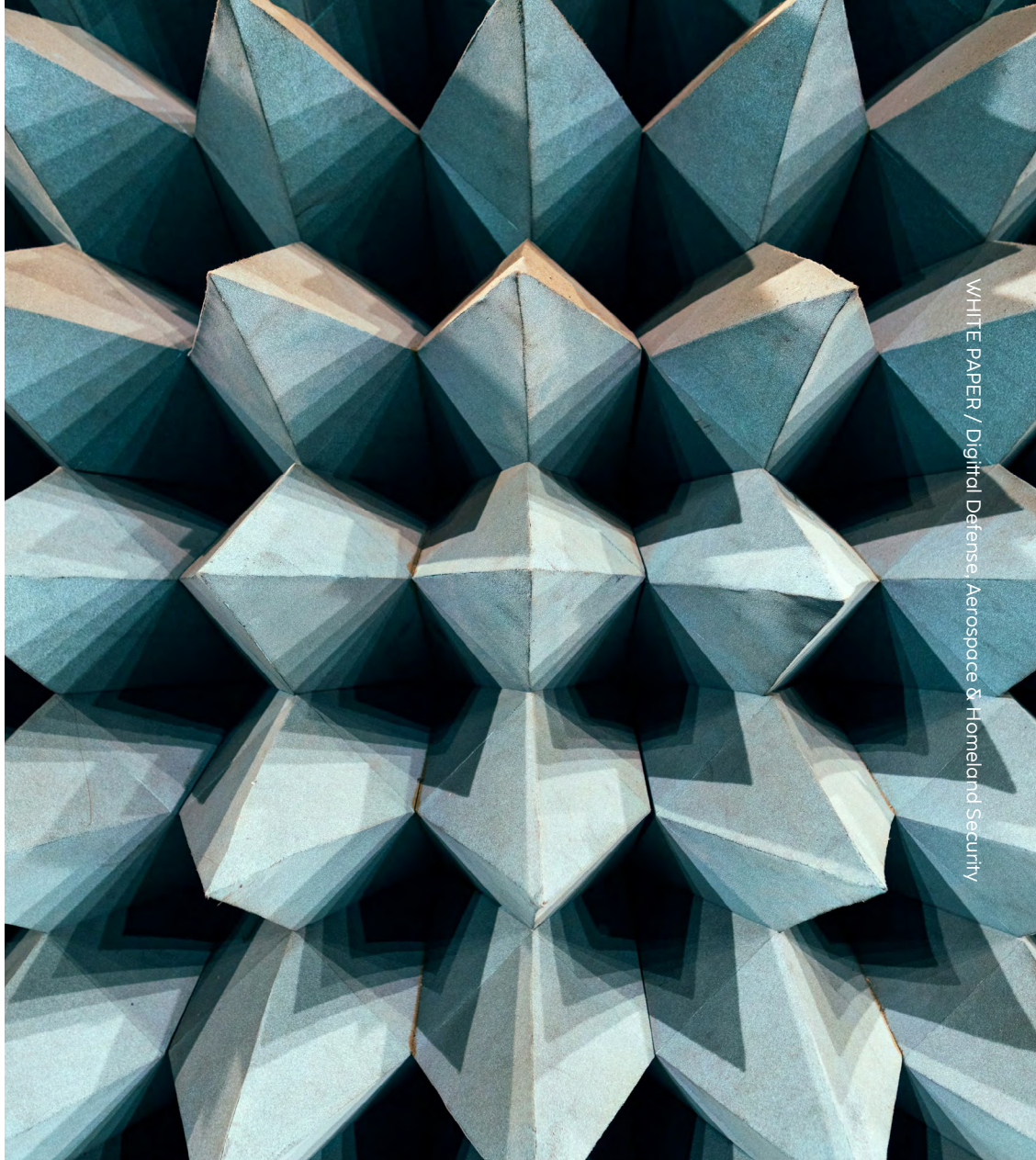
WHITE PAPER

Digital Defense, Aerospace & Homeland Security



Authors

Massimiliano Camilli
Technical Manager Defense, Space & Homeland Security
ENGINEERING
massimiliano.camilli@eng.it
in Massimiliano Camilli

Chris Draska
VP of Sales for North America - Industries eXcellence
ENGINEERING
chris.draska@eng.it
in Chris Draska

Ernesto La Mattina
Head of AI & Advanced Analytics Research Unit
ENGINEERING
ernesto.lamattina@eng.it
in Ernesto La Mattina

Fabio Sala
VP of Industries eXcellence - USA
ENGINEERING
fabio.sala@eng.it
in Fabio Sala

Giuseppe Vella
Head of Border and External Security Research Unit
ENGINEERING
giuseppe.vella@eng.it
in Giuseppe Vella

Summary

01 Trends, challenges and opportunities

In recent years, we have witnessed different types of global threats and phenomena that require significant interventions in defense by governments.

In addition to the territorial level, Defense's field of action has expanded to other areas of society, including the economic/financial field and, above all, the cyber field. The chessboard of defensive actions has changed, becoming more widespread and multidimensional.

To cope with evolving conflicts and technologies, defense departments work closely with the private sector, ensuring the use of state-of-the-art technologies to mitigate the risk of obsolescence. These departments must therefore enter into alliances with technology partners that can provide expertise and knowledge complementary to their own. In doing so, governments can no longer rely only on their traditional suppliers, the Defense companies, but must also rely on high-tech companies that boast much greater investment in research.

Co-operation between these worlds is not only desirable but necessary, in order to pool the expertise of each and govern the Digital Transformation in a critical sector for nations and citizens.

It is precisely on the issue of cooperation that a second challenge emerges: collaboration between Defense departments. The various branches fail to exchange the data and information necessary for the Digital Transformation of Entities. In addition, the use of digital platforms arouses strong resistance within departments for several reasons: firstly, because of the investment in terms of money and time required (consider training, for example) and secondly, because, with the increasing reliance on technology, all military equipment will become increasingly interconnected, increasing exposure to cyber risks. The challenges are therefore manifold and we at ENG, with our extensive experience in supporting governments, are ready to tackle them with strategically important projects.

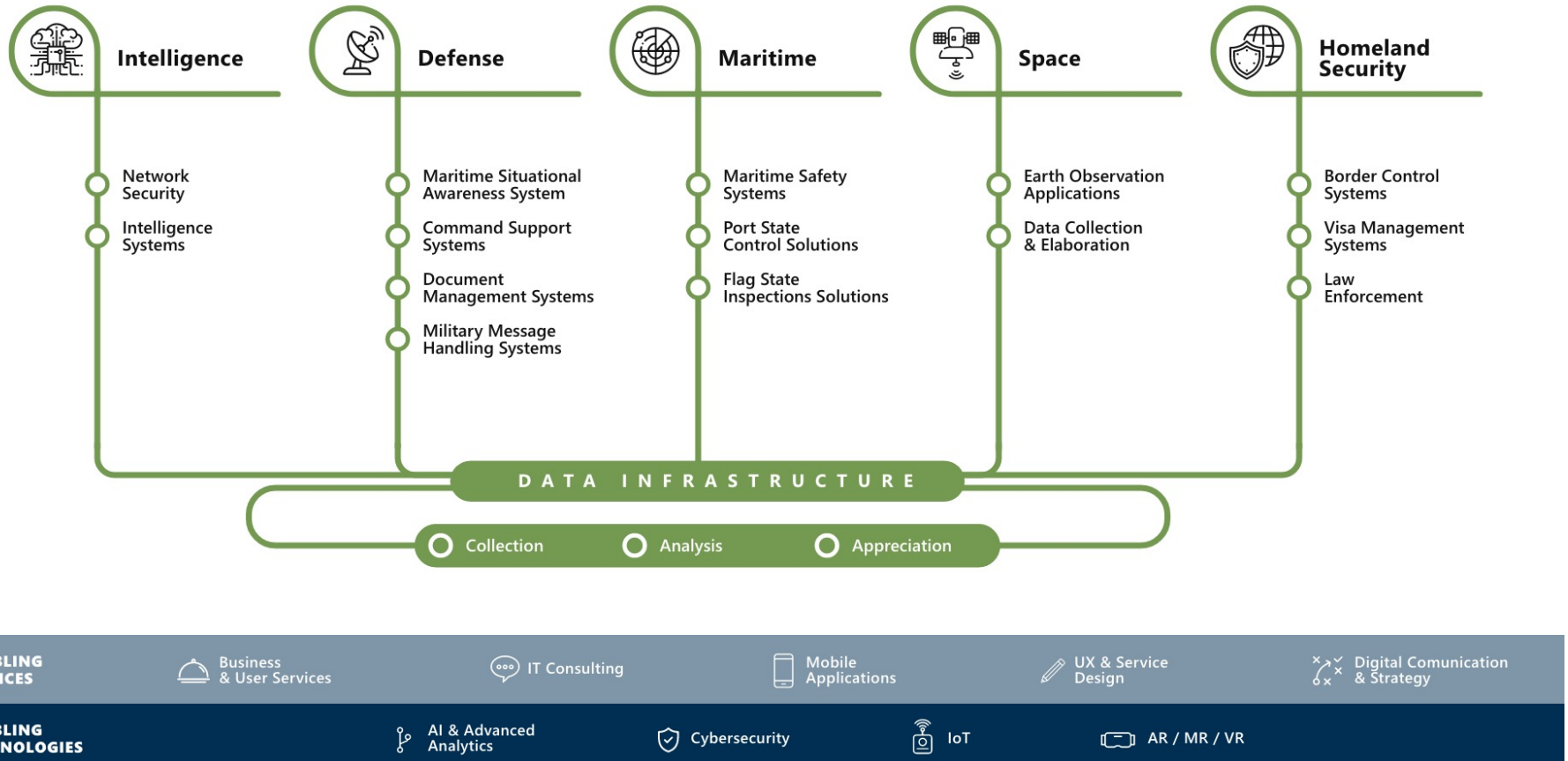
02 ENG for Digital Defense

We work in Digital Defense, Aerospace & Homeland Security to **facilitate the secure acquisition, management and distribution of data related to military and national security operations**.

We also provide logistical support, related to the land, sea, air, space and cyber domains. We proactively support and accompany companies, positioning ourselves as a credible and reliable technology partner for national and international defense and security institutions.

Our targets in Digital Defense, Aerospace and Homeland Security are:

- **promoting** the military/civilian dual-use paradigm, encouraging the re-use of skills acquired and solutions implemented in both sectors;
- proactively **contributing** to technical, technological and process innovation in highly specialised niche domains;.
- **supporting** users in their Digital Transformation journey..



Digital Defense, Aerospace & Homeland Security

We enable the secure acquisition, management and distribution of data concerning military and homeland security operations, as well as logistic support for maritime, land, air, space and cybernetic domains.

25+
YEARS OF EXPERIENCE

15+
CLIENTS

50+
BUSINESS SPECIALISTS

20+
ONGOING PROJECTS

5+
RESEARCH PROJECTS LIVE

ADVISORY

MANAGED SERVICES

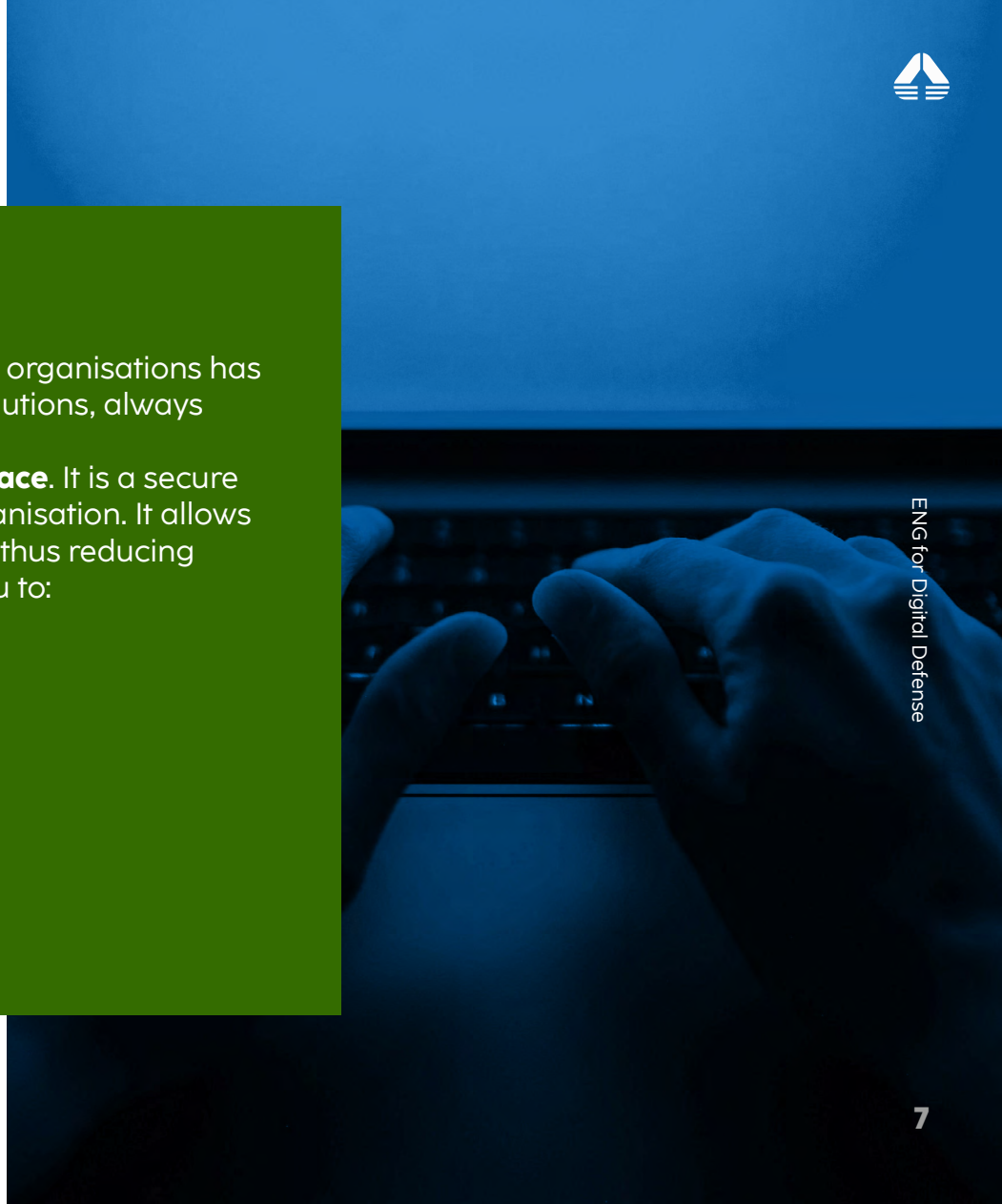
TECHNOLOGY & IMPLEMENTATION

Remote Sensing
AI
Combat Systems
Command Support Systems
Document Management Systems
Decision Support System
Underwater Systems
Predictive Analysis
Real Time
Military Healthcare Systems
Logistic Support Systems
GIS
Data Satellite Processing Systems
SIGINT Systems
BIG DATA
Earth Observation Data

vDESK: a high level of security and flexibility

With Digital Transformation, the sense of vulnerability on the part of organisations has also grown. To meet their security needs, we have innovated our solutions, always aiming for maximum data protection.
vDESK transforms the traditional workstation into a **Digital Workplace**. It is a secure and encrypted platform, integrated with other IT systems in the organisation. It allows work activities to be digitised, increasing flexibility and productivity, thus reducing costs and downtime. Through a single dashboard vDESK allows you to:

- profile users in a simple and intuitive way;
- use a range of integrated applications;
- get support from a virtual assistant;
- set up clearly visible alerts and notifications;
- receive constantly updated information.



03 Defense

We implement and maintain a wide range of systems, which support users in operational and logistical activities:

- Command Support Systems
- Maritime Situational Awareness and Intelligence Systems
- Military Messaging Systems
- Document Management Systems
- Military Health Support Systems and Information/ Cybersecurity Solutions

The collaboration between our team of experts and the Engineering ECM (Enterprise Content Management) Competence Centre also gave impetus to the implementation of systems dedicated to information processing and in particular to **document management** and **military messaging** (STANAG 4406).

Concerning the former, as ENG we developed and maintain the Document Management and Computer Protocol System that manages over 4 million documents and more than 17,000 users each year for the Defense General Staff, Segredifesa and the Italian Army.

As far as systems supporting **Military Health** are concerned, we are involved in the re-engineering and functional expansion of the Defense Administration Health Information System (SISAD).

In addition, we are working on the implementation of the Hospital Information System (SIO) that will be adopted by the Celio Military Hospital.

Finally, within the Defense sector, limited to the world of **classified** information, we deal with Information/ Cybersecurity with regard to the following aspects:

- Application Security
- Perimeter security of IT infrastructures (Network Security Architecture, Vulnerability Assessment, Event and Log Management, End Point and Mobile Security, Data Loss Prevention, Advanced Persistent Threat)
- Cyber Threat Intelligence and security in the exchange of information between networks at different classification levels, security of critical infrastructures (development of decision support systems and prevention and/or intervention policies following the assessment, through modelling and dynamic simulation, of impacts due to incidents and/or threats on interconnected critical infrastructures).

In addition, we also worked directly with the European Defense Agency on two particular topics: Strategic Technology Foresight and the procurement of materials and components for European defense industries.

As part of our Research & Innovation activities, we coordinate two complementary European projects:

- **PYTHIA** (Predictive methodologY for TecHnology Intelligence Analysis), funded in the context of the Preparatory Action on Defense Research programme, with the aim of developing an innovative methodology to make strategic technology forecasts in the Defense context, through Big Data Analytics tools and predictive models. The consortium is characterised by a wide geographical coverage, with partners from 6

different European countries whose organisations are Ministries of Defense, think tanks specialised in strategy and defense, technology providers and integrators.

- **SOLOMON** (Strategy-Oriented anaLysis Of the Market fOrces in EU defeNce) which provides the European Union with methodologies and tools to ensure a reliable production chain for European arms industries. The objective is to minimise the technological dependence on non-European countries, linked to ITAR and EAR restriction regulations, to define possible roadmaps to address these risks.

Another project funded by DG_DEFIS Unit A3 is **SEANICE** (Antisubmarine Warfare European Autonomous Networked Innovative And Collaborative Environment), which aims to study, develop and set the basis for the provision of an advanced anti-submarine defense system.

This project, based on an operational scenario, exploits new cutting-edge technologies such as data management, communication technologies, Artificial Intelligence and a blend of assets, both manned and unmanned, to best perform an ASW (Anti-Submarine Warfare) mission.

© engineering

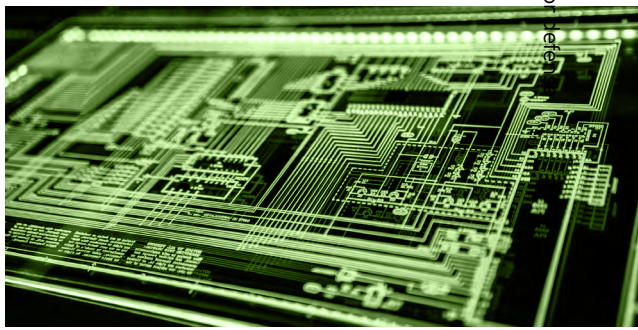
04 Cybertech: digital security for defense

Cybertech, the Engineering Group's company specialized in solutions and services for cybersecurity, has strengthened its presence in the Defense, Space, and National Security sectors in recent years, offering innovations to the major Italian institutions in the field.

Our clients continue to entrust our experts with a wide range of services that combine proven professional experience, in-depth industry knowledge, and cutting-edge technologies, such as:

- forensic analysis services, to extend and substantiate investigative capabilities in response to cybersecurity incidents, investigating activities on various types of devices (end-user devices, mobile devices, network machinery, or the web);
- design and delivery of digital identity protection services, access management, and control, to ensure correct usage by authorized personnel and prevent potential intrusions;
- continuous monitoring services for activities on networks and devices to ensure effective and reliable protection of all corporate assets.

With innovative technologies and advanced practices, our team continues to offer customized security solutions to meet the evolving needs of our clients, ensuring resilience and readiness in today's threat landscape.



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

Our global **Industries eXcellence** division is also involved in Digital Defense, Aerospace & Homeland Security projects.

In this market segment, production is aimed directly at government agencies and has to comply with strict standards and regulations, especially in the United States, one of the world's largest military, naval and aviation powers. Our US team has been working in this field for years to provide consultancy, technology solutions and services dedicated to Industry 4.0 for the US Department of Defense.

On the technology side, defense contractors who produce aircraft and ships for the US need to speed up design and production times. Thanks to our expertise in Digital Manufacturing, we provide vertical solutions and system integration services that support them in achieving their goals, while meeting

stringent regulatory requirements.

Our Digital Industry group is involved in building submarines, radar systems, land vehicles, aircraft and shipyards for the US government. We drive the Digital Transformation of manufacturing, provide and integrate IT systems to manage data and production processes, and offer solutions to optimise asset repair.

Some examples:

- **supporting corporate standardisation activities** for the US Navy, with aircraft support services (research, design, systems development and engineering, acquisition, test and evaluation, training, repair and in-service technical and logistical support). A solution has been implemented to manage production data in a centralised repository, enabling its use in downstream processes.
By creating a single data source, the customer was able to reduce time-to-market and improve the efficiency of fleet repair processes.

- **supporting the transformation to Industry 4.0** for a leading US defense and aerospace company, active in four areas: aerospace systems, mission systems, technology services and innovation systems. A Solution Maturity Model was created to accompany the customer's transformation towards its Industry 4.0 vision, with the aim of improving data-driven decision-making, increasing competitive advantages and automation (across multiple production sites), and supporting it in the transition to closed loop production.

- **supporting the design phases** of one of the leading manufacturers of submarines for the US Navy for over 100 years, and winner in 2017 of a major contract with the US government to produce the next generation of submarines. Siemens Next Generation Planning (NGP) was implemented - a first in North America - allowing the customer to transform design data, using 4th Generation Design, into a detailed production plan. The aim was to maximise performance and scalability, to support the assembly of complex structures.

- **process optimisation support** for a major commercial ship manufacturer, which won a contract to support the production of ships for the US government. Simulation techniques of production facilities were implemented to help the customer increase the efficiency of ship assembly and production processes.

- **supporting the design of a shipyard** for a US naval base and the headquarters of the US Pacific Fleet. A project was initiated to construct an advanced simulation model of the current naval base to analyse the layout and processes in a virtual environment, thus facilitating a complete redesign and restructuring of the base. Following this model, decisions will be made on where to construct new buildings and which ones to remove, whether new equipment needs to be purchased, and which repair services need to be carried out to avoid blockages, thus creating a plan for the design of the future construction site.

06 Intelligence

We have been in the intelligence business for years. We deal with the integration of systems and sensors for **Signals Intelligence** (SIGINT) and **Acoustic Intelligence** (ACINT) and the security and logic of the networks and environments dedicated to the exchange of information that characterise this operational community.

Our solutions facilitate the collection, exploitation, processing and sharing of data acquired from different types of sensors.

In this sector, we are the technology partner of choice for National Agencies and also NATO. We created and maintain the platform for the collection and analysis of intercepts and the emitter database, through which the details and characteristics of individual sensors can be derived. On the Italian Navy's MPV (Multi Purpose Vessel), we dealt with the integration of on-board sensors and the implementation of the sub-system for the land-board-land connection, with particular reference to sending specific tasks, collecting information and forwarding it to land installations. We are currently setting up the new National Database of Issuers.

We collaborate with the Italian Navy in the realisation of several innovative solutions. For example, we created a **DSS (Decision Support System)** for the classification of features detected in the open sea by analysing the relevant signal acquired with SONAR sensors.
A fundamental aspect was the platform for the detection and tracking of identified targets, using bi-static SONAR-type sensors, in a non-cooperative configuration.
This technology allows submarines to remain undetected while acquiring information about their surroundings in passive mode, avoiding the emission of signals from on-board SONARs.

For the National Amphibious Component, we are constructing **UAVs (Underwater Automated Vehicles)** for reconnaissance of landing beach waters, capable of operating in shallow waters and in the surf zone (from 10 metres to 50 centimetres depth).

For the securing of networks, environments and systems dedicated to the exchange of sensitive information, we dealt with security approval support (protection of state secrets), designing and implementing the necessary measures for this purpose: security risk assessment, vulnerability assessment, systems hardening, etc.

In addition, we developed software diodes (Information Exchange Gateway) for the interconnection of networks and information systems of several states (Communication and Information System and/or Command Control and Information System). Used for multiple purposes (joint operations, coalitions, exercises) and with different security domains, they ensured complete interoperability, compliance with specific security requirements and seamless data flow.

We are one of the leading technology partners in the international CAESAR and MAJIIC projects for the acquisition, storage, processing and sharing of ISR (Intelligence, Surveillance and Reconnaissance) information.

07 Maritime

We started engaging with maritime surveillance about 20 years ago, managing activities related to the Italian Navy's command support system: Maritime Command Control and Information System - Italy. The adoption of the European Directives on the monitoring of merchant maritime traffic by Member States triggered a virtuous circle with projects in the EU through the re-use of experience gained in the military sphere, such as SafeSeaNet/STIRES for the European Maritime Safety Agency - EMSA, Consolidated European Reporting System/Single Vessel Database for the UK Maritime and Coastguard Agency - MCA.

In particular, we dealt with maritime safety systems through the control of merchant maritime traffic, the support of inspections aimed at verifying safety requirements on board merchant vessels arriving at a European port or belonging to a specific ship register (Port State Control and Flag State Inspection).

We were also involved in the realisation of support systems for port activities oriented towards the implementation of the European Directive 2010/65/EU, which introduces the concept of Single Interface.

These achievements have been central to European research projects (FP7 and H2020) on maritime and border surveillance, such as PERSEUS, BlueMassMed, SAGRES, PROMERC, EUCISE-2020, ALFA, MARISA and EFFECTOR

- ALFA (Advanced Low Flying Aircrafts detection and tracking) analyses the problems, modus operandi and operational contexts of the Spanish SIVE (Spanish Sistema Integrado de Vigilancia Exterior) and SIVICC (Sistema Integrado de Vigilância, Comando e Controlo) control centres, which are also in charge of monitoring illicit activities related to drug trafficking between Morocco and the coasts of Western Europe, mainly Spain and Portugal. From the operational context, we developed a set of requirements implemented in a unified GIS interface, representing light aircraft involved in illicit trafficking, identified by electro-optical sensors, passive radio frequency antennas and radar, and classified by the ALFA system as threats to be monitored.

- MARISA (Maritime Integrated Surveillance Awareness) provides integrated management of information from the different information systems of the Ministries of Defense of the EU countries involved in the initiative. The management of Big Data generated by the navies participating in the project enables the integration of different information systems and the aggregation of all the information from the various sensor components (e.g. satellites, radar, weather forecast systems) into one centralised point. Integrating this data with vessel detection systems at sea also makes it possible to generate alerts in a timely manner and detect criminal phenomena such as smuggling of goods, transport of migrants or illegal fishing.

- EFFECTOR (An End to End Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical OpeRations) is a research project that aims to improve the capabilities of maritime surveillance and data sharing systems at tactical and strategic levels by introducing applied solutions for enhanced border security. EFFECTOR implements a multi-level data lake platform for end-to-end interoperability, data exploitation and advanced situational awareness image exchange with the CISE (Common Information Sharing Environment) network and EUROSUR (European Border Surveillance System) operated by FRONTEX. Specifically, one of the main objectives is to disseminate the information generated by the CISE nodes with the EUROSUR framework. With the support of the EFFECTOR consortium, we spearheaded the development of a CISE adapter to enable FRONTEX to exchange information with CISE nodes during EFFECTOR project trials.

The experience gained in the civil sector has enabled us to expand the functions of military systems, for example, in the implementation of the Italian Navy's MSA (Maritime Situational Awareness) system SMART and the inter-ministerial systems for monitoring the maritime domain in Italy and abroad (DIISM, MARS and NEREUS).

Our Maritime offering also includes systems for the integrated logistics management of a port (Port Management System), with particular reference to the import, export and transshipment of goods. ENG therefore represents a European benchmark for the implementation of MDA (Maritime Domain Awareness) solutions.

08 Space

In the Space domain, our solutions focus on **Earth Observation**. In this area, we developed the SIMONA (Satellite assets Integration for Maritime situatiON Awareness) platform for coastal control and navigation safety. Through the integration of different satellite assets, SIMONA implements a series of services that can assist the Italian Coast Guard and Navy in maritime surveillance activities and support the Coast Guard in Search and Rescue (SAR) operations, thanks to the acquisition of information that cannot be used with traditional assets.

The services implemented concern:

- **enrichment of the operational scenario** to overcome the coverage limitations of current devices (AIS, radar) through the use of two satellite assets, Earth Observation and satellite communication. Earth Observation was exploited by acquiring SAR satellite images subjected to a visual analysis process (called ship detection), whereby vessels present in the area are identified. In addition to identifying ships, the implemented algorithm is able to calculate the size of the vessel

and, through wake analysis, estimate the vessel's course and speed. The second source of information is the on-board radars of cooperating naval units, real remote sensors that contribute data from shore-based sensors to the identified situation.

- **supporting operations at sea for safe navigation**. The service is based on two different components: an app for smartphones (Android and IOS), which can be used to call up SIMONA services while browsing using 3G/4G telephone connectivity, and a device called SATCOMBOX for satellite communications via the ORBCOMM network. Like car black boxes, this device has two other very important components inside: a GPS for geolocalisation, and Bluetooth, which the smartphone uses to connect to the device using the satellite connection to access SIMONA services - even in the absence of telephone network coverage, which can be a factor when moving away from the coast.

Also in the Space sector, we have gained important experience in the management, storage and processing of large volumes of data produced by sensors positioned across a large number of satellite constellations. For ASI (Italian Space Agency), we have recently been involved in demonstrating the GALILEO system's ability to meet the requirements indicated by IMO regulations for the introduction of the World Wide Radio Navigation System (WWRNS) in the various port operations, through the study and prototype implementation of a centralised alert and warning system. In the context of this project, the AIS signal was used to transmit complementary information for performance optimisation and to improve decision-making aspects by increasing the safety of navigation within ports and in offshore waters.

In addition, for ESA (European Space Agency) we are ensuring two important services that are essential for the day-to-day work of the Agency: Workplace Management and the Service Desk.

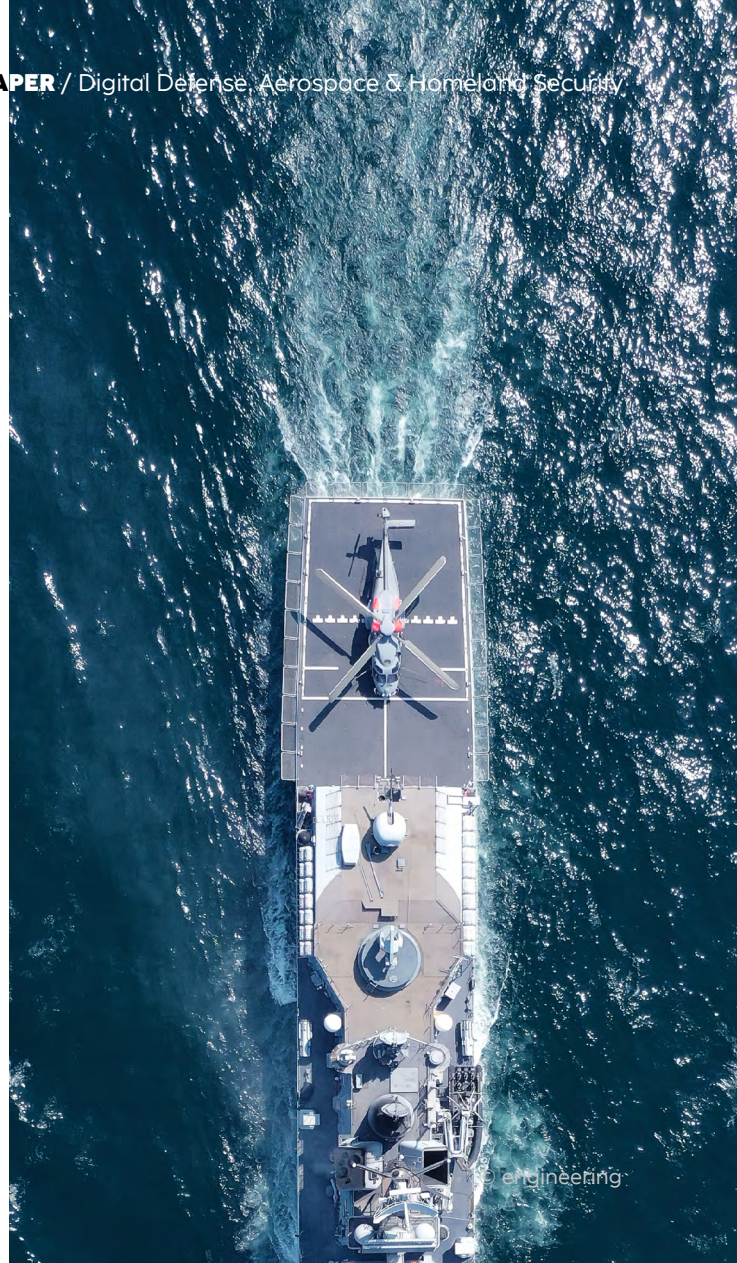
Finally, our company has been accredited by the Presidency of the Council of Ministers to participate in the tenders launched by the European Global Navigation Satellite Systems Agency (GSA) concerning the Galileo Public Regulated System (PRS).

09 Homeland Security

In the area of Homeland Security we cooperate with the Italian Ministry of the Interior on two different issues: the first concerns the management and issuing of visas, the second is related to maritime border control. At the Laeken Council at the end of 2001, the European Council instructed the Commission to set up a centralised visa management system to facilitate cooperation, security and controls in the Schengen area. The VIS (Visa Information System) project was born from these assumptions.

We have been involved in the project since its inception, both by the Ministry of Foreign Affairs and the Ministry of the Interior, to design and implement the Italian component concerning the issue of visas and their control at the border and in the territory - in accordance with Regulation (EC) No. 767/2008 of the European Parliament and the European Council and the Visa Code. In particular, the I-VIS Information System allows:

- the checking of visas at the border by querying the central C-VIS database through biometric comparison
- the issue of visas at the border, including by capturing biometric data and querying AFIS, SIS II, SDI, N-VIS and C-VIS databases
- electronic communication, via the Maritime Agencies Portal, of the data of seafarers applying for visas.



The services of the I-VIS system are also used by the Immigration Offices of the police headquarters for visa control activities concerning the national territory.

For the monitoring of maritime borders, on the other hand, we initiated and maintain the National Coordination Centre, an Integrated TLC System for the control and management of illegal immigration by sea, SIA. The SIA was developed to support the bodies in charge of monitoring the phenomenon of illegal immigration by sea by acquiring the following data through interfaces with external systems:

- AIS (Automatic Identification System) Series Messages
- VMS (Vessel Monitoring System) messages
- VTS (Vessel Traffic System) data
- "Contact" messages from the OTH - Gold series (Over The Horizon - Gold)
- messages on "illegal immigration events" in XML format
- "illegal immigration events", "SAR events", entered through the SIA system's WEB interface
- multimedia files

The acquired data is processed by the system through the CRM and BI modules for the generation of reports and statistics. The SIA also allows the presentation of the current situation (maritime traffic, illegal immigration events, SAR operations, etc.) on reference cartography (CM93/3).

In the context of Homeland Security, we have gained extensive experience over the years, participating in and coordinating numerous national and European projects, aimed at exploring the domain of public security through a multidisciplinary approach.
The ultimate aim is to support law enforcement agencies in adapting their investigative and intelligence technologies to the emerging challenges in the fight against organised crime and terrorism.

The result of this intense research activity is ATLANTIS (AI-based plaTform for LAw eNforcement inTelligence and InveStigation), a technology platform with advanced Artificial Intelligence-based services designed to search, acquire and analyse heterogeneous data from the internet, including the deep web and dark net.

The platform allows the aggregated extraction of information, enabling its use for intelligence purposes or for the reconstruction of criminal events, the formulation of investigative hypotheses and the collection of evidence that can be used for judicial purposes.

The platform's functionalities have evolved and refined over time thanks to the experiences gained in research projects and currently include:

- **collaborative Management of Investigative Activities**: by leveraging advanced Machine Learning and Artificial Intelligence technologies, the platform supports law enforcement agencies in combating terrorism and cybercrime (project AIDA - Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies).
  An interesting verticalisation on the domain of illegal drug and arms trafficking was addressed in ANITA - Advanced tools for fighting oNline Illegal TrAfficking. Building on ANITA's experience, the ARIEN project (ARtificial IntelligencE in fighting illicit drugs production and traffickiNg) is further developing the platform to improve the investigation of international drug trafficking and support phenomenological analysis and drug intelligence.
- **application of functionalities to OSINT-type intelligence investigations** (Open Source INTelligence), with a particular focus on countering online terrorist propaganda, radicalisation and training of jihadist terrorist cells, often conveyed by audio-video content disseminated both on the surface web and the deep web (DANTE project - Detecting

and ANalysing TErrorist-related online contents and financing activities).

- **automatic management of security events extrapolated from video archives** (SURVANT project - SURveillance Video Archives iNvestigation assisTant).

- application of functionalities to different use cases and operational scenarios with the implementation of the concept of **Community Policing**, aimed at promoting and facilitating cooperation between law enforcement agencies and citizens, also by means of gaming techniques (projects TRILLION - TRusted, CItizen-LEA coILaboratIon over sOcial Networks, SmarT SENSE - Tools and methodologies for Smart sEcure urbaN SystEm and APPRAISE - fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts).

- evolution of tools to support digital forensic and intelligence investigations (STARLIGHT - Sustainable Autonomy and Resilience for LEAs using AI against high priority threats).

Thanks to the ATLANTIS platform, law enforcement agencies can obtain:

- a significant reduction of investigation time through integration of the investigation phases (acquisition of resources, clues and evidence, export of investigative hypotheses according to standard formats for the prosecution phase)

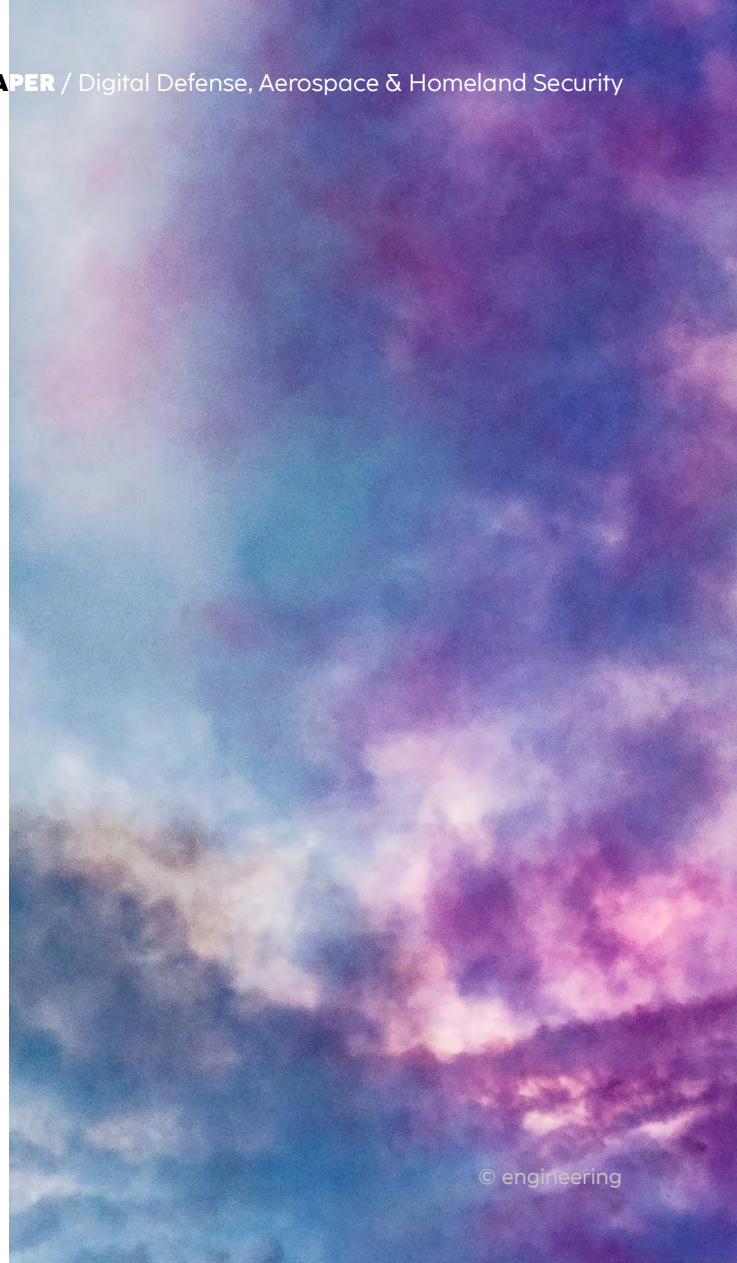
- a reduction in time spent on manual searches on the internet

- support for automatic textual content analysis

- automatic suggestion of clues, evidence and resources useful for investigations

- expansion of investigative tools through easy integration of new services or services already in use by law enforcement agencies.

Homeland Security research is also helping to solve the age-old problem of the shortage of useful datasets to train Machine Learning and Artificial Intelligence algorithms in the area of citizen security. On this topic, the LAGO (Lessen Data Access and Governance Obstacles) project is working on defining the reference architecture for the realisation of a reliable **EU Research Data Ecosystem**.



10 What is the future for Digital Defense?

The Digital Transformation is creating numerous opportunities for the industry, opening up new digital fronts that will intersect with the challenges on the ground - whether land, air and sea - where the focus will be on data protection and management, through technologies such as IoT, AI and Cybersecurity.

The Digital Transformation is creating numerous opportunities for the industry, opening up new digital fronts that will intersect with the challenges on the ground - whether land, air and sea - where the focus will be on data protection and management, through technologies such as IoT, AI and Cybersecurity. Comprehensive, accurate and real-time information translates into strategic, logistical, tactical and intelligence superiority as it enables more effective decision-making and strategies. Cybersecurity will therefore be increasingly central to any nation's defense strategy, aimed at ensuring the maximum protection of its citizens, moving from a reactive to a more proactive stance, becoming more autonomous and self-evolving, identifying hidden vulnerabilities and blocking attacks in a preventive manner.

In this scenario, research and technological innovation, supported by appropriate investment policies and effective governance, will be key to meeting the challenges of the industry. The success of these activities, however, cannot disregard the collaboration between institutions and innovative, reliable and competent technology partners, who can accelerate the evolution process of Defense organisations, enabling them to keep pace with continuous technological change.

We position ourselves as a strategic partner to accompany governments, institutions and their suppliers on this evolutionary path and to accelerate the development of new solutions and technologies. We believe in the need for partnerships with companies that are based on trust and technical skills - but above all on process expertise. We pursue this path according to the military/civilian dual-use approach, which will be increasingly central to the sector.

In the current historical context and for the years to come, the reuse and sharing of skills acquired and solutions realised in both sectors will be essential. From a strategic point of view, the military instrument will increasingly act in conjunction with the civil authorities to guard the territory, supporting them during the occurrence of natural disasters. Furthermore, from the point of view of operability and safeguarding investments, being able to rely on systems that are "multi-purpose by design" will, in fact, increase the resilience of an entire country system, while optimising the resources deployed.

www.eng.it

Engineering Group

@LifeAtEngineering

@EngineeringSpa