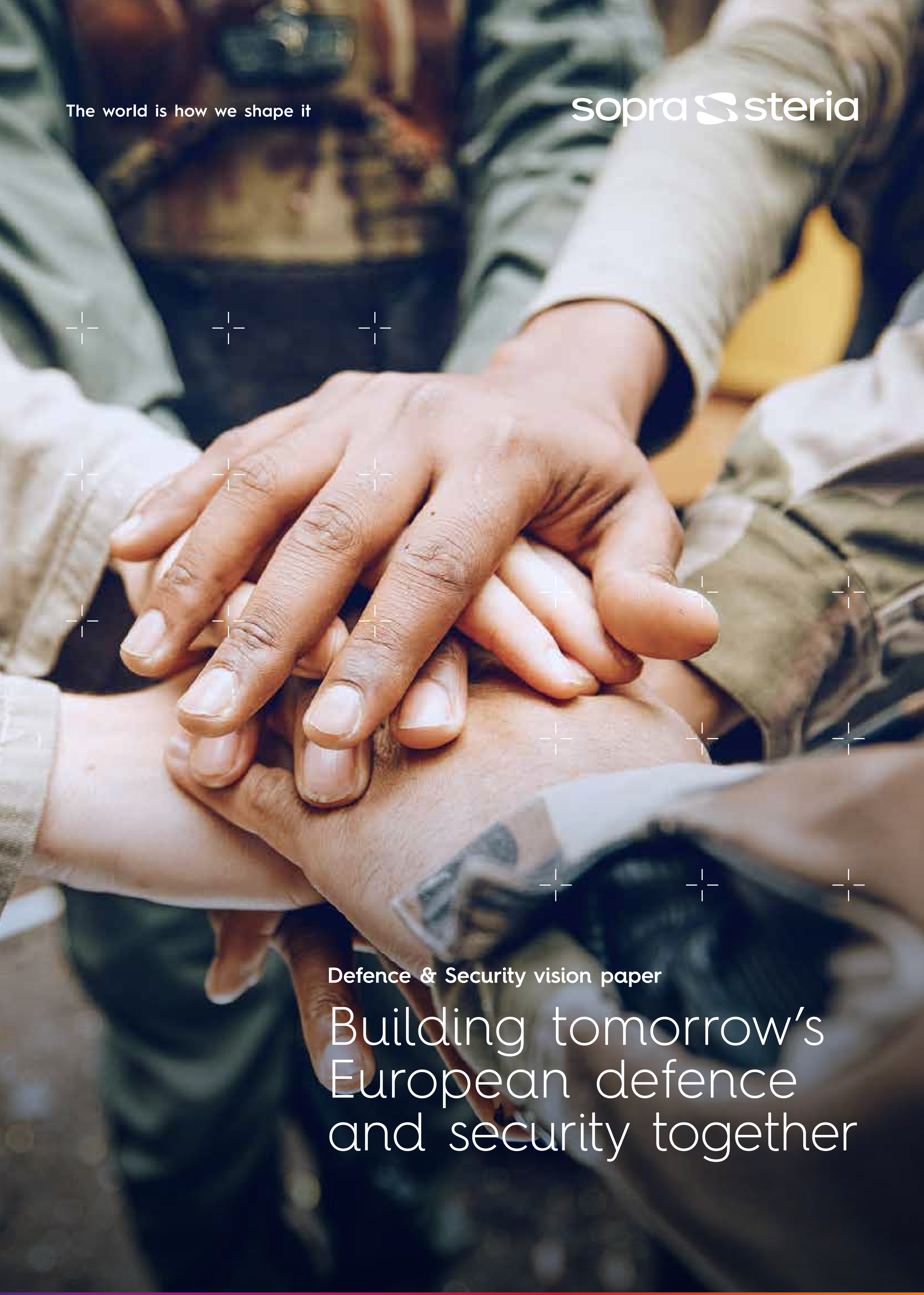
The world is how we shape it



Defence & Security vision paper

Building tomorrow's European defence and security together

"Building tomorrow's European defence and security together": based on this mission, Sopra Steria aims to contribute to shaping a stronger Europe - one that can face the challenges and dangers ahead, one that is more protective and equitable for all its citizens, and one that is sovereign enough to defend the foundations of our democracies.

In a world full of tensions and uncertainties, which is also witnessing the advent of disruptive new technologies, we are much more than a digital services company in the Space, Defence & Security sector. We are a major player in the field, responding to the major security challenges of today and tomorrow. With a presence in more than 14 European countries, we are a sovereign, **European defence and security digital industry player, serving the armed forces, interior and justice ministries**, bringing innovation in digital technology and business areas[1] as well as comprehensive solutions to our customers. In France, some 1,000 employees are already helping to strengthen the security of goods, people, and both the national and European territory by meeting the challenges of sovereignty, trust, and ethics.

This document is based on the observation that the world is in a state of upheaval, and that thanks to our expertise in cutting-edge technologies, safety-critical systems, and our business know-how in a wide range of fields, we are preparing armies, homeland security forces, and the justice system to meet the challenges they face.

With this vision paper, we are reaffirming our commitment and our contribution to European defence and security, both at present and in the future. Drawing on our strengths, we are anticipating tomorrow's world and building it together with other defence and security players, while remaining aware of the risks weighing on Europe and beyond, and fully confident in the future.

Laurent GIOVACHINI
Deputy Managing Director Sopra Steria

[1] Public security & identity, command and control, cyber defence, maintenance and logistics, general operational support, and military space.

Summary

01. 5 - 6
Supporting Defence's technological transformation to face a fast-changing world

02. 7 - 10
Mastering multi-environment, multi-field (M2MC) operations and accelerating the digital transformation of defence and security

03. 11 - 12
The foundations of our vision

04. 13 - 15
Our three guiding principles in serving our customers

05. 16 - 17
New technologies for Defence and Security

- Artificial intelligence 18 - 23
- Quantum technology 24 - 29
- Sovereign combat cloud 30 - 31
- Digital twins 32 - 36
- Extended reality 37 - 38

06. 39 - 40
Together with our partners, we are building the European defence and security of tomorrow

Supporting Defence’s technological transformation to face a fast-changing world

01.

From an era of crises to an era of shocks

Admiral Vandier, Major General of the French Armed Forces, recently stated that we are transitioning from an era of crises to one of shocks, marked by new and more uncertain environments than ever before[2]. The world is indeed facing renewed strategic competition in all areas. From the Indo-Pacific to Europe, through Africa and the Middle East, an arc of tension is forming. In Europe, war made a striking comeback in February 2022. The invasion of Ukraine represents a strategic shift that raises numerous concepts: nuclear risk, the return of a global strategy and hybrid actions, high-intensity conflict, the return of symmetrical, multi-environment, and multi-field warfare, the use of dual technologies such as the Starlink satellite constellation, the use of artificial intelligence, and the "droning" of the battlefield.

The Hamas attack on Israel highlights the main features of so-called "asymmetric" warfare and the crucial importance of intelligence. It demonstrates that the relationship between the weak and the strong can change with support from third-party states, often operating in the shadows: simultaneous land, sea, and air operations meticulously prepared for months, rocket attacks, infiltration of fighters from the air, and more.

Lastly, climate change has major geopolitical consequences, including the displacement of populations, the risk of states disappearing, food crises, international instability and security issues, terrorism, international crime, the intensification of migratory crises, and disruptions to supply chains.

Confronting the present and preparing for the future

All these upheavals have major consequences for our customers. The COVID-19 pandemic, the war in Ukraine, and international tensions have triggered significant changes. Since April 2022, growth in the industry has stalled, mainly due to the war in Ukraine and containment measures in China. Consequently, significant supply tensions have emerged in Europe. Moreover, the war in Ukraine and the subsequent energy crisis have highlighted two key issues: dependence on Russia for gas, and thus for the electricity it generates, and the strong interdependence between various players. Supply chains are struggling to keep pace with the demands imposed by major groups. For example, Safran has experienced problems with its subcontractors, who supply 65% of the parts used in the manufacturing of Leap engines produced by CFM, a joint venture between General Electric and Safran.

For the European Union, the war in Ukraine has confirmed its heavy dependence on China, particularly for critical raw materials and rare-earth elements. The upheaval caused by these crises and shocks has not only been material; it has also impacted organization and personnel, moral force and information warfare, equipment through-life support, network security, and data protection. However, not all organizations have the human or technological resources to confront these challenges. Facing them today while paving the way for the future is the mission that Sopra Steria has set for all players in the world of defence, including companies, industries, ministries, and international organizations such as NATO and the European Union. Their renewed confidence attests to our success.

[2] Opening speech by the Chief of Staff of the French navy at the "Naval Defence" symposium, Euronaval 2022 exhibition.

02.

Mastering multi-environment, multi-field (M2MC) operations and accelerating the digital transformation of defence and security

Sopra Steria is a global leader in digital transformation and an active member of the European Defence Technological and Industrial Base (DTIB), with over 40 years of experience in the Defence & Security sector. We have a deep understanding and expertise in the sector and the markets of our customers, including entities such as the French Ministry of Defence, the European Union, and NATO. This expertise is a crucial asset in assisting them to address the new challenges they face.

Mastering multi-environment / multi-field operations

BROADENING THE SPECTRUM OF DOMAINS

The international arena is fraught with heightened tensions. Conflicts are emerging between regional players supported by powers with greater authority. The ongoing war in Ukraine exemplifies the resurgence of interstate warfare and symmetrical engagements. The spheres or fields of conflict have undergone a transformation, expanding to encompass the intangible realm and spaces where rules were either undefined or insufficiently delineated, such as the high seas and outer space. It is no longer solely about land, sea, and air. Conflicts now extend into cyberspace, space, and the realms of information and electromagnetic fields. This concept is known as multi-environment / multi-field (M2MC - multi-milieux - multi-champs), also referred to as multidomain operations in the United States.

Such operations require the integration and synergy of new combat domains (information, cyber, and spatial) within joint and combined operations (land, sea, and air), with a swifter decision-making loop "aimed at surprising, overwhelming, or disrupting the adversary[3]." In this context, digital technologies play a pivotal role, including cloud computing, artificial intelligence, extended reality, and soon-to-be quantum technologies.

CYBERSPACE AND L2I

Cyberspace encompasses a wide range of activities and stirs up every kind of greed: espionage, crime, sabotage, and influence. In recent years, there has been an increase in cyber attacks against hospitals, strategic defence industries, and public institutions, with no way of identifying the perpetrators. In France, between January 2022 and June 2023, the ANSSI dealt with an average of 10 attacks per month involving local authorities, affecting 42 out of the 101 French departments and 12 out of the 18 French regions.

These are alarming figures. Informational warfare, which offers a wide range of effective means of action, has also taken on a very important role in the ways our adversaries act, with hostile actions carried out against our interests, whether in certain theatres of operation (notably in the Sahel region) or on national territory. France's Cyber Influence Warfare doctrine (L2I - *Lutte informatique d'influence*), which refers to military operations conducted in the field of information in cyberspace, represents a major capability area that needs to be mastered in order to detect, characterize, identify, and react to these massive and varied attacks.

[3] Étienne Faury, "Multi-domain operations: a military revolution", La Revue Défense Nationale, 2020 : chocs stratégiques - Regards du CHEM - 69th session.

SPACE AND VERY HIGH ALTITUDE

• **Space**: "The space issue is fundamental if we are to remain part of the club of nations capable of retaining sovereign intelligence and observation resources", stated Sébastien Lecornu, the French Minister of the Armed Forces.[4]. Observation, intelligence, communication, protection of national interests, and prevention of environmental risks - space today plays an essential role in defence, homeland, and civil security. As a result, this strategic domain is becoming an area of major tensions and challenges. The spectrum of possible actions is wide: jamming, taking control of, or even destroying satellites. Space reflects geostrategic disturbances on Earth.

• **Very high altitude**: Between space and sky, the upper airspace (EAS), situated between 20 and 100 kilometres, has become a new defence concern[5]. This altitude range is gradually being populated by new objects serving vastly different needs, both civilian and military, such as suborbital aircraft, stratospheric balloons, and hypersonic gliders. Given these significant developments, it is imperative to establish cooperation among all stakeholders to ensure the safe, responsible, and equitable utilization of this space.

MARITIME SPACES AND THE SEABED

• **Maritime spaces**: France boasts the world's second-largest maritime territory, spanning 11 million square kilometres. The French navy safeguards France's interests and promotes peace through five primary missions: intelligence gathering, risk prevention, intervention in conflict zones, protection of seas and oceans, and assistance to ships, including deterrence with its SSBNs[6].

• **The Seabed**: Once largely inaccessible, the seabed now holds significant strategic value. The advent of advanced unmanned underwater drones capable of military operations is transforming these depths into new arenas of conflict. Particularly noteworthy is the increasing interest in the deep seabed, driven by challenges in rare metal and natural gas supplies, with potential reserves of gas, hydrocarbons, and lithium. Additionally, conserving biodiversity remains a paramount mission for France and its overseas territories. Furthermore, submarine communication cables play a vital role in global information exchange. The French National Agency for the Security of Information Systems underscores their importance, highlighting their role in "the communication space formed by the global interconnection of automated digital data processing equipment"[7]. Today, over 95% of worldwide communications rely on submarine cables.

[4] Objectives of the French military programming law (LPM - Loi de programmation militaire) 2024-2030: mastering new areas of conflict | French Ministry of the Armed Forces (defense.gouv.fr).
[5] Agnès d'Heilly, Director of Public Affairs at Ariane Group, at the "From sky to space. New operational challenges at very high altitude" symposium, École militaire, January 2023.
[6] The missions of the French navy: Missions and Organisation / The French navy - www.lamarinerecrute.fr
[7] ANSSI 2011, Defence and security of information systems - France's strategy report (Consulted on 05/04/2022).

Accelerating the digital transformation of defence and security

Achieving the capability objectives required to meet the many challenges facing our customers necessitates a long-term digital transformation. This is the challenge at this operational level. It encompasses the information and communication systems of armed forces in operations, as well as cybersecurity, data control and protection, and inter-service, joint, and combined interoperability.

This digital transformation extends beyond Defence. Digitizing the French Ministry of the Interior is a major challenge. In France, the Ministry of the Interior's Guidance and Programming Act (LOPMI - *Loi d'orientation et de programmation du ministère de l'Intérieur*) underscores the need to invest in technology and digital transformation. This means better incorporating digital technology into public policies, preparing for major sporting events by strengthening cybersecurity, simplifying everyday life for public service users by overhauling complaints procedures and digital identity, and transforming digital working methods by bringing law enforcement closer to the public in public spaces.

SOLUTIONS FOR CIVIL PROTECTION

In Germany, Sopra Steria has developed the IGNIS-Plus solution specifically for fire and rescue services. The system's scalability and high adaptability provide a basis for potential applications across the sector, including authorities and organizations with security tasks, as well as factory fire brigades. IGNIS-Plus is successfully used by various fire and rescue centres in several German metropolitan areas and conurbations as an operations control system, ensuring maximum reliability even during peak loads.

As a combination of software and hardware, IGNIS-Plus meets diverse requirements and delivers the fast response times needed for comprehensive deployment management.

Digitizing the justice system should also enhance efficiency by simplifying procedures and fostering cooperation among all stakeholders, particularly in the criminal justice system. Judges and those involved in the justice system need access to high-performance tools, and litigants should be able to apply for legal aid, initiate legal actions, and monitor their cases online. Additionally, it should be easier for prisoners to navigate the criminal justice system. Lastly, minors in the judicial youth protection system require more effective monitoring.

These initiatives form the foundation of our forward looking vision, focusing on innovation and the pooling of expertise

03.

Foresight: integrating uncertainty

"Tomorrow will be nothing like yesterday. It will be new and will depend on us. It is less something to be discovered than something to be invented." At Sopra Steria, we strongly believe in the words of Gaston Berger, the inventor of the term "foresight".

To reinforce their capacity for innovation, their business processes, and the resilience of their organizations, our customers need to develop solid strategies. To do so, they must analyse the world as it is - full of uncertainties and upheavals - and also prepare for the future through foresight.

Innovation: a comprehensive approach to integrating disruptive technologies

The increasingly complex defence and security environment requires a global perspective and a robust technological innovation strategy to ensure that services are constantly adapted to the evolving constraints characteristic of this strategic sector. In this context, two major technologies stand out: artificial intelligence and quantum technology.

Our customers believe that AI will become essential in the future, and they are right. AI is less associated with futuristic robots and more with tools for productivity, prediction (e.g., maintenance through the convergence of IoT and AI, as well as the metaverse and digital twins), decision support (e.g., collaborative combat with augmented intelligence), improving living and working conditions, management, and more. We help our customers manage the challenges associated with introducing AI into their organizations. Similarly, as physicist Julien Bobroff points out, "Quantum technologies are at a turning point". These quantum technologies extend beyond cyber defence (attack and defence), communication networks, and cryptography. They actually cover a much wider spectrum of defence fields. Quantum technology has three main areas of application: cryptography, sensors, and computers (optimization and simulation). In all three segments, defence applications are possible, including military space and telecommunications, submarine localization or stealth, detection of chemical and biological weapons, health, new materials, and more.

Support and pooling of expertise

At Sopra Steria, we work closely with our customers in the field to offer comprehensive solutions and optimal service, backed by technological innovation.

Today, organizations such as governments, ministries, and private bodies face multiple challenges in terms of defence and security. Better control of data and information is essential to minimize risks and ensure strategic and robust digital autonomy.

At Sopra Steria, we are convinced that pooling expertise and information enhances efficiency and guarantees the security of both people and data.

Our three guiding principles in serving our customers

04.

Being a trusted third party at the heart of innovation

What does it mean to be a Trusted Third Party as a sovereign European tech company? It involves addressing issues of political confidence (Sopra Steria focuses on serving the interests of governments and critical European companies), digital confidence (security), and economic confidence (ensuring critical technologies remain European).

In an increasingly complex and tense world, and in a competitive economic environment characterized by an informed and demanding customer base, innovation means maintaining technological superiority over France's and the European Union's adversaries, ensuring our security, and staying ahead of our competitors.

Sopra Steria collaborates with its customers to develop tailor-made solutions that leverage digital technology for the benefit of people. For more than 40 years, our relationship with our customers has been based on trust and reliability.

Committing to ethical technology

Artificial intelligence, cloud computing, quantum computing, the industrial metaverse, 3D printing - our world has entered a new phase of technological acceleration that offers greater efficiency in production and organization for manufacturers. For the armed forces, law enforcement, and the personnel of the French Ministry of Justice, these technologies provide operational efficiency, accessibility, and transparency.

However, this digitization raises many questions: personal data, platform transparency, algorithm traceability, the role of humans in decision-making, and more. How can we imagine the future digitization of our economy, social life, private and professional behaviour, armed forces, and public authorities without considering an ethical framework? The economic development of businesses, the operational deployment of armies and law enforcement agencies, and the digitization of the justice system can no longer proceed without taking social and environmental impacts into account.

"Digital ethics encompass all the principles and values that apply to the design, production, marketing, promotion, use, consideration, and management of all the effects induced by digital technologies and their constituent elements or those necessary for their operation. These include social and environmental impacts, the protection of personal data and individual free will, and the principle of non-discrimination. It is not a crutch or an additional step but a means to action and a foundation for trust[8]."

Sopra Steria is committed to digital ethics to promote responsible, humane, and sustainable digital transformation strategies. We have created a speech competition on digital ethics and launched an ethical business award. But beyond these official aspects, we integrate digital ethics into every stage of the transformation, whether in consulting or integration.

> If an ethical approach is not adopted, companies may inadvertently expose themselves to more risks than benefits. They may not sufficiently identify and implement the right safeguards to manage or mitigate these risks.
>
> **Kevin Macnish**
> Consulting Manager in Digital Ethics, Sopra Steria UK

[8] Floran Vadillo, Consulting Director, Ethics & Sovereignty, Digital ethics: what choices for action based on trust? The Exploratory, Sopra Steria Next.

A sovereign player serving customers throughout Europe

Sopra Steria is a sovereign French company at the heart of the European Union, serving customers in fourteen countries across various fields. In a post-Covid era marked by the war in Ukraine and heightened international tensions, the issue of sovereignty has become a major concern once again. Our unique positioning places us at the core of the European DTIB.

> We envision the future combat cloud as a global mesh network for redistributing data and sharing information at strategic, operational, and tactical levels. The cloud serves as both an accelerator and a vector for operational and logistical transformation and efficiency.
>
> **Hugues Valentin**
> Cloud Center of Excellence, Sopra Steria

05.

New technologies for defence and security

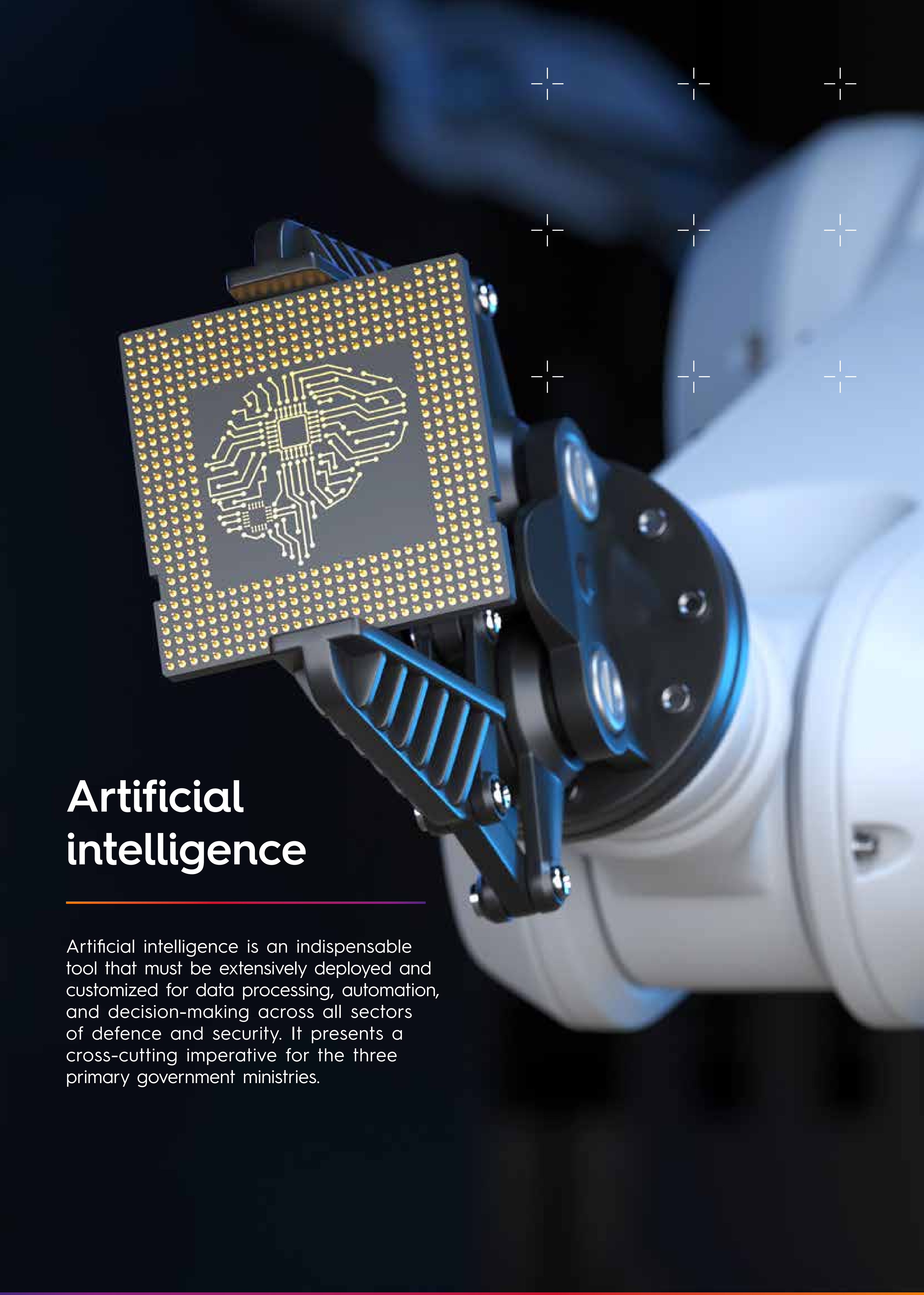
Sopra Steria is a key partner in digital sovereignty. With a long-term vision for the benefit of regal ministries in both France and Europe, we are renowned for our transformation capabilities and industrial offerings in six major business areas:

- **Operations & General Support**: asymmetrical combat and the return of high-intensity conflict present multifaceted threats to our armies. The sovereign combat cloud is an essential tool for preparing them for various circumstances and types of confrontation. The cloud also supports General Support functions, including human resources and payroll, both in France and the UK.
- **Command & Control**: this involves a set of organizational and technical attributes and processes that use human, physical, and information resources to accomplish missions, perform tasks (C2), and report back.
- **Cyber Defence**: cyberspace is complex and includes several areas such as information warfare, post-quantum cryptography, and the cybersecurity of systems and artificial intelligence.
- **Public Security & Identity**: the state, through its Ministries of the Interior and Justice, is responsible for public order and security, aiming to protect the population and ensure fair, transparent, and effective justice.
- **Maintenance & Logistics**: the operational effectiveness of our forces depends on the efficiency and quality of support services such as operational readiness and logistics.
- **Military Space**: military space encompasses orbital operations and "combat," meaning passive and active actions conducted by a state in space to ensure the integrity of national space capabilities and services, maintaining freedom of action in this environment. Space warfare also includes actions on ground systems (receiving stations, command and control systems, etc.).

Multi-environment/multi-field integration: technologies in business domains

Cyber Defence	General support for operations	Maintenance & Logistics	Command & Control	Public Security & Identity	Military space
AI	Trusted cloud	Quantum technology	AI	AI	Quantum technology
Quantum technology	Digital twin	Digital twin	Quantum technology	Digital twin	AI
Digital twin	AI	AI	Digital twin	Trusted cloud	Digital twin
	Extended reality		Extended reality	Extended reality	

In the Defence & Security domain, characterized by its multi-environment, multi-field nature, it is crucial to align the technologies we excel in with the recognized business areas. Our comprehensive understanding and expertise empower our partners to navigate the ever-evolving constraints of defence and security effectively.



Artificial intelligence

Artificial intelligence is an indispensable tool that must be extensively deployed and customized for data processing, automation, and decision-making across all sectors of defence and security. It presents a cross-cutting imperative for the three primary government ministries.

Command & Control

Digital technology is profoundly shaping the Command & Control concepts of military operations. Meanwhile, artificial intelligence has become indispensable within the armed forces. The war in Ukraine has highlighted the application of AI at the tactical level, which will expand to operational and strategic commands. These commands require the most realistic view possible of the theatre of operations to formulate orders effectively and in a timely manner. Having a realistic vision is one aspect, but acquiring it at the optimal moment and comprehensively enough to understand the context and, above all, ensure the accuracy of the information, is another matter entirely.

In this context, mastery of AI offers combatants a decisive advantage.

"Today, faced with multifaceted enemies and dangers that strike civilians and soldiers indiscriminately, in a complex, dual-use, multi-domain environment, C2 must make it possible to secure and retain the initiative and the informational, and therefore decision-making, advantage over the enemy. This requires advances in technology and adaptation of AI.[9] "

In 2021, Sopra Steria and CS played a key role in the supply of a protection solution for sensitive military sites, which should equip 28 sites by 2025, divided between the French Air Force, the French Space Force, and the French Navy. This innovative solution lays the foundations for future multi-domain protection solutions by combining the "safety" (protection against external malicious acts) and "security" (protection against internal accidents) components in a single C2 system. Designed by CS, CRIMSON is expected to be the foundation of Sopra Steria's future solutions for multi-environment operations. The aim of this offering is to enable armed forces to achieve and maintain information superiority, which is key to operational success.

CS is working on an innovative project with new artificial intelligence approaches for the detection and automatic identification of threats positioned on the coastal fringe and for anti-drone warfare at the sea-land interface. This project, TIAMAT, complements CS's global offer for maritime surveillance and protection, covering an extended area from port zones to the limits of the Exclusive Economic Zone (EEZ). Thanks to the TIAMAT project, CS offers algorithmic solutions based on artificial intelligence for decision support in maritime environments.

SSG VISION

In this context, and building on the success of our CRIMSON and rAIse[10] programmes (focused on AI), our vision is based on understanding AI not only as an end in itself but also as a formidable engineering tool. Reinforced by CS, Sopra Steria fully aligns with this global defence and security AI plan, as demonstrated by the CRIMSON program, which is currently integrating artificial intelligence.

Our ambition is to detect and collect useful and validated information to achieve information superiority and assist the Strategic Command, or any other military, civil, or dual command centre, in making decisions while avoiding cognitive saturation.

Ultimately, the goal is to have trustworthy AI at both operational and strategic levels, specifically for decision-making. Since machines can produce erroneous analyses from erroneous data, trustworthy AI is central to our concerns.

More broadly, we envision a next-generation operating system that is robust against cyber attacks, grouped within a constellation of command and control systems, interoperating within a Cloud. These systems can be tailored to specific domains (land operations, naval operations, anti-drone warfare, etc.) or span multiple domains to provide synchronized results. They will be multi-domain, reinforced, and resilient, thanks to artificial intelligence.

"We are convinced that new, ultra-powerful algorithms will enable the creation of forward-looking scenarios for external operations. For instance, they can suggest the optimal route for a convoy or identify the best drop zone for an airborne operation.[11] "

With the use of Large Language Models (LLM), it will be possible to plan, conduct return of experience (RETEX), and build scenarios by leveraging mission knowledge. We can envision the benefits of an armed forces information system equipped with generative artificial intelligence, allowing, for example, detailed reporting and note-taking for infantrymen post-mission. Combined with AI, the digital twin will enhance simulations and analyses based on RETEX and foresight, thanks to dynamic virtual representations of ongoing missions. Multi-domain C2 opens a pathway to achieving both technological and strategic breakthroughs. Technically, this tool is within reach, and Sopra Steria, along with its subsidiary CS, is firmly committed to this direction, leveraging their combined expertise.

[9] Philippe Loviconi, Operational Advisor, Multi-Domain Protection.

[10] Launched in the first half of 2023, rAIse is a major internal programme aimed at adopting generative artificial intelligence. This initiative will impact all of Sopra Steria's business consulting teams, internal development tools, and partnership strategies.

[11] Nicolas Martin, Sales Manager, Sopra Steria Group, Defence & Security Command.

Cyber defense

Cyberspace is indeed the fifth combat environment. At Sopra Steria, we have fully integrated cyberspace into the major challenges of today and tomorrow, both in France and Europe. For instance, in Germany with the Bundeswehr, we are working in the field of cybersecurity to ensure the availability, confidentiality, and integrity of data.

Additionally, Sopra Steria and CS are supporting a player in the nuclear industry in the complete overhaul of its Restricted Distribution information system.This ambitious and innovative information system features French technological innovations such as the implementation of a secure cloud and, above all, the use of a dual-level hardened workstation. This workstation, based on the SEDUCS UNIFYER solution - a ground-breaking innovation designed and developed by CS GROUP - enables two environments with different sensitivities to be used on a single physical workstation, while reinforcing the overall security level of the information system on a day-to-day basis, improving the user experience and complying with regulatory requirements.

This project will enable CEA/DAM to make a significant leap forward in its operations, facilitating remote work, mobility, connected meeting rooms, secure videoconferencing, and exchange platforms, all while maintaining or even increasing the level of security and easing the daily work of all employees.

Cybersecurity and data protection are at the heart of our defence and security expertise. For example, we are working on interoperability and interconnection between armed forces, and we are convinced that Data Centric Security (DCS) will eventually reduce the existence of numerous networks to a single network. This will facilitate the exchange, sharing, and consumption of data, with optimal data-centric defence. We are also developing a DCS component that meets NATO standards.

SSG VISION

In this tense cyber environment, artificial intelligence is essential. We have been working for three years on trustworthy AI, which is protected against cyber attacks and respects ethical rules (equity, privacy, non-discrimination, etc.).

"Because artificial intelligence is everywhere, in everyone's hands, unless it can be trusted, this new technology is worthless.[12] ***"*** Trustworthy AI is the only truly usable form as it guides our actions. The learning data, algorithms, and architecture must be transparent and unbiased. Our vision is based on practical use cases that enhance the security of networks, equipment, and the people involved. Sopra Steria is an active member of the French "Confiance.ai" collective, which designs and manufactures trust-based artificial intelligence systems and brings together nearly 50 partners, including manufacturers, SMEs, academics, and start-ups. One of its major objectives is to offer a set of tools that not only design but also validate, certify, and explain AI systems. This is the very purpose of the trusted environment that Sopra Steria provides. Beyond the national framework, "Confiance.ai" is collaborating with the German consortium led by VD to implement a Memorandum of Cooperation. This aims to support the European regulation on AI (AI Act) by creating a joint Franco-German label for trusted and responsible AI. The goal of this collaborative effort is to provide guidelines and specifications for AI applications and to prepare ecosystems for compliance with the AI Act. In practical terms, these key players in France and Germany intend to offer a common repository for trusted AI. Ultimately, this will speed up time-to-market, particularly for SMEs and SMIs, by providing them access to solutions they would not have been able to develop on their own.

> The mastery and possibilities offered by AI create major military superiority capabilities. The issue of strategic autonomy and dependence on third parties is just as important as that of autonomy in the context of nuclear deterrence.
>
> **Simon Marsol**
> European Business Coordination Defence & Security

[12] Jean-Luc Gibernon, Development Director, Cyber Campus, Sopra Steria.

Cyber defence: information warfare

"Sopra Steria's great strength lies in its ability to address cyber issues on both a large and small scale. This is reflected, for example, in the establishment of operational cybersecurity centres for major industrial groups, which entrust us with their security, as well as in the production of specific tools in limited series. In this context, the combination of skills between consulting experts and IT engineers is Sopra Steria's significant native advantage".[13]

As part of the Cyber Centre of Excellence, we contributed to the publication of a reference document on the fight against the manipulation of information last May, in collaboration with the French Ministry of the Armed Forces, several digital companies, researchers, and students from grandes écoles. Jean-Yves Le Drian, former French Defence Minister and former French Minister for Europe and Foreign Affairs, who wrote the preface to the document, points out that "the information space is one of the preferred fields of action of the powers which, with the aim of increasing their advantage and asserting their own model, intend to undermine the foundations of our democratic societies, hinder our influence in the world, and destroy the very conditions for international collective action, which is nonetheless essential in the face of the major ecological, technological, and human upheavals of the 21st century.[14]"

We have also set up a "study circle", an embryonic think tank called PEGASE, focused on information warfare, with the aim of contributing to the nation's resilience in this area and advancing thinking on the subject (methods, threats, experiences, prospects). These discussions will help generate ideas on this highly topical threat and design tools, techniques, and technological and human responses to meet these major challenges.

We are also a founding member of the board of directors of the cyber campus set up at the initiative of the French President and the French National Agency for the Security of Information Systems (ANSSI). Additionally, we have been an active member of the European Cyber Security Organisation (ECSO) since 2020 and contribute to the cyber chair at the Institute of Advanced Studies in National Defence (IHEDN).

SSG VISION

Nowadays, we think of cybersecurity in terms of the vulnerability of information systems, computer viruses, espionage, and cybercrime. However, the omnipresence of information warfare, combined with the fight against information manipulation and L2I, has become a major challenge for our country. Indeed, informational attacks are regularly carried out to discredit a state or a company, and even to undermine the very foundations of our democracies. In this context, artificial intelligence represents a risk, particularly with *deep fakes*, but it is also a remarkable tool in the fight against malicious AI.

At Sopra Steria, our ambition is to become a benchmark player in information management and L2I. We are convinced that in 10 years, information warfare will have the same importance as cyber defence and cybersecurity today. Current work in cybersecurity, particularly studies into the *modus operandi* of attackers and how to identify them, will be able to adapt to the constraints of information warfare to anticipate, identify, and combat information attacks. We also believe that "intelligent storage", the sorting and recovery of data, and the automation of identification and response processes will all be key assets in tackling this growing threat. In the space sector, for example, we are working on data integrity, ensuring that orbital data has not been transformed without the knowledge of the sensor and/or processing system before being sent back as real business data to a C2 or strategic decision-making system.

> Sopra Steria Benelux plays a crucial role in the defence and security sector by providing innovative solutions and specialised services. Its activities encompass various strategic areas, helping to strengthen the operational capabilities and resilience of government institutions and security forces.
>
> **Didier Gilbert**
> Aerospace, Defense & Security Business Unit Director

[13] Bruno Courtois, Defence and Cyber Advisor, Sopra Steria.

[14] The fight against the manipulation of information (pole-excellence-cyber.org)

Homeland security & Identity

New technologies, such as artificial intelligence and data analytics, are transforming security services and playing an increasingly crucial role within the French Ministry of Justice. The Ministry has embarked on an unprecedented digital transformation plan, resulting in profound changes to its operations. We are already working on the Digital Criminal Procedure, anticipating the imminent digitalization of civil procedures, which will entail significant changes to the information systems of the prison administration and the judicial protection of young people.

In law enforcement, where technology is already integral:

"proximity remains key, and technologies are enabling us to meet the safety challenge. Moreover, security is no longer just a national issue but a European one, with interoperability between different countries and European regulations. Sopra Steria already operates interoperable information systems in France and Europe, particularly for border control[15]".

This is all the more important as the migration situation in Europe is expected to become more challenging, making AI an essential tool for addressing this major issue.

Additionally, the proliferation of sensors and the use of satellite images allow us to create multiple data sources that can be merged for better threat management. Overall, AI is capable of addressing the security challenges facing Europe, which is also plagued by uninhibited organized crime. In 2019, criminal revenues amounted to 130 billion euros, representing 1% of the European Union's GDP[16].

We have already developed SELFIM, an AI tool that helps detect license plate fraud. Its success is evident through the implementation of DevOps and Cloud approaches, which have strengthened team collaboration and accelerated the deployment of innovative solutions that complement the existing deterministic approach.

In Belgium, Sopra Steria is assisting the Belgian Integrated Police (Federal and Local Police) in the digital transformation of police services by providing modern tools and platforms. This includes automating processes and integrating advanced technologies such as artificial intelligence and data analysis to enhance decision-making and operational efficiency.

Climate change is another pressing issue, with catastrophic events occurring more frequently. With CS, we are already engaged in fire prevention efforts. For instance, the CRIMSON platform is used by many Departmental Fire and Rescue Services (SDIS) to oversee firefighting operations and by the Alpes-Maritimes department to monitor forest fires throughout its territory.

Clearly, all areas will be impacted across all European countries.

SSG VISION

In the future, ramping up AI for all security forces and use cases, including border control, criminal investigations, biometrics, criminal data analysis, crisis management, and drone image analysis, will be essential.

For immigration and border control, we aim to develop advanced biometric identification tools such as contactless fingerprinting, which will be a significant focus over the next 10 years. Image and behaviour analysis, intelligence gathering, criminal records management, sharing of biometric information, and advanced communication and intelligent translation tools are all critical areas as Europe faces increasing migratory flows.

In response to the challenges posed by climate change, AI will play a crucial role in civil security. Future climate and environmental models will identify disaster patterns and analyse the impacts of major climatic events to better understand and anticipate threats. Building on the success of CRIMSOM, we are prepared to tackle this immense challenge.

[15] Étienne Loth, Homeland Security Market Director, Sopra Steria.

[16] The EU's action against organised crime - Consilium (europa.eu)

Maintenance & Logistics

Maintenance is crucial for the armed forces. Innovating to optimize processes and make equipment available more quickly and widely is essential. This innovation involves analysing historical data, developing Health and Usage Monitoring Systems (HUMS), creating decision-support tools, and providing remote assistance using connected glasses. Predictive maintenance and additive manufacturing with 3D printing are already helping to reduce the load on operational logistics and optimize the supply chain.

SSG VISION

Our daily lives are greatly affected by the fact that in all sectors (energy, transport, industry, telecommunications, finance, insurance, etc.), there are numerous optimization problems that we currently cannot solve. Quantum technology has the potential to solve many of these problems completely and almost instantaneously, representing a revolution in itself.

"Knowing that AI will also be optimized much more efficiently thanks to quantum technology, we are convinced that this revolution will be significantly amplified by the combination of AI and quantum.[17]"

While 2023 marked the advent of generative AIs, these are based on existing technologies (notably Transformers) that we had already integrated. These technologies can be used not only in a generative manner but also in a discriminative or extractive manner. Although users primarily see the generative aspect, the most well-known generative AI applications (ChatGPT, Bard, etc.) often combine extractive and generative AI, with extractive AI typically excelling at extracting relevant information and generative AI synthesizing this information. Thanks to artificial intelligence, maintenance can be conducted remotely, enabling faster assessments with less local expertise and more predictive maintenance.

In 2021 and 2022, we successfully used extractive AIs of the Perceiver type (a variant of Transformers) for two projects:

- In a Naval Group project to detect and classify malfunctions in submarine pumps using highly unsteady and noisy signals from a vibration sensor sampled at more than 25 kHz;
- In a proof of concept (POC) to predict breakdowns in a fleet of lorries based on information reported asynchronously over several weeks or months by their on-board supervision system.

[17] Michel Poujol, Artificial Intelligence Programme CTO, Sopra Steria.

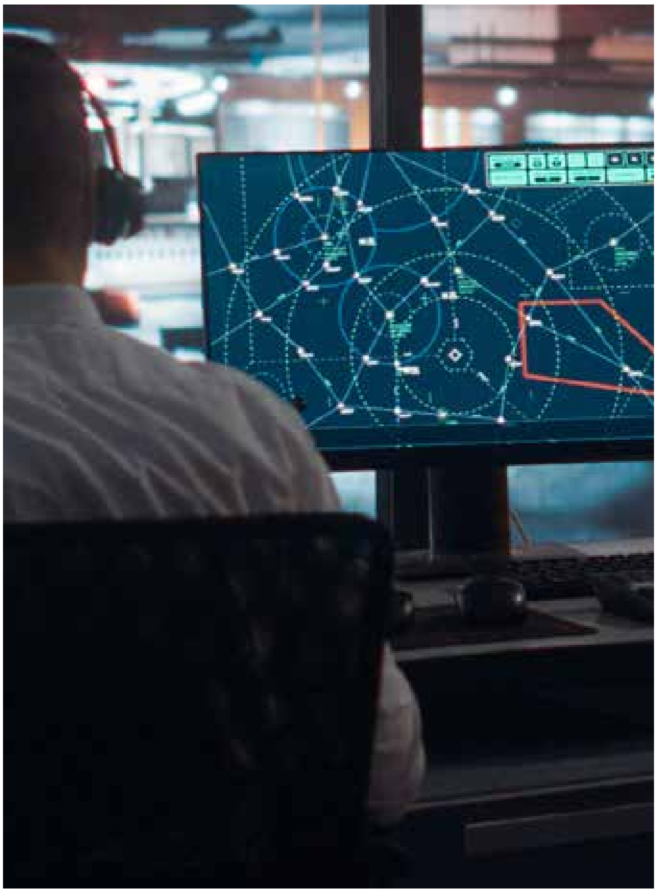
Quantum technology

Second-generation quantum technology is still in its infancy, but governments, armies, the defence industry, and start-ups already see the vast range of possibilities opening up. The quantum race has well and truly begun in the defence sector, as it introduces a new dimension of anticipation and calculation. It also increases the accuracy of sensors and offers additional methods for securing communications or breaking encrypted data. We are committed to this disruptive technology for decades to come.

Command & Control

Since 2022, the French Ministry of Defence has placed significant hopes on quantum computing technologies. This phenomenal computing capability is expected to be a major asset for the highly sensitive simulation work conducted by the Military Applications Division of the French Alternative Energies and Atomic Energy Commission (CEA). However, while eagerly anticipated for its potential to enhance analysis, this capability also raises concerns in the field of cryptography. Quantum technology can be applied in numerous areas: navigation, ISTAR (intelligence, surveillance, target acquisition, and reconnaissance), electronic warfare, quantum radar and lidar, underwater warfare, biological and chemical simulation, new materials design, and man-machine interfaces. This disruptive technology is set to become a cornerstone of future warfare by enabling the environment to instantly adapt to threats. However, it also prompts us to consider how to protect our data and communications, as this promising technology will be shared and potentially used by our adversaries.

"We are ready today to meet the challenges of tomorrow in 10 years' time. Such is our vision in the key areas of cryptography, sensors, and quantum computing.[18]"



> INA is more than just a breakthrough in mobile network analysis. It exemplifies how co-creating with our partners around innovative technologies can generate a positive and measurable impact in the telecommunications industry. Through our collaboration with Telefónica, we have developed a unique solution that combines performance, operational efficiency, and network sustainability. We are extremely proud of this joint achievement, which underscores our commitment to a more responsible digital world and sets new standards in our respective industries
>
> **Sven Wissman**
> Global Industry Lead Telecommunications de Sopra Steria

[18] Charles Praud, TME Innovation and International Development Director at Sopra Steria.

SSG VISION

Sopra Steria aligns with the new paradigm imposed by quantum technology for many applications. Quantum technology will not only offer improvements and new capabilities but will also require doctrines and concepts to evolve from the tactical to the strategic level.

Quantum sensors, for instance, offer unparalleled precision, particularly in areas like C2, electronic warfare, and imaging.

"By 2035, quantum sensors are expected to achieve such fine precision that they can identify vehicles over long distances through micro-vibrations and the correlation of micro-signals. This presents an extraordinary tool for armed forces.[19] »

Quantum computing, which aims to harness the quantum properties of matter (superposition, entanglement, etc.) to perform massive data operations, will revolutionize intelligence and targeting with extremely short decision-making loops. Remember Giulio Douhet's assertion[20]:

"Victory favours those who anticipate changes in the character of warfare, not those who adapt to them once the change has occurred."

Aware of this major challenge, Sopra Steria has been vigilantly monitoring technological advancements for years and collaborates with partners in the Quantonation fund, exploring domains like molecular design, high-performance computing, cybersecurity, and ultra-precise detection. Our pragmatic approach involves selecting use cases before formulating mathematical problems, aiming to develop algorithms that provide optimal solutions.

"We are not interested in technology for technology's sake. We are not here to oversell technology, but to provide a pragmatic vision to support an organization's strategy; that is our expertise.[21]"

Working closely with Telefonica, Sopra Steria is revolutionizing network management and planning by launching Intelligent Network Analysis (INA), a digital twin solution that explores how quantum technologies can enhance connectivity and energy efficiency in mobile networks.

Utilizing the Azure Quantum solution, Sopra Steria and Telefonica experiment with the latest quantum technology advances to improve network capacity and reduce energy footprints in infrastructures deployed in Germany. This deployment showcases how quantum technologies can enhance performance, energy efficiency, and sustainability.

Successfully implemented on Telefonica's mobile data network, this quantum simulation combines real-time mapping and dynamic traffic management within a single system. It optimizes infrastructure planning, which was previously conducted without digital support. With millions of possible combinations, network mapping was a significant challenge for conventional computers and required considerable computing time. Quantum technology offers real-time analysis of network capacity to smooth IP traffic flow. The quantum component of INA will also facilitate better absorption of traffic peaks without the need to oversize infrastructures. By identifying potentially superfluous connections and reallocating the load to different parts of the network, INA enables full exploitation of the network's capacity without requiring hardware upgrades or extensions.

Telefonica in Germany is experimenting with quantum computing to significantly reduce its energy and environmental footprint, creating a more sustainable network while improving the quality of service for its mobile users.

[19] Guillaume Roy, Head of IoT, Industry 4.0, Consulting Director, Digital Expertise Centre, Sopra Steria.

[20] Italian aviation strategist and strategic bombing theorist.

[21] Charles Praud, TME Innovation and International Development Director at Sopra Steria.

Cyber defence: post-quantum cryptography

ANSSI is now issuing a warning, echoed by numerous think tanks: quantum cyber attacks threaten to upend the countries of the European Union in the coming years. Advances in quantum computing will render current encryption systems obsolete. Immediate preparation is essential. Data protection strategies must extend beyond 2030, necessitating plans for migrating cryptographic mechanisms.

While quantum technology is not yet operational, the impending value of quantum computers is undeniable. With their immense computing power, they will swiftly crack encrypted codes and break keys in parallel, rendering currently unbreakable algorithms vulnerable. Urgent action is therefore required to ensure readiness in the near future.

In the short term, all symmetric algorithms and asymmetric encryption methods need replacement. The United States has introduced the concept of "store now, decrypt later", highlighting the importance of storing data now for decryption when the technology matures. Developing post-quantum encryption resistant to quantum computers is paramount. Cyberspace possesses a potent geopolitical dimension, underscoring sovereignty concerns, especially amid heightened international tensions and the competitive landscape between China and the United States.

SSG VISION

Post-quantum cryptography aims to develop new cryptographic systems capable of protecting against quantum attacks, as quantum computation can be used to crack current digital protections. With CS, we are enhancing confidence in cryptographic services through key generation, signature, and signature verification using post-quantum cryptography that is resistant to attacks by quantum computers.

The extensive cryptographic renewal project impacts many sectors, including the French Ministries of the Armed Forces, Interior, and Justice, as well as the banking and financial sectors. Sopra Steria and CS are proactively addressing this sensitive and strategic issue, offering solutions for migrating to post-quantum cryptography. Partnering with Cryptonext Security, part of the Quantonation fund, we provide migration plans and assist our partners in making the right technological choices. Our strength lies both internally and externally.

Military space

Similar to the air and cyber-defence domains before it, space is evolving into a battleground for major powers and potentially private entities as well. The space sector is witnessing an unprecedented wave of innovation known as *New Space*. The development of new space resources has democratized access to space technologies, involving a greater number of players and nations. Consequently, the militarization of space is progressing, utilizing techniques common to other domains.

The war in Ukraine provides numerous immediate lessons, and space is no exception. Commercial space capabilities are playing a prominent role, including symmetrical warfare between two states with space capabilities and allies, along with significant involvement from start-ups.

New Space is intricately linked to the war in Ukraine. Starlink is a case in point. By severing its services to Ukraine, Elon Musk prevented a large-scale drone attack on the Russian military port of Sevastopol. This unprecedented event also raises concerns about technological monopolies and the direct involvement of private entities in conflicts.

In the context of New Space, quantum technology holds the potential to revolutionize various sectors. Europe, through its EuroQCI initiative launched in June 2019, aims to establish a secure quantum communications infrastructure covering the entire European Union, including its overseas territories, by 2027, supported by the European satellite constellation IRIS2. EuroQCI will safeguard sensitive data and critical infrastructures by integrating quantum systems into existing communication infrastructures, offering an additional layer of security based on quantum physics. This initiative will bolster the protection of European government institutions, data centres, hospitals, energy networks, and more.

VISION SSG

"When discussing military space, we primarily refer to Orbital Warfare and Space Situational Awareness Warfare. However, space warfare also extends to Earth, with the deployment of resources capable of affecting an adversary's space capabilities through cyber attacks and strikes against ground infrastructures.

In this context, quantum technology is gradually emerging, connecting satellites, encryption, computing solutions and capacities, and security at all levels, including camouflage and stealth. Quantum technologies will play a crucial role in securing military actions in space and protecting both space itself and the satellites operating within it, defensively and offensively.

First and foremost, quantum technology serves as a multiplier of technologies. We believe that combined with digital twins, it will help to link the quantum computing environment to reality. Ground-based digital replicas of objects in orbit and their missions will enable anticipation of hostile military effects, ranging from jamming to the neutralization of solar panels rendering satellites inoperable. We believe that the digital twin serves as a catalyst for intelligence, providing real-time situational awareness for optimal decision-making. Whoever has the most accurate data to make the decision in real time will win. In addition, this breakthrough technology will enable satellites to optimize their sensors and effectors by adapting them to each situation. For example, it can find the best angle of attack using a laser to neutralize the solar panels of a hostile satellite. Our goal is to achieve satellite autonomy in optimizing its mission and making decisions within its mission perimeter, using controlled intelligence for protective actions. In the long term, the aim is to increase its self-defence capabilities, and eventually, with political authorization, to develop offensive capabilities.

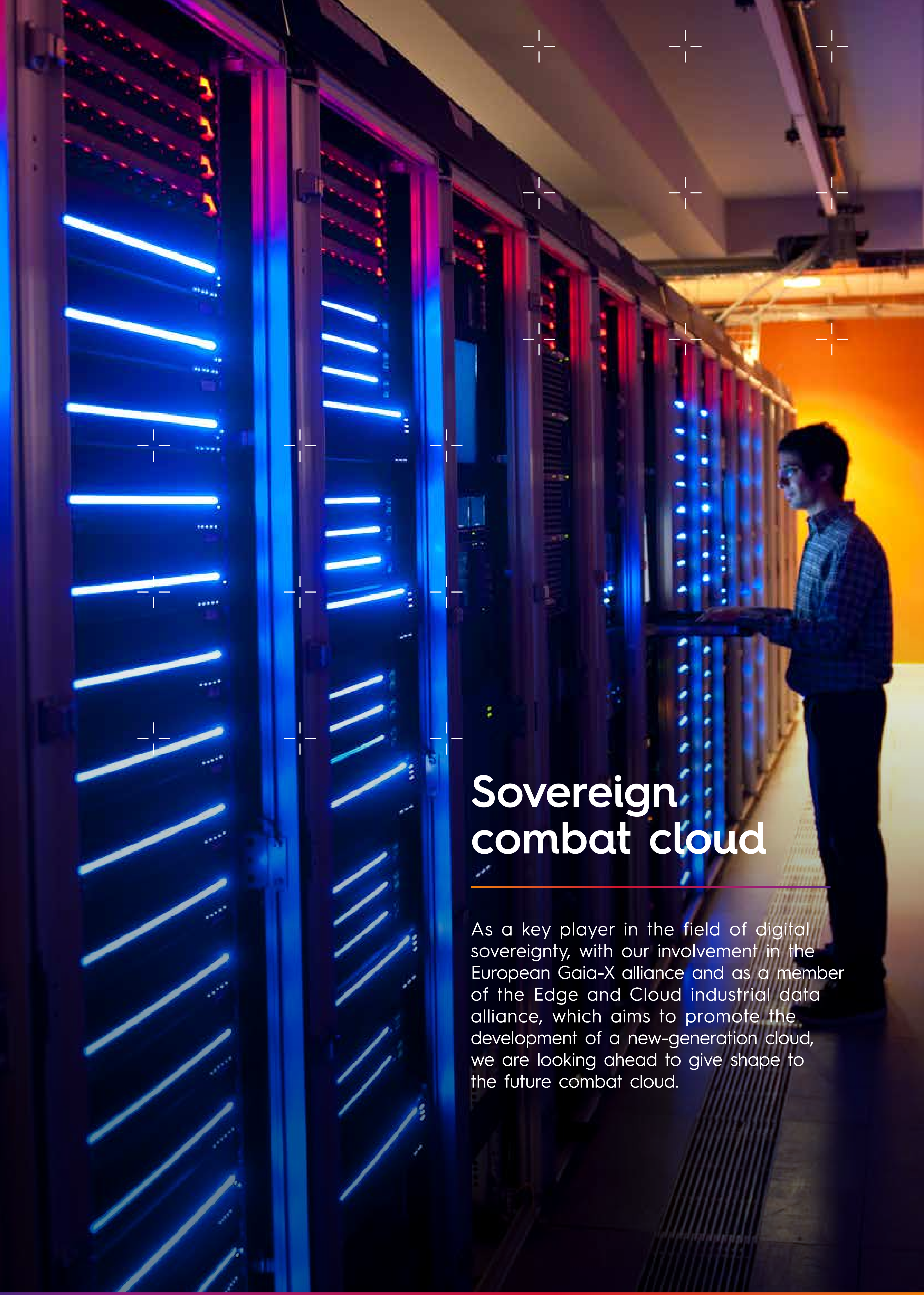
Quantum technology is opening up new possibilities, such as new materials for camouflaging satellites. Achieving in-orbit stealth involves both the physical non-detection of the satellite and the actions it can perform. Optimizing the allocation of scarce resources in space is another application on which our teams are already working.

Finally, the network of satellites will, thanks to quantum technology, organize defence in orbit more efficiently and enable inter-satellite communication without relying on Earth. It will enable continuous, real-time information sharing everywhere, allowing all forces to take simultaneous and coordinated action. In the future, it may be necessary to use lasers to control shooting in space.

"Quantum technology promises significant changes, facilitating timely decision-making in orbit while enhancing and securing information flows. Anticipation will be key, with quantum technology providing increased reliability.[22]"

This technology will also enable "decision-making intelligence", ensuring satellite autonomy. Hence, we are actively positioned in sensor and quantum computing domains for system optimization, especially for critical systems.

[22] Nicolas Sauvage, C2 and Space Operations Expert, Sopra Steria.



Sovereign combat cloud

As a key player in the field of digital sovereignty, with our involvement in the European Gaia-X alliance and as a member of the Edge and Cloud industrial data alliance, which aims to promote the development of a new-generation cloud, we are looking ahead to give shape to the future combat cloud.

General support for operations

The war in Ukraine is revealing the main features of high-intensity warfare today and in the future. Among these, digitization has become unavoidable and the cloud has emerged as one of its essential tools. The increasing importance of information processing capacity is evident, as demonstrated by initiatives such as the US *Joint Warfighting Cloud Capability* programme.

Cloud technologies have demonstrated their benefits in civilian applications for cross-referencing and sharing heterogeneous data. Armies have similar ambitions: to lift the fog of war, speed up their decision-making loop, detect changes, alert each other to dangers, reorganize, ensure supply logistics, and gain information superiority by exploiting all possible sources to the maximum. All this must be achieved while maintaining an infrastructure that is independent, economically and energetically viable, and capable of withstanding attacks. While it is an operational challenge, cloud defence is as much a strategic imperative as it is a sovereignty issue[23].

SSG VISION

"We believe that in the future, the cloud will offer vast computing, storage, and information processing capacities, particularly on-premise, thanks to artificial intelligence, in an ultra-secure way.[24]"

Our vision is based on the efficiency of interoperability and the sharing of platforms and applications not only among the French armed forces but also within Europe and the Atlantic Alliance. We are a natural partner for European institutions and a key player in major digital sovereignty initiatives. We are also a member of the European Edge and Cloud Industrial Data Alliance for the next-generation cloud. Transforming the way allies collaborate - enhancing intelligence sharing, shortening information processing, and expediting decision-making through exchanges between command systems - is central to our technological considerations and the support we provide to our customers. For instance, the British government benefits from the BlueJaySecureCollaboration solution, thanks to Sopra Steria UK. This high-performance private cloud offers scalable and secure access to all users while meeting stringent security and data access requirements.

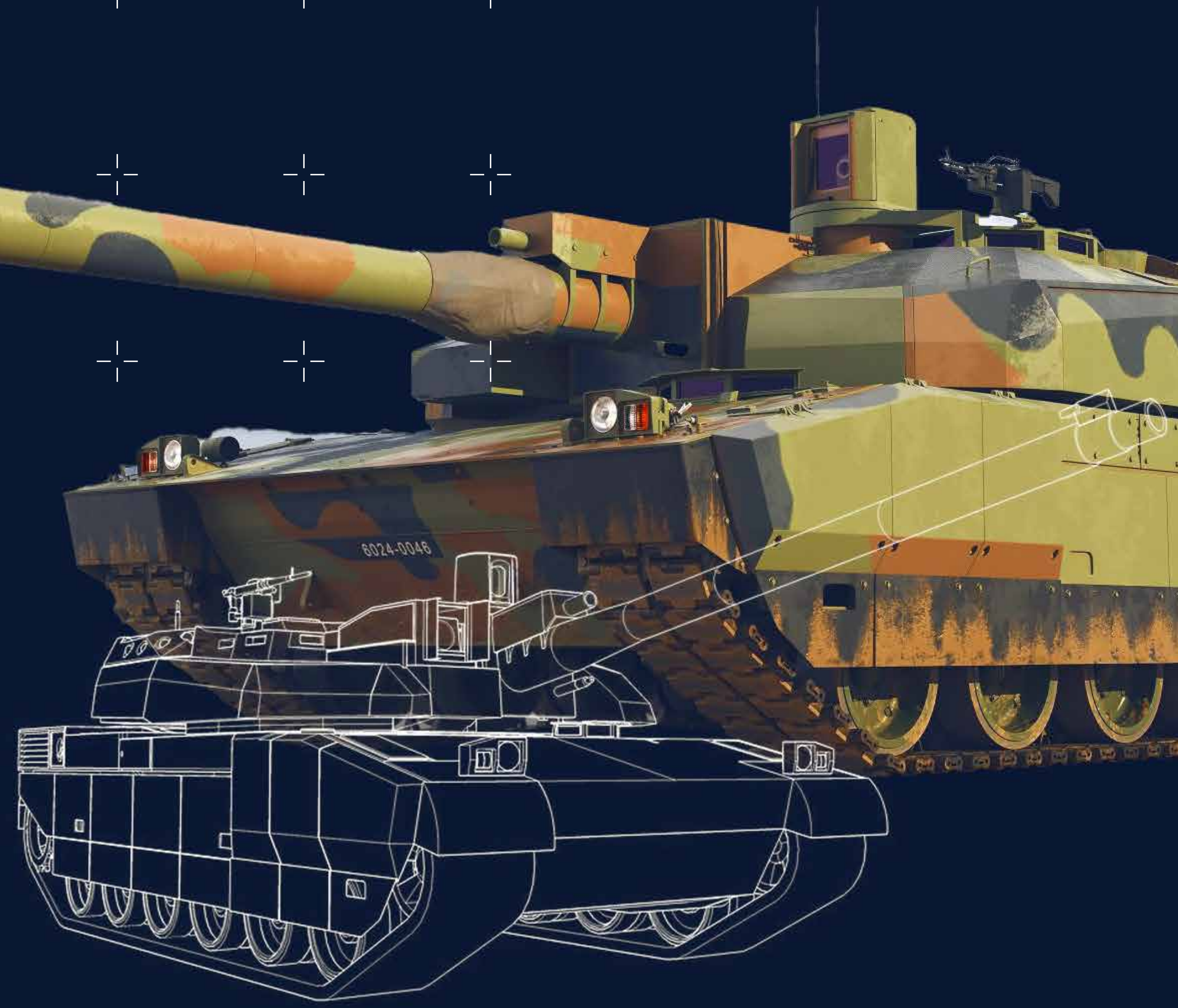
Ensuring that our armed forces are ready at all times, with a high rate of equipment availability, is a major challenge. The cloud is a tool that will revolutionize Through Life Support (TLS) with predictive and intelligent maintenance supported by data enhancement and its sharing across a chain comprising all subcontractors. Updating aircraft in flight, major technical overhauls of ships, aircraft carriers, and submarines, and modernization programmes are already possible thanks to the cloud. By 2035, multi-service and multi-national data sharing will be feasible, enabling extensive processing in the cloud, distributed to the *far edge*, ensuring tactical and strategic superiority.

However, logistics, interoperability, and operations must be considered alongside security. The cloud, with its disconnected technologies, will facilitate edge computing to encrypt data at the closest possible point, thereby enhancing cybersecurity. The war in Ukraine has underscored the shift of data warfare to the cloud. This war also represents a significant paradigm shift in France and Europe, bringing issues of sovereignty (digital, defence, energy) and autonomy (strategic) back to the forefront. Our vision hinges on a sovereign and autonomous cloud, reducing dependence on hyperscalers and their data centres. The French Ministry of Defence has devised a multi-tiered cloud strategy - central, edge, and far edge - with operational cloud capacity for the latter two, ensuring autonomy when networks are unavailable. Looking ahead, the next stage in the development of the multi-domain combat cloud is imminent, with a target set for 2035. Our objective is to establish a decentralized combat cloud, resilient to cyber threats, fostering collaboration across all domains - land, air, sea, space, and cyber. This interconnectedness will seamlessly link all forces, integrating diverse platforms to enable real-time and continuous information exchange among the armed forces.

We envision the future combat cloud as a global mesh network for redistributing data and sharing information at strategic, operational, and tactical levels. The cloud serves as both an accelerator and a vector for operational and logistical transformation and efficiency.

[23] French Institute of International Relations (IFRI - Institut français des relations internationales) study, "Cloud defence: an operational challenge, a strategic imperative and a sovereignty issue"

[24] Hugues Valentin, Cloud Centre of Excellence, Sopra Steria.



Digital twins

As an expert in the field of the metaverse and digital twins through its Digital Expertise Centre, Sopra Steria has embarked on the path to Industry 5.0 and operational efficiency. In the tense context of a return to high-intensity warfare, multi-domain Command & Control, and secure maintenance and logistics present real challenges for our armed forces and those of Europe. Our expertise in digital twin technology is therefore a significant asset.

Command & Control

The use of digital twinning in military and dual-use applications is a game-changer. By integrating the physical and digital worlds through robust connectivity and the use of artificial intelligence and simulation technologies, decision-makers and commanders can better understand their environment, enabling them to make informed decisions when necessary. Digital twins will help operational commanders develop their campaign plans more effectively, anticipate and adapt their actions and tasks on the basis of up-to-date data. This capability, applied to all levels of command - strategic, operational, and tactical - provides a significant advantage by offering informed actions and decisions based on timely, high-quality data. The twin will offer recommendations on optimizing resources in various scenarios. For instance, the use of a drone in different configurations is a good example, and the war in Ukraine underscores the importance of optimizing resources according to the adversary's posture. Digital twinning will enhance understanding of threats and potential countermeasures.

For commanders responsible for providing resources, support, and training in the continuum of crisis, confrontation, and conflict, digital twinning offers substantial benefits. A twin can optimize the management of infrastructure - whether land, air, or sea - improve energy utilization, providea different perspective on safety, and facilitate the deployment of personnel for specific tasks. For digital twins to be effective, trust in the data is crucial. Both data accuracy and trustworthiness are fundamental. Indeed, if the data entering the digital twin environment is corrupted or false, it will lead to erroneous information and potentially disastrous command decisions.

The creation of the twin is based on data from sensors deployed on the real object to be twinned, but also on simulation models and AI to reproduce the behaviour and characteristics of the physical twin to aid decision-making. It is thanks to the sensors that the connection with reality is established. The quality of the sensors and their ability to capture reality are at the heart of the concept.

In the concept of digital twinning, there is a permanent exchange of information and data between the physical twin and the virtual twin. This flow must occur at regular intervals, in line with the operational rhythm. This exchange is the key to the success of the concept in an operational environment where the decision or information provided to decision-makers will be based on the latest information received.

The digital twin transcends mere simulation by introducing the concept of "dynamic reality", enabling decision-makers to demand more from the twin. This is because there is an element of monitoring and optimizing the physical object based on a digital Observe, Orient, Decide, and Act loop.

Until now, digital twinning in the military sector has primarily been viewed through the lens of maintenance and logistics. The ability to track the wear and tear (attrition) of a helicopter rotor or a ship's engine via a digital twin and real-time data flow enables predictive and corrective maintenance as needed, serving as a tool for anticipation and optimization.

However, the true value of a digital twin is even greater when applied to multi-domain C2 operations. It has the potential to redefine the planning, conduct, and execution of operations, ultimately providing a strategic overview of all activities. Digital twinning is feasible only with robust connectivity and an IT infrastructure capable of collecting, storing, and utilizing real-time data, which also enables simulations.

The UK Ministry of Defence relies on Sopra Steria to deliver reliable digital inventory management services and integration capabilities that support effective decision-making through access to relevant data. Maintaining, modernizing, and transforming the British Army's logistics and support services are significant challenges. At Sopra Steria, we leverage our company-wide digital capabilities in engineering solutions throughout supply chain management, utilizing enabling digital technologies such as digital twins, blockchain, and secure collaboration environments to ensure the UK Army effectively meets these challenges.

SSG VISION

There are several use cases where digital twins bring significant added value to defence, particularly in the military. Operational use cases are just the tip of the iceberg. Sopra Steria clearly identifies the opportunities that exist within this technology and its related business domains.

Multiple use cases can be developed across various fields (land, sea, air, space, and cyber). Multi-domain operations are a perfect illustration of how digital twins can be utilized in mission planning and execution, decision support, training, and simulation across a broad spectrum of functions (logistics, operations, health, etc.).

For instance, to plan an operation, the commanding officer of a force deployed in a theatre of operations can leverage digital twin capabilities with the latest available data. This includes identifying the best 3D zone for an amphibious operation, demining routes, and resupplying units at sea before an assault. In essence, the twin suggests action plans based on a range of factors, including the complexity of the landing, knowledge of the terrain and seabed, assessment of threats, availability of accurate information, and the capabilities of the units, including their level of training.

We firmly believe that the digital twin operates across various levels of combat. The strategic commander who has other operations under his command can anticipate and distribute his forces more effectively. This twinning capability enables planning to move from prediction to decision.

At the tactical level, commanders have the ability, thanks to the digital twin, to conceive, plan, and adjust their operational forces and resources for optimal positioning to execute a successful operation. For example, employing drones to "refresh" the twin's data with real-time information before a landing or deployment of forces can be highly beneficial. Indeed, the landing force commander will be able to reassess and revise his intentions based on the recommendations from the digital twin. Using a digital twin requires absolute trust in the collected data and its use in near-real-time configurations through various algorithms and models. In such a context, the philosophical question of man's position in relation to the loop will likely arise. Indeed, with such a powerful tool, we might be tempted to rely entirely on the twin without considering the human factor. Today, it is recommended that people remain in the loop. This has always been our conviction, regardless of the technology. And it will remain so.

Maintenance & logistics

The first half of this decade has seen a major upheaval in the way things are done within the defence ecosystem. Military organizations and companies in the defence sector have faced significant supply chain disruptions caused by various factors, including the Covid-19 pandemic, the war in Ukraine, natural disasters, difficult economic conditions, and generally tense international relations. Simultaneously, organizations are navigating an expanding array of choices within a rapidly evolving landscape of emerging technologies such as blockchain, robotics, and artificial intelligence.

One of the emerging technologies already impacting the sector is digital twins, which improve supply chain adaptability in the event of a strategic surprise. Digital twins, which combine enabling technologies and analytical capabilities, create virtual models of processes, systems, or objects, informed by real-time data.

Generally speaking, Industry 4.0 is central to our expertise. For example, in Spain, Sopra Steria is optimizing manufacturing processes in the aerospace sector using robotics, IoT, cloud computing, virtual reality, and artificial intelligence. At Sopra Steria, we are dedicated to deploying innovative digital solutions for Through-Life Support (TLS).

SSG VISION

The new coupled digital twin platforms enable the merging of real data from 3D scans (including LIDAR) with modelling data, enriched further by the generation of synthetic data to complement or detail the real point clouds. These enriched synthetic models can then be used as training datasets for AI, optimizing the movement of production robots (Zvision and Nvidia Isaac Sim) and logistics robots. AI training on digital twins also allows us to anticipate corrosion or structural fatigue problems in the short, medium, and long term (beyond 30 years), facilitating predictive maintenance operations (Siemens Energy simulations). Our expertise in the fields of the metaverse and digital twins is widely recognized. We have initiated various Industry 4.0 management programmes covering services, processes, technology, and sustainable organizational models, including the digitalization of 35 sites worldwide for Renault. Additionally, we are involved in numerous IoT projects, offering advice on methodology and deployment using 5G technologies, edge computing, and on-board AI for monitoring and controlling industrial equipment, all with associated cybersecurity. In collaboration with Schréder, a leading manufacturer of automated arms, we enhance their product offerings for customers.

Our partnership with Nvidia allows companies to develop customized 3D pipelines, facilitating large-scale simulations of physically realistic virtual worlds. This enables us to create virtual simulations perfectly synchronized with the real world, grounded in physical reality, and powered by AI. Such capabilities can range from identifying the most efficient location for a production line to mapping a combat zone using hybrid reality. This opens up new use cases and fosters collaboration around a digital twin within a company or military unit and its ecosystem.

"The benefits of the digital twin for defence supply chains and operational readines are numerous. This technology is the model that integrates all use cases.[25]"

The conflict in Ukraine compels us to anticipate future developments. Whether it is a supplier default or an embargo on strategic materials, disruptions are common. The digital twin reconfigures the logistics ecosystem to enhance resilience, including proactive measures, thanks to the benefits of the simulation it enables. We have long relied on preventive maintenance to anticipate breakdowns. However, we are now aiming for even greater optimization of the maintenance phase and simulation for functional breakdowns, which will be used to replace parts or change equipment (such as sensors with 3D printing and lighter, more intuitive screens), as well as for advanced operator training. As a result, performance gains are achieved at both technical and financial levels.

Looking ahead, we envision entering a system of systems capable of providing a robust logistical support centre in OPEX or at home, facilitated by digital twins that optimize machines and equipment while reducing the logistical footprint. We are confident that this system will meet the strong demand for pooling and collaboration between armed forces within the European Union, as well as the standardization of digital twins to reduce equipment unavailability factors. Additionally, thanks to 'what if' scenarios, we can explore potential actions to increase system resilience and facilitate pooling between different partners.

"Combined with AI and other enablers such as virtual and augmented reality or the Internet of Things (IoT), this updated and shared technology will improve automation, autonomy, remote control of operations, and decision support.[26]"

Thanks to the maintenance, update, and sharing of digital twins, including in real-time, technical and technological limits will be pushed back. This system of the future will pave the way for large-scale simulation, with beneficial impacts at tactical and operational levels for the armed forces. The digital twin of the future will open up new fields of application and a whole new vision.

[25] [26] Pierre-Antoine Arrighi, Director, Digital Expertise Centre, Sopra Steria, David Maurange, Consulting Director, Digital Interaction & Metaverse, Digital Expertise Centre, Sopra Steria Next.

Extended reality

Sopra Steria is committed to supporting change in the industrial sector by offering secure, optimised and innovative solutions. The use of virtual and augmented reality in the strategic sectors of defence, security, aeronautics and aerospace helps to accelerate and optimise the design of new projects.

Public security & identity

Envisioning tomorrow's roles for the armed forces, law enforcement, and civil protection means rethinking their training and mission planning. As a result, new technologies are set to develop significantly within these forces. Extended reality is one such technology, opening up a whole new world of possibilities.

The notion of extended reality refers to a combination of technologies that enhance reality through digital factors. This form of reality, also known as mixed reality, combines virtual reality and augmented reality. This more recent technology offers synthetic objects added to the real world that can be viewed by individuals. These objects resemble holograms and interact with the real world, coexisting with it.

Command & control

The Red Team at the Defence Innovation Agency (DIA) fully understands the importance of extended reality and digital twins for the armed forces. In its forward-looking scenario, "Chronicle of a Cultural Death Foretold," it introduced the concept of "safe spheres" or extended reality bubbles, where digital twins are integrated, creating virtual replicas of real objects with which interaction is possible[27]. Digital tools are already being used to optimize logistics and maintenance. They also assist in planning military operations by utilizing data analysed by artificial intelligence, providing soldiers with a precise view of the battlefield.

CS has developed CRIMSON Sentinel, a hypervision solution dedicated to the centralized management of protection and security systems and the conduct of operations. It relies on a powerful 2D/3D mapping engine to provide a comprehensive, synthetic, and intelligible situation report and to operate the digital twin of the site to be secured.

CRIMSON Sentinel facilitates information sharing, coordination, and decision-making, with rights management tailored to a need-to-know basis and a graphical rules editor for task automation.

SSG VISION

"We believe this technology will be essential for security forces, armed forces, and civil protection. Imagine a firefighter on a mission seeing information displayed in their helmet and glasses, coupled with lidar or a thermal camera, providing data on the temperature of an area, the risk to their team, analyses of material conditions, and the risk of collapse.[28]"

Mixed reality can also provide a complete map of the location. This is a forward-looking technological area, and we are convinced that in the future, for the armed forces (simulations, training, real operations), security forces, and civil protection, reality will be mixed: soldiers, firefighters, police officers, and *gendarmes* will be aware of their physical environment but will also consider multiple virtual parameters to help them carry out their missions.

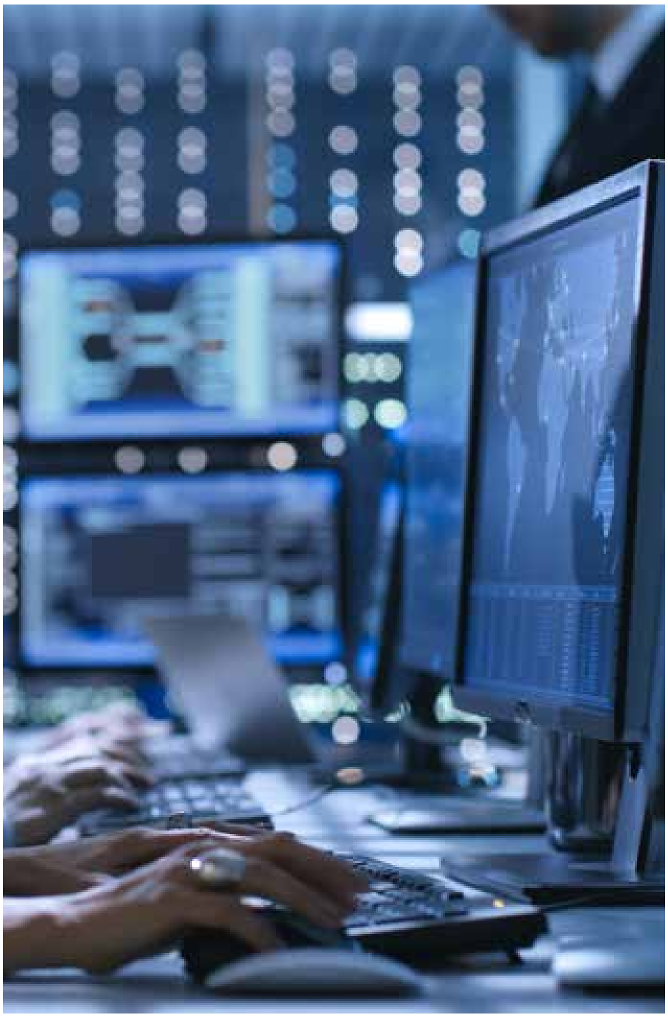
[27] https://redteamdefense.org/en/season-1/chronicle-of-a-cultural-death-foretold

[28] Étienne Loth, Homeland Security Market Director at Sopra Steria.

Together with our partners, we are building the European defence and security of tomorrow

06.

Building Tomorrow's Defence and Security Today. We have transitioned from a stage of crises to one of shocks. The world is in a state of tension: high-intensity warfare has made a resounding comeback, while asymmetric warfare persists. Climate change is causing disasters and tragedies, and security is a primary concern for French and European citizens. Our strategy for efficient defence and security relies not only on mastering disruptive technologies but also on our expertise in key operational areas. This distinctive approach, coupled with our understanding of the major challenges facing the three main French Ministries responsible for defence - the Armed Forces, the Interior, and Justice - positions us as the leading industrial benchmark in digital defence.



With in-depth knowledge of the defence and security sectors and major international issues, we can comprehensively assess the geopolitical "tectonics" reshaping the world.

With over 40 years of experience, we are a global leader in digital transformation and a member of the Defence DTIB.

We collaborate with numerous defence and security partners in Europe and worldwide. As a key player in digital sovereignty, we are developing expertise in critical areas.

We believe that "technology is an exceptional tool, a true lever of efficiency capable of suggesting new methods of engagement[29] ", as well as strengthening and securing logistics chains, and enhancing the efficiency of internal and civil security forces and the justice system. Nonetheless, we recognize that human expertise remains central. Decision-making is driven by well-trained individuals utilizing technology, which is why we place equal emphasis on professional expertise.

[29] Boris Laurent, Defence & Security Manager, Sopra Steria Next, author of "Technologie et nouvelle modalité de l'engagement tactique", in *La tactique au XXIe siècle. Le retour de la bataille*, edited by Thibault Fouillet, Foundation for Strategic Research, published by Édition du Rocher, October 2023.

The world is how we shape it

sopra steria