sopra steria

BEHIND EVERY SOVEREIGN DECISION

DEFENCE, SECURITY & SPACE

Trend report

NEXT PERSPECTIVES

This trend report was produced in partnership with CS Group and Sopra Steria Next

Benoît CHATELAIN
Global Head of Defence, Security & Space - Sopra Steria
benoit.chatelain@soprasteria.com

Pierre LOPEZ
Global Head of Defence, Security & Space - CEO CS Group - Sopra Steria
pierre.lopez@cs-soprasteria.com

Our Defence, Security and Space team and experts

Frédéric DUSSART
Executive VP Defence & Security
frederic.dussart@cs-soprasteria.com

Eve GANI
Director of Business Development & Institutional Relations - Defence, Security & Space - Sopra Steria
eve.gani@soprasteria.com

Sylvain D'HOINE
Director Space Business Unit
sylvain.dhoine@cs-soprasteria.com

Simon MARSOL
CTO Defence, Security & Space
simon.marsol@soprasteria.com

Cédric GENIN
Head of Consulting Defence, Security & Space
cedric.genin@soprasteria.com

Thierry LEMPEREUR
Director Defence, Security & Space, France
thierry.lempereur@soprasteria.com

Valérie LAINÉ,
Partner, Defence, Security & Space Consulting, France
valerie.laine@soprasterianext.com

Editorial team

Alain DURAND, Marine CASSOU, Boris LAURENT, Charles MARTY

Internal contributors

Lieutenant General (ret.) Manuel ALVAREZ, Major General (ret.) Bruno COURTOIS, Rear Admiral (ret.) Christophe EUGÈNE, Major General (ret.) Jean-Jacques PELLERIN, Frode LILLEDAHL, Louise MONJO, Charles PRAUD, François GRIME, Oana Alina SUCIU, Philippe SERAFIN, Florian MEHATS, Josepha RASAMUEL, Julien MONTROZIER

INTRO DUCTION

The sudden return of power

The return of power has ended Europe's strategic innocence. For three decades, Europe believed it was evolving in a stable environment, governed by law and solid alliances, and buoyed by the illusion of peaceful globalisation. This interlude has come to an abrupt end. The world is once again becoming conflict-ridden, fragmented and unpredictable. War is no longer a distant prospect: it is becoming a permanent condition.

We are witnessing a historic turning point, but Vegetius's old adage, *"Si vis pacem, para bellum"*[1] *("If you want peace, prepare for war")* remains as relevant as ever, as does the insight of Thucydides, who had already understood that, *"It is in the nature of man to oppress those who yield and to respect those who resist."*[2]

Whilst the nature of war remains unchanged, it is now characterised by a new model of strategic superiority based on a fourfold saturation. Saturation of space through the proliferation of constellations; cognitive saturation driven by disinformation campaigns and deepfakes; saturation of the battlefield through the proliferation of drones; and finally, data saturation, resulting from an explosion of sensors and information flows.

The war in Ukraine and the conflict in Iran serve as a stark reminder: saturation wears people down, disrupts operations and overwhelms systems. It depletes stocks, disrupts supply chains and puts industrial resilience to the test. Technological superiority alone is no longer enough; it must be sustained over the long term and on a massive scale. Admiral Vandier[3] has warned: *"We must prepare ourselves, otherwise we will suffer what the Gulf states are currently suffering."* (...) The challenge

(1) Vegetius, *De re militari.*

(2) Thucydides, *History of the Peloponnesian War,* 431–411 BCE, trans. Jacqueline de Romilly, Robert Laffont, 'Bouquins' series, 1990.

(3) Supreme Allied Commander for NATO Transformation.

is not to simply do more of what we were doing before. It is now *"to find answers to the challenges posed by Russia or Iran in their methods of warfare, in terms of the sheer volume of weapons and the speed at which they evolve."*[4]

In this context, however, sovereignty is no longer an ambition, but a prerequisite for action. Strategic autonomy gives us the ability to decide and act without being at the mercy of others, in an environment where any dependency can become a vulnerability.

In this new strategic and geopolitical framework, superiority no longer rests solely on costly systems, deemed indestructible and designed for the long term, but rather on the ability to absorb this saturation and on scale. As systems multiply and become commonplace, the value shifts: it no longer lies in the platforms themselves, but in the software that makes them intelligent, interconnected and capable of producing an effect.

The trends presented in this document are based on these observations. They describe a coherent system of forces, serving a single objective: to preserve freedom of action in a contested and saturated world, whilst guaranteeing Europe's strategic autonomy.

In the face of the ongoing shift, they form part of three imperatives that now shape action:

- ↘ **Monitoring and managing saturation:** maintaining situational awareness across all domains, from space to cyberspace and information networks, through SSA, C2 architectures and data fusion;

- ↘ **Act faster than the adversary:** fully exploit artificial intelligence, data spaces and, in the future, quantum technologies to accelerate decision-making and retain the initiative;

- ↘ **Building and regenerating for the long term:** reindustrialising, producing at scale, shortening innovation cycles and breaking the asymmetry between low-cost threats and costly defence, by focusing on intelligent and affordable mass production.

(4) Admiral Vandier, March 2026.

In this context, Sopra Steria stands out as a key player in the transformation of Defence and Security in Europe. Convinced that today's challenges shape the future, we harness innovation, expertise and hybrid approaches to strengthen the security of states, systems and data.

As a leading European partner in digital sovereignty, we contribute to building European strategic autonomy. By connecting systems, data and stakeholders, we enable resilient and interoperable operations, from command to execution, through C2, AI, cybersecurity, autonomous systems, the secure cloud and supply chain resilience. We operate at the heart of operational capabilities: we master, integrate and combine critical technologies to inform decision-making, accelerate action and strengthen resilience across the entire operational and informational spectrum. By connecting systems, data and stakeholders, we contribute directly to strategic advantage.

Benoît CHATELAIN **Pierre LOPEZ**

"In a world where saturation is becoming the norm, the question is no longer whether we must adapt, but how quickly — and with what priorities."

Monitoring and managing information overload

↘

TREND 01.

Winning the war before the war: acting in the information domain

— P. 8

TREND 02.

Strengthening air defence through counter-drone measures

— P. 12

TREND 03.

Providing Europe with a space defence capability

— P. 16

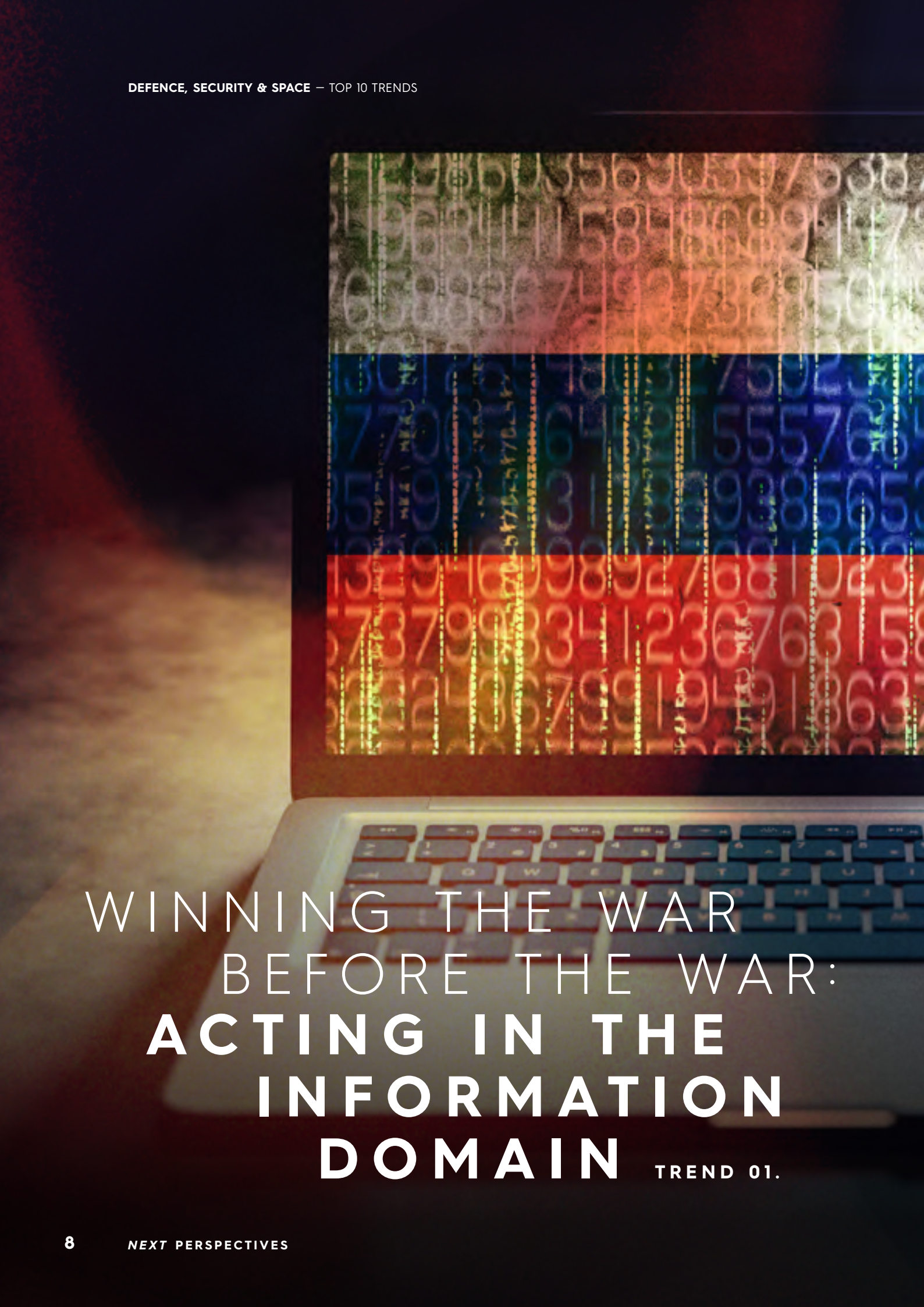
TREND 04.

Orchestrating multi-domain military action

— P. 20

Acting faster than the adversary

Building and regenerating for the long term



WINNING THE WAR BEFORE THE WAR: **ACTING IN THE INFORMATION DOMAIN**

TREND 01.

In contemporary conflicts, victory is not won solely on the physical battlefield. It is also decided in the cognitive domain and cyberspace, where the credibility of states, the reputation of armed forces and trust in alliances become strategic targets.

Digital technologies blur the boundaries between the physical and informational domains. Social media, platforms and algorithms are instruments of influence in their own right.

Information warfare aims to preserve strategic credibility and national cohesion over the long term. Its military component, cyber influence warfare, forms part of the cyber continuum alongside defensive cyber warfare and offensive cyber warfare. Led in France by the Cyber Defence Command (COMCYBER), it detects and neutralises attacks targeting forces in operations. Together, they contribute directly to sovereignty.

"Digital technologies blur the boundaries between the physical and informational domains."

Amplified by generative AI, digital campaigns produce strategic effects at marginal cost and under the guise of plausible deniability: deepfakes, micro-targeting and the mass dissemination of content saturate the media landscape. Hacking and the selective dissemination of data reinforce these dynamics, often supported by automated networks. Europe is thus facing persistent campaigns: nearly 20,000 cases of pro-Kremlin disinformation have been recorded.[5] The aim: to weaken our societies by creating multiple fractures. Yet, whilst armies win battles, it is nations that win wars.

The financial impact is also enormous. According to a groundbreaking study conducted by Sopra Steria, globally, the economic cost of disinformation is estimated at $417 billion, equivalent to 15% of France's GDP in 2024.[6]

In response to the industrialisation of information manipulation, Sopra Steria is developing an integrated end-to-end approach. Informed by its think tank on countering information

(5) EUvsDISINFO.

(6) Sopra Steria, *The Global Economic Impact of Disinformation.*

threats, the Cercle Pégase, the group brings together an industrial ecosystem at the heart of information dynamics.

This approach is brought to life through **SENSEE**, a platform designed to detect and manage information attacks. Supported by a network of French companies specialising in AI and data analysis — including Visibrain, Magic LEMP, OPSCI.AI, Label4.AI and others — it coordinates the collection, analysis and response to disinformation campaigns. Automated monitoring, detection of weak signals and coordination of actions enable attacks to be anticipated and characterised.

In addition, **Somulator**, a simulation tool developed with the Norwegian Defence Research Establishment and deployed by Sopra Steria, trains both military and civilian organisations to manage information crises by recreating realistic social media environments.[7] The solution has been used by the Norwegian Armed Forces since 2023 during exercises to simulate information environments in times of crisis.

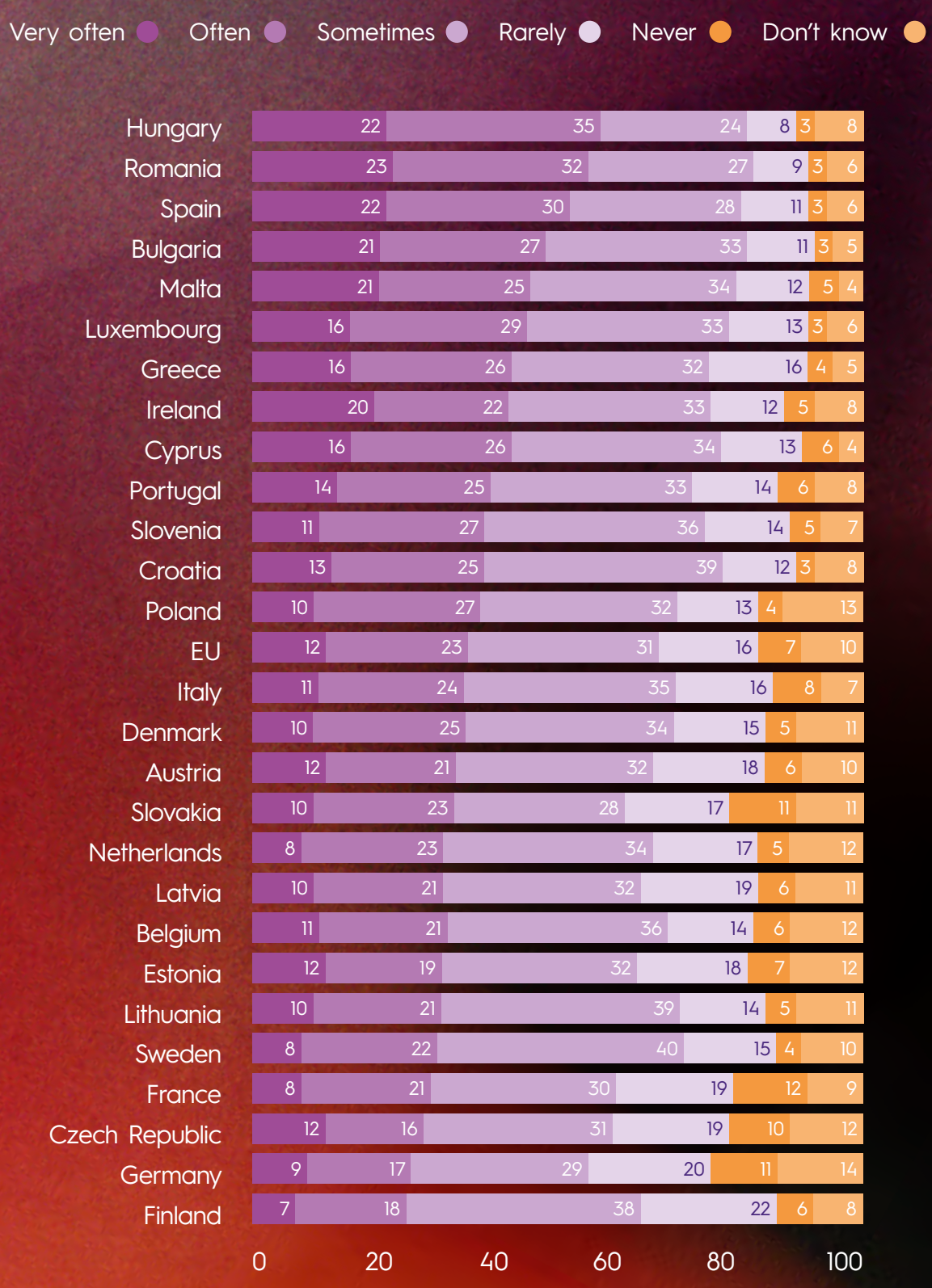
Finally, Sopra Steria offers an information monitoring service for targeted geographical areas: regular analyses, scenarios and strategic recommendations. The group thus provides dual expertise: technological and strategic. Familiarisation with the challenges of information warfare, cutting-edge tools, close client relationships and connections with recognised geographical experts are distinguishing factors highly valued by clients. Together, these elements safeguard legitimacy and operational effectiveness.

Information warfare is ongoing. It targets legitimacy first, before capabilities.

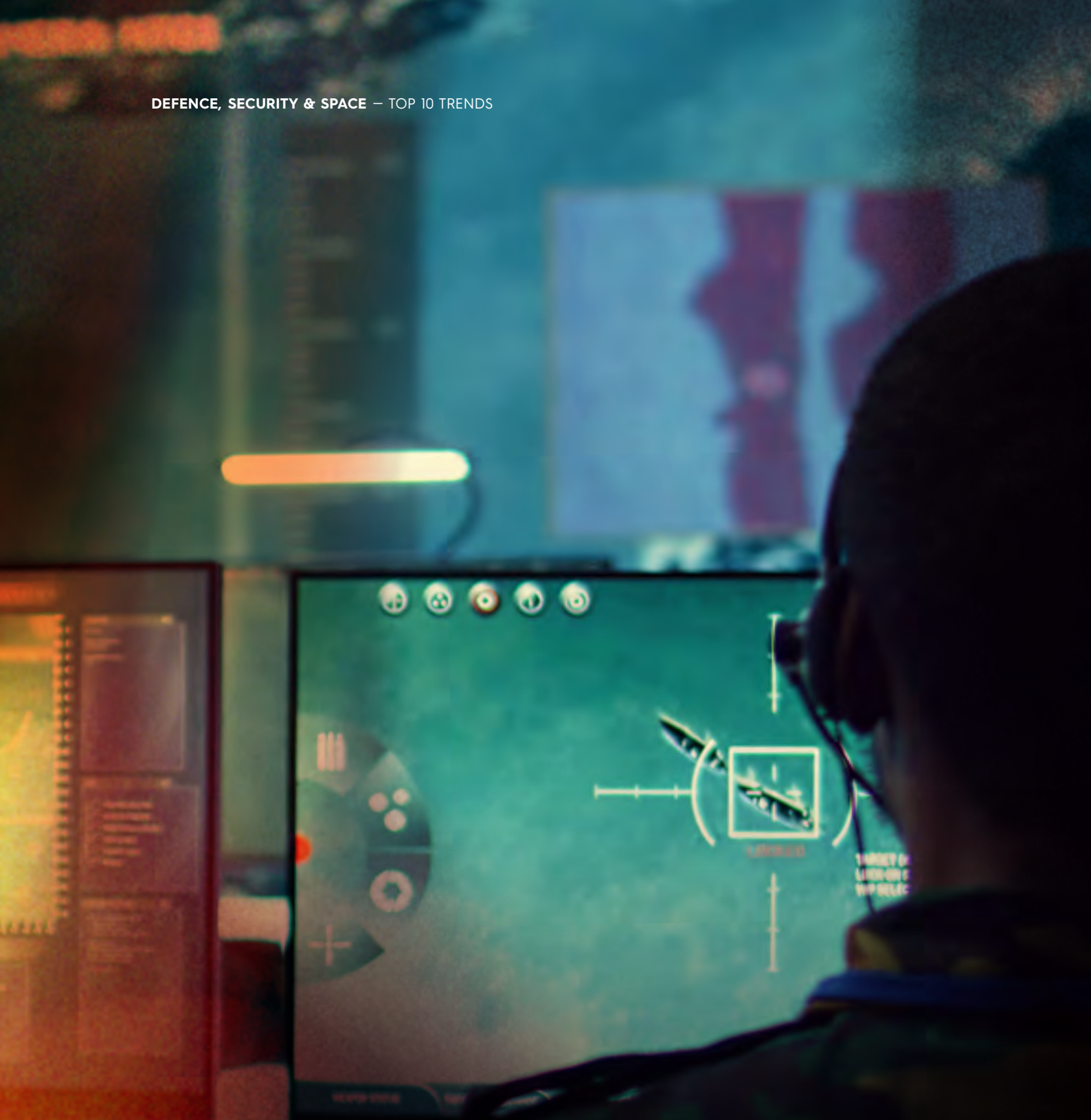
Detect earlier, understand faster, respond more precisely: information superiority is built over time. Sopra Steria supports defence and security stakeholders to strengthen this resilience and preserve their freedom of action.

(7) Somulator is used by the armed forces, the public sector (ministries, local councils), the education and research sectors, the healthcare sector and NATO.

PERCEIVED EXPOSURE TO DISINFORMATION (2025)



Source: Euronews, Eurobarometer survey on social media 2025 – Do you think you have been exposed to disinformation and fake news in the last 7 days?



STRENGTHENING AIR DEFENCE THROUGH **COUNTER-DRONE MEASURES**

TREND 02.

The ubiquity of drones at the heart of modern conflicts highlights the need to update the protection of our forces and critical sites. Europe's adversaries are adopting saturation and attrition tactics based on mixed platforms: drones, artillery, ballistic and cruise missiles, hypersonic projectiles, etc. This multiplicity of threat factors necessitates a multifaceted response.

The mass industrial production of drones and the overwhelming rate of mixed salvos are undermining the cost-effectiveness of air defence. A Russian Geran-2 drone, produced at a rate of over 5,000 units per month, costs €30,000,[8] nearly 20 times less than a dedicated air-to-air/surface-to-air missile such as the MICA[9] (MBDA), which costs €600,000 and has a low production rate.[10] Some drones are being upgraded to withstand jamming — wire-guided systems, multi-constellation support or embedded AI. Finally, "low-cost" interceptor missiles and modern anti-aircraft guns suffer from short ranges and require a very dense network.

The Ukrainian countermeasure is a system of interoperable systems: a massive deployment of low-cost drones and missiles (Sting, Octopus), combined with decentralised electronic warfare (EW) solutions and data fusion systems specialising in drone tracking, achieve an effectiveness rate of over 90% against Russian munitions. The Israeli defence system employs a similar combination, including its "Iron Dome" batteries and "Iron Beam" directed-energy weapon (DEW) systems.

Countering this threat requires integrating air defence with counter-drone (C-UAS) measures, by implementing several solutions: on the one hand, distributed sensors — radars, multispectral cameras, passive sensors — in each environment, and multi-sensor fusion within Command & Control (C2) systems capable of handling anti-swarm scenarios. Secondly, multi-layered and interoperable effectors — Aster missiles, low-cost anti-missile and counter-drone tools, EW systems targeting the communications and C2 systems of drone swarms capable of responding to saturation attacks.

(8) Meta-défense, September 2025.
(9) Missile for Interception, Combat and Self-defense.
(10) *L'Opinion,* March 2026.

"A pioneer in the fight against drones in France, the group has been developing BOREADES for over ten years and continues to invest and innovate to ensure its solution is constantly evolving and to stay ahead of the evolving drone threat."

The European Air Shield project, at the heart of the European Commission's Readiness Roadmap, is set to lead to the procurement of air defence systems through to 2030.

Sopra Steria responds with the **BOREADES** C2 system, a multi-sensor data fusion system specialised in C-UAS and multi-target tracking, and interoperable with any sensor or effector meeting the SAPIENT standard, or with any air defence systems (SAP, L16). BOREADES is ITAR-free, sensor-agnostic and can orchestrate the entire C-UAS chain (from detection to neutralisation), interfacing with various counter-drone or anti-missile effectors, including the Helma-P (CILAS) DEW system or interceptor drones.

BOREADES has been operational for over 10 years, is rapidly deployable thanks to short testing and scaling cycles, has proven its worth during the 2024 Paris Olympic Games — within programmes such as PARADE, MILAD and RADIANT — and can be mounted on ground platforms such as the Serval or Proteus.

Sopra Steria is also developing optronic systems to optimise drone detection in challenging environments (urban settings, adverse weather conditions, etc.).

Finally, to ensure effective protection against the drone threat, BOREADES is interoperable with air defence systems as well as sensitive site security and protection systems via its CRIMSON and STARLINX solutions. As a multi-domain C2 system utilising the latest digital twin, simulation, extended reality, and artificial intelligence technologies, CRIMSON facilitates information sharing, coordination, command, and decision support. STARLINX serves as a standalone or complementary multi-tactical data link C2 system for joint and combined operations.

INTEROPERABILITY OF THE BOREADES C2 SYSTEM

BOREADES C2 is an open system capable of interconnecting with existing systems via SAPIENT for sensors and effectors and via L16, SAP, etc. for air defence C2.

Source: Sopra Steria

PROVIDING EUROPE WITH A SPACE **DEFENCE CAPABILITY**

TREND 03.

Space has become a fully-fledged arena of conflict. The war in Ukraine provided an illustration of this from the very outset, with the Russian attack on the ground terminals of the KA-SAT satellite, aimed at disrupting military communications. Since then, the threats have diversified: jamming, blinding, cyberattacks, anti-satellite weapons and even offensive orbital capabilities.

These attacks go far beyond the military sphere and can directly affect economies. For example, nearly 20% of the UK's GDP is linked to satellite services, and a disruption to GPS would cost its economy around £1 billion a day.[11]

Within this context, the space sector is therefore undergoing rapid and profound change, marked by increasing militarisation and a refocus on defence and security issues.[12] Europe is thus demonstrating its commitment to strategic autonomy by developing its own observation, positioning and secure communications services, no longer relying on non-European systems.

Regarding communications, Europe is investing around €200 million in the initial studies for IRIS², whilst Germany is simultaneously accelerating its SATCOM Bw project, backed by a massive investment of €8 billion to €10 billion.

The European Resilience from Space (ERS) programme, led by ESA, is part of this ambition. With a budget of around €1.2 billion, it aims to pool national capabilities and coordinate dual-use systems. Its operational launch is planned for around 2028, which aligns with the European Union's next Multiannual Financial Framework (MFF)[13] and demonstrates that ERS forms part of a medium-term vision for European space sovereignty.

However, having space capabilities is not enough if they are not protected. Faced with adversaries capable of jamming or offensive actions in space, securing assets becomes essential. The European Space Shield project thus aims, by 2030 and as a direct continuation of the ERS, to provide Member States with a service to

(11) UK Ministry of Defence, *Strategic Defence Review 2025*.
(12) European Space Agency, *Report on the Space Economy 2025*.
(13) Multiannual Financial Framework (2028-2034).

protect space assets and services. It will, here too, draw on the EU's dual-use space capabilities and promote the development of interoperable national defence capabilities, particularly around Galileo and space surveillance.

In this context, Space Situational Awareness (SSA) is becoming a key issue. The increasing number of satellites and the development of constellations heighten the risk of collision and complicate the management of space traffic.

"Space Situational Awareness (SSA) is becoming a central issue."

In response to these challenges, Sopra Steria is taking action at various levels:

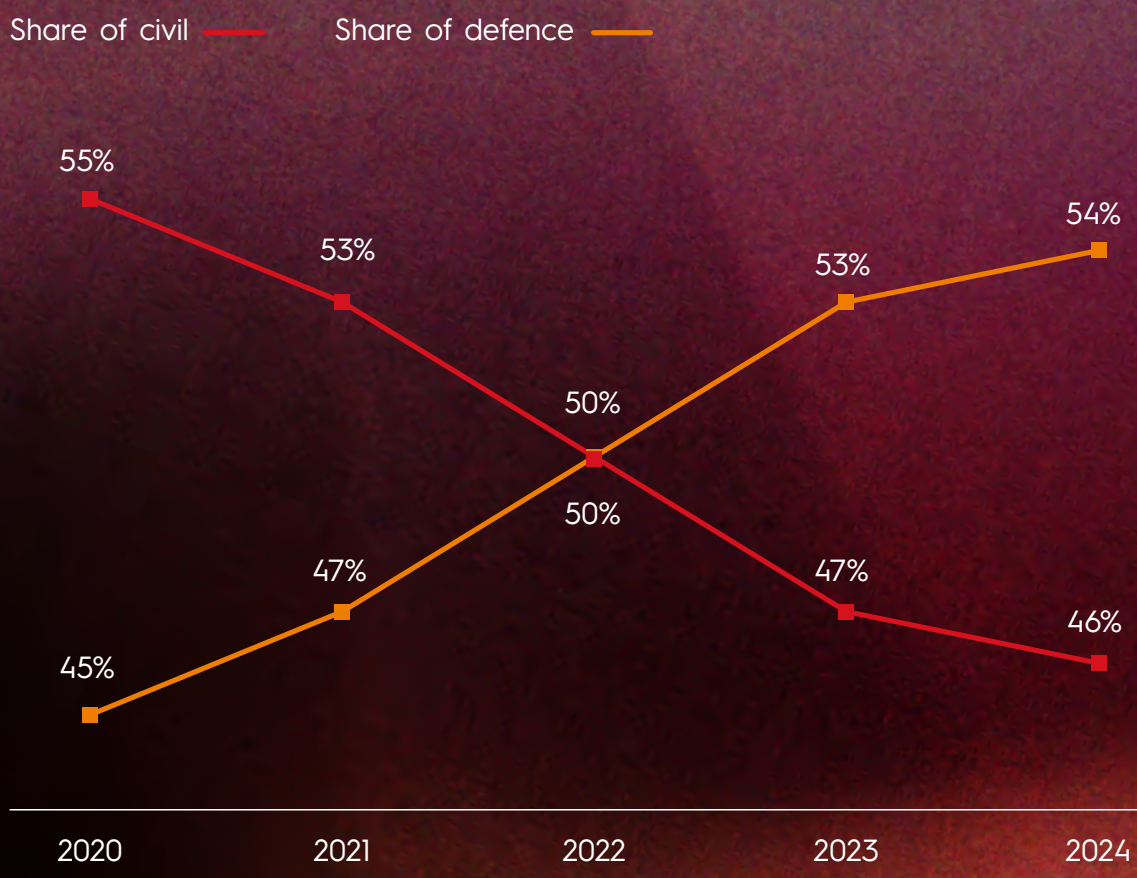
↘ **By developing the concept of a virtual constellation based on the GOSMIC ground segment product line.** A virtual constellation is not a single physical satellite system, but a coordinated set of missions and sensors operated independently by different countries and organisations. The aim is to improve the availability and accessibility of data by drawing on multiple satellite missions operated by various space agencies and companies.

↘ **By designing and operating, on behalf of CNES,**[14] the new French Space Traffic Evaluation and Management System **(STREAMS)**, which is based on a national catalogue of space objects, a permanent collision risk detection and management service, and an agile platform enabling the rapid integration of innovations from the surveillance ecosystem.

(14) French space agency.

CIVIL AND DEFENCE SPACE BUDGETS

Trend in the distribution of civil and defence space budgets worldwide (2020–2024)



Source: European Space Agency

ORCHESTRATING MULTI-DOMAIN MILITARY ACTION

TREND 04.

The return of symmetric conflicts relying on multi-domain operations (MDO) is a game-changer. In addition to the five main fields of confrontation (land, sea, air, cyber, space), cross-cutting domains (electromagnetic, informational) and shared spaces (very-high altitude, the seabed) are now contested. MDOs simultaneously mobilise capabilities (sensors and effectors) across several of these domains to achieve a military effect. They rely on fast-evolving communication systems for data exchange, accelerating the operational tempo and shortening the decision-making cycle. The aim is to maintain operational superiority, which requires not only controlling the flow of data but also ensuring the synchronisation of effects within an ever-shorter timeframe.

Several digital innovations contribute to the implementation of MDO by armed forces: advanced AI automates the gather-process-distribute cycle for multi-source, multi-format tactical data; the use of satellite constellations accelerates and ensures the reliability of data access and transmission; the implementation of combat clouds allows for mature collaborative combat platforms; weapon systems across all domains are now interoperable. These innovations help reduce the cognitive load associated with the mass processing of tactical information within a short timeframe, which is essential to the success of MDO operations.

The results are evident on the ground in both Ukraine and Iran: ultra-short kill chains (identification by drones, artillery fire, battle damage assessment and retasking within minutes), tactical manoeuvres conducted through the integration of multi-domain assets (ISR[15] from commercial satellites, jamming, strikes by kamikaze drones), etc. The decentralisation of assets and capabilities (tactical jammers, micro-drones, etc.) streamlines the decision-making chain and enables very short OODA loops.[16]

(15) Intelligence, Surveillance, Reconnaissance.
(16) Observe-Orient-Decide-Act.

This new agility especially depends on the ability of forces to access data at the tactical level. Because of this, it is essential to ensure the security and control of digital infrastructure (data centres, submarine cables) which are now considered prime targets, as demonstrated by Iranian strikes on AWS sites in early 2026.

These operations are thus limited by the reliability of data access and management. The destruction of service infrastructure, jamming actions or cyberattacks can weaken the operational transmission chain and force a return to suboptimal procedures — in this case, the excessive cognitive load on the operator may jeopardise the implementation of MDO.

In this context, interoperable command and control (C2) systems, orchestrating multiple dual-data sensors, are essential.

To coordinate joint and allied operations, Sopra Steria is working alongside the armed forces with the **CENTERIS** solution, a highly modular and adaptive hypervision system compatible with NATO standards (L16), capable of integrating business applications and third-party innovations, including those for 2D planning and ground logistics (Sopsight.ai solutions[17]). CENTERIS is based on the CRIMSON Defence solution, delivering tactical situational awareness and digital twin capabilities for the theatre of operations, as well as ISR, robotic systems management, and AI-driven command support. Built on an architecture incorporating data-centric security, CENTERIS introduces a fresh, data-centric approach to multi-domain operational command, combining military assets and dual-use infrastructure.

"The destruction of service infrastructure, jamming actions or cyberattacks can weaken the operational transmission chain."

(17) Multimodal, explainable and sovereign AI solutions, contributing to multi-domain operational superiority.


SECRET_OPERATION
OPERATION_STATISTIC
sub procedure
sendBit(dim b as
boolean)
if (b) then
gpio.2 = 1
delay_us(1125)
gpio.2 = 0
delay_us(375)
else
gpio.2 = 1
delay_us(37
end if
end sub
SECRET_INFORMATION

BUILDING SOVEREIGN, SECURE AND **TRUSTWORTHY DEFENCE AI**

TREND 05.

The rise of artificial intelligence is transforming conventional warfare and reinforcing hybrid strategies — which combine military, cyber and information operations, amongst other actions. AI is becoming a strategic lever, but also a source of instability. Whilst the United States and China are investing heavily in advanced defence technologies, Europe must remain competitive and invest in the development of reliable, robust and sovereign artificial intelligence solutions for its defence capabilities.

Investments are materialising. Government agencies dedicated to defence AI are being created: the DAIC[18] in the UK and the AMIAD[19] in France, with announced funding of €2 billion by 2030.[20] Major industrial players are supporting start-ups in the sector — Saab with Helsing (over €1.5 billion raised), Dassault Aviation with Harmattan AI (around €200 million raised). At the same time, industrial cooperation is intensifying to design AI solutions tailored to critical systems across all sectors. For example, Dassault Aviation and Naval Group are collaborating with Thales within the cortAIx accelerator, which designs AI tools for the detection, classification and identification of threats.

Decision support for command, assistance with targeting and strike execution, and the protection of critical infrastructure: defence AI is finding ever-increasing applications. Thanks to its ability to process data rapidly and on a massive scale, AI is becoming a genuine game-changer for operational performance. However, deploying artificial intelligence in the military sector presents numerous challenges. Standards for reliability, security and transparency are particularly high. The solutions developed must operate in strategic command centres, at the operational edge on field sites, and at the far edge for embedded systems.

Enhancing the explainability and transparency of AI systems requires standardising model evaluation metrics and integrating explainability components throughout the design chain. Security and sovereignty

(18) Defence Artificial Intelligence Centre.
(19) Ministerial Agency for Defence Artificial Intelligence.
(20) French Ministry of Armed Forces and Veterans, March 2024.

demand a closed environment: design and deployment must rely on dedicated infrastructure. The integration of embedded AI requires a reduction in computational complexity and optimisation of the training phases to design smaller models. The speed at which models can be retrained to cope with enemy adaptations is also key — whilst ensuring that their acquired performance does not regress. Finally, to ensure trustworthy AI in defence, the AI must make recommendations, whilst humans retain full responsibility for actions.

Sopra Steria is committed to addressing these challenges through its involvement in trusted AI ecosystems, such as ANITI and the ETA[21] — of which Sopra Steria is a founding member alongside IRT SystemX and Thales. Sopra Steria offers a **sovereign and trusted AI infrastructure,** combining the **InnerData** MLOps platform for the industrialisation of the entire AI project lifecycle with the **IAKa** solution, dedicated to generative and agent-based AI and designed for critical environments.

"The speed at which models can be retrained to cope with enemy adaptations is also key."

As a solutions architect for multiple use cases, Sopra Steria has expertise in the industrialisation and trust chain for autonomous digital AI solutions and solutions integrated into weapon systems. At European level, the design of shared AI models requires data-sharing infrastructures between allies. Sopra Steria is actively contributing to the development of a European data space for defence.

(21) European Trustworthy AI Association.

ETA – EUROPEAN TRUSTWORTHY AI ASSOCIATION

Industrialising and disseminating the methodology and components of trustworthy AI:
- Maturing key components for robustness, data and traceability;
- Supporting organisations in their AI transformation.

Sopra Steria is both a founder and technology provider of the ETA, supporting its members in our key areas of expertise:
- Platforms;
- Technical maturation.

LEVEL OF ADOPTION

LEAD							
Air Liquide	IRT SystemX	Naval Group	Safran	Sopra Steria	Thales		
USE							
Airbus	CEA-List	CRIM	DFKI	EDF	IRT Saint Exupéry	LNE	MBDA
Numalis	Omundu	Octopize	RAI UK	Safenai	Simula / VIAS	TNO	University of Southampton
ENGAGE							
Bureau Veritas	Eodyn	EyeSnap	KNDS	LGM	MO Avocat	National Technology	

Source: European Trustworthy AI Association.

SHARING AND UTILISING **DATA IN OPERATIONS**

TREND 06.

The strengthening of multi-domain and inter-allied operations, as well as the acceleration of decision-making through artificial intelligence and advanced data analytics techniques, rely on the seamless integration of networks, platforms, weapon systems, sensors and data. Cloud and connectivity must therefore be fully integrated into defence platforms and systems in order to harness the full technological potential in the pursuit of operational superiority.

To ensure secure information sharing on the battlefield and between allies, European states must safeguard sovereignty over data management and storage. States will thus preserve their capacity to analyse, understand and protect critical data. Several initiatives are emerging: since July 2025, 12 NATO countries[22] have been participating in the Allied Software for Cloud and Edge Services (ACE) programme, aimed at accelerating and facilitating the sharing and storage of classified information across all operational environments.

At the same time, the European Defence Agency (EDA) is laying the foundations for a European data-sharing space (DAIDS project[23]). Both schemes are expected to be operational by 2030.

The development of a sovereign military cloud will help reduce vulnerabilities and potential dependence on non-European solutions. A European defence data space based on a federated and decentralised architecture — and complying with NATO standards — where each piece of data remains under the control of its owner, makes cross-border data sharing possible whilst preserving everyone's sovereignty. Beyond storage, data qualification will be key, particularly for effectively feeding AI models. AI could, moreover, itself be used for data quality assurance.

(22) Belgium, Canada, Germany, Denmark, Spain, the United States, Finland, France, Greece, Italy, Luxembourg, Norway, the Netherlands, Romania, the United Kingdom and Sweden — and Allied Command Operations.

(23) Defence Artificial Intelligence Data Space.

According to ENISA's 2025 report,[24] digital infrastructure and services are the main target of cybercrime in Europe, accounting for 13.7% of recorded incidents. More specifically, 27.7% of data breach incidents affect digital infrastructure and services. Ensuring the security of defence data in storage and sharing environments will therefore be key. Beyond the protection of networks and infrastructure, security is now refocusing on the data itself, thanks to the so-called "data-centric security" approach. Each piece of data is protected individually, notably through encryption, strict access control (multi-factor authentication, application of the principle of least privilege), traceability of actions (logging), and robust backup and replication mechanisms.

Sopra Steria is introducing the principles of **data-centric security** as part of the **European Defence Data Space** project led by the European Defence Agency (EDA) in collaboration with the French Alternatives Energies and Atomic Energy Commission (CEA) and Cloud Data Engine. Drawing on its unique position as both a sovereign digital player and a defence contractor,

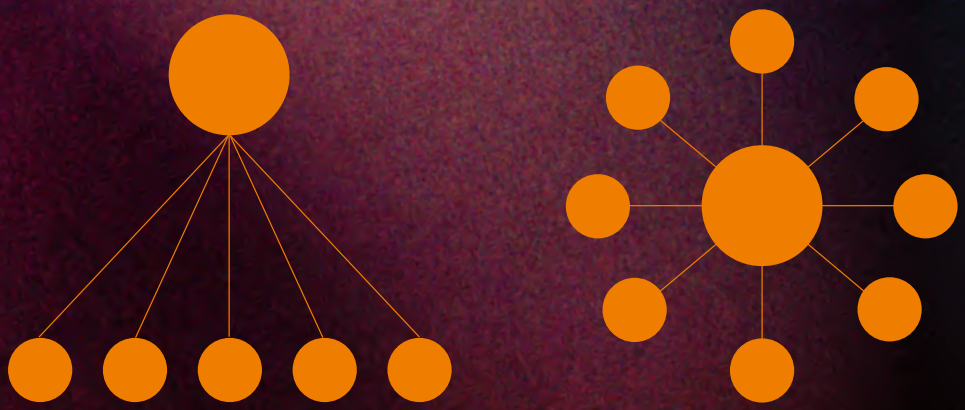
"Digital infrastructure and services are the primary targets of cybercrime in Europe, accounting for 13.7% of reported incidents."

Sopra Steria is applying civilian best practices to the military sector. Its expertise in designing data spaces is underpinned by its involvement in the Data4NuclearX (nuclear) and Decade-X (aerospace) projects and its role as leader of the InfrateX consortium.[25] Finally, Sopra Steria plays a central role in the development of the **Secure Cloud** in Europe. For example, the group is one of the first European integrators of OVHcloud's On-Prem Cloud Platform (OPCP): a European solution enabling the deployment of a complete, secure and sovereign cloud infrastructure directly on-site, including in isolated (air-gapped) environments.

(24) European Union Agency for Cybersecurity, Threat Landscape 2025.

(25) The InfrateX consortium is responsible for implementing the Simpl programme for the European Commission's DG Connect.

DATA EXCHANGE: TRADITIONAL PLATFORMS VS. DATA SPACES



TRADITIONAL DATA PLATFORMS

- Centralised operations
- Platform owner defines commercial and technical frameworks
- Platform-managed transactions
- Data is (often) used by suppliers for commercial purposes

DATA SPACES

- Distributed system
- Shared governance framework per data space
- Participants' autonomy
- Traceable and transparent transactions between participants
- Data usage control specific to data space but based on common vocabularies
- Interoperability between data spaces

Source: Gaia-X Hub France.

MOVING FROM EXPLORATION TO ACTION WITH QUANTUM

TREND 07.

A disruptive technology, quantum computing opens up the prospect of almost instantaneous battlefield awareness: GPS-free navigation, detection with unprecedented precision, accelerated simulation and advanced communications security. Does this spell the end of the "fog of war" described by Carl von Clausewitz? Or merely its displacement, given that war remains subject to friction — human error, complexity, chance, adversity? The debate remains open.

The European Armament Technological Roadmap[26] identifies AI and quantum computing as strategic priorities: mastering them is key to European autonomy. But this revolution is double-edged. Future quantum computers could undermine current encryption systems and fuel the "harvest now, decrypt later" approach. The challenge is clear: to protect communications, strengthen resilience and preserve operational credibility.

Global competition is intensifying. The United States and China are investing heavily, whilst Europe seeks to preserve its sovereignty. Technologies are advancing rapidly: superconducting qubits, trapped ions, photons. Hybrid approaches are emerging, combining classical and quantum computing. This dual nature is accelerating the pace of development, with civilian applications indirectly supporting military capabilities. France, for its part, *"is well in the race."*[27] *"Quantum computing must be viewed not as a theoretical subject but as a strategic, concrete and now fully operational one."*[28] France is thus tripling its investment by adding €200 million to the €120 million allocated for the period 2024–2030.

Quantum technology rests on three pillars: computing, sensors and networks. Computing opens up new possibilities in cryptanalysis, simulation and optimisation. Sensors — gravimeters, atomic clocks, GPS-free navigation — promise major gains. The quantum magnetometer

(26) European Commission, White Paper on European Defence – Readiness 2030.
(27) General Engineer for Armaments Patrick Aufort, Director of the Defence Innovation Agency, April 2026.
(28) Catherine Vautrin, Minister for the Armed Forces, April 2026.

could transform submarine detection by revealing variations in the magnetic field, calling into question the invisibility of deterrent assets. Quantum networks secure communications via key distribution.

Sopra Steria is integrating quantum technology into an operational framework by testing concrete use cases for defence, in collaboration with a network of leading partners, including Quandela, Pasqal, and Cryptonext, via the Quantonation fund. Two key areas are emerging: the resilience of critical networks against attacks or failures, and logistical optimisation in complex environments.

In the space sector, the QC4GEO project is exploring the contribution of quantum computing to the classification of satellite imagery, with the dual objectives of accuracy and speed. In simulation, work on the Lattice Boltzmann model is paving the way for enhanced performance. At the same time, quantum neural networks are being developed to process massive volumes of data.

"Does this spell the end of the 'fog of war' described by Carl von Clausewitz?"

Finally, cybersecurity is at the heart of the challenges. Sopra Steria is integrating post-quantum cryptography into its **Datasphere** solution to anticipate the obsolescence of current standards and ensure the long-term protection of sensitive data. This solution complies with ANSSI's recommendations regarding the transition to post-quantum hybrid encryption schemes and is interoperable with international security standards (NATO, NIST).

Quantum technology is no longer a distant prospect. It is becoming a practical tool.

Anticipate, test, integrate.

Being ready in time will make all the difference — Sopra Steria supports you in this transition.

A RAPIDLY GROWING MARKET

The market for defence quantum technologies remains emerging but is growing rapidly.

$10
BILLION BY 2030–2035

Depending on the scope of the analysis, it is currently valued at between $1 billion and $3 billion, with projections ranging from $3 billion to over $10 billion by 2030–2035,[29] representing annual growth rates of between 15% and 25%.[30]

At the same time, public investment is taking shape on a large scale: over €1.8 billion in France,[31] £2.5 billion in the UK[32] and several hundred million euros in Germany, with a growing proportion dedicated to defence and security applications.

€1.8
BILLION IN FRANCE

(29) Custom Market Insights, Quantum Warfare Market 2025–2034; Fortune Business Insights, Quantum Warfare Market 2026–2034.

(30) Insight Monk, Quantum Warfare Market 2024-2035.

(31) *LaREF*, March 2025.

(32) *JDN*, June 2025.

RESTORING **STRATEGIC DEPTH**

TREND 08.

The return of high-intensity wars and attrition conflicts, which mobilise vast numbers of personnel and resources, is redefining strategic requirements. Beyond technical superiority, logistical depth and mass are becoming decisive factors. The European Commission's Readiness 2030 plan estimates capability requirements at €800 billion.[33] European states are called upon not only to modernise their armed forces, but also to strengthen their resilience and their ability to sustain the effort over the long term. The time has come for massive rearmament.

In France, the 2024–2030 Military Programming Law allocates €413 billion to the armed forces,[34] a budget likely to be revised upwards. Germany, for its part, is planning expenditure of over €100 billion in 2026 alone.[35] Whilst the budgetary effort is very real, the persistent reliance on non-European defence equipment and the question of industrial capacity to scale up remain. Ensuring strategic autonomy requires strengthening the competitiveness and responsiveness of the defence industrial and technological base.

The objective is unequivocal: it involves producing both increasingly complex systems and simpler ones in large quantities, within tight deadlines, whilst maintaining high standards of quality and performance. This shift is already underway. KNDS, for example, has tripled its monthly production of CAESAR guns, rising from two units before the conflict in Ukraine to six in 2024.[36] At the same time, new entrants are demonstrating their capacity for innovation and industrial acceleration: Harmattan AI, founded in 2024, aims to produce 10,000 drones per month as early as this year,[37] whilst Exail Technologies has become the European leader in underwater demining drones within four years.

(33) European Commission.
(34) Ministry of the Armed Forces (France).
(35) *La Tribune,* January 2026.
(36) *Capital,* March 2025.
(37) *L'Usine Digitale,* January 2026.

Innovate fast, test fast, deploy fast. To move from long cycles and small batches to a lean inventory economy, factories and processes must transform. Shorter design cycles require the modernisation of information systems, incorporating collaborative tools, modelling, simulation, etc. Production ramp-up will depend in part on the adoption of new technologies, particularly artificial intelligence. Summaries of complex assembly instructions, detection and management of non-conformities, technical support: the use cases are numerous.

Strengthening digital continuity between different business functions (engineering, production, support) and within the extended enterprise, including subsidiaries and suppliers, is essential. Producing more, and faster, requires not only securing supply chains, but also providing subcontractors with the financial and technological resources needed to support the ramp-up.

With the **BluejaySecureCollaboration** platform, Sopra Steria ensures secure collaboration between defence stakeholders, thereby helping to accelerate the delivery of critical programmes. Sopra Steria is also participating in the data space project led by the European Defence Agency alongside the CEA[38] and Cloud Data Engine.

With **Connectiv-IT's** software suites, Sopra Steria addresses the challenges of digitalising the sector's supply chain and MRO services. Its **SCR²M**[39] solution enables manufacturers to identify and quantify the financial impact of supply chain disruptions, thereby allowing them to take proactive measures to avoid delays or contractual penalties.

(38) French Alternative Energies and Atomic Energy Commission.
(39) Supply Chain Risk and Resilience Management.

"Beyond technical superiority, logistical depth and mass are becoming decisive factors."

INTEGRATING DRONES INTO COMBAT AT SCALE

TREND 09.

Mere ISR tools until the late 2010s, drones now see transformative use in contemporary theatres of operations across all domains: land, sea and air. Whilst the heavy MALE drone was predominant until the conflict in Ukraine, the economies of scale enabled by smaller systems make them ubiquitous: repurposed civilian models, loitering munitions, swarm drones, etc.

Advances in embedded AI, ultra-low latency enabled by 5G and satellite deployments, and falling costs of radar, multispectral and LiDAR sensors are driving rapid growth in the UxV[40] sector. Less expensive than conventional defence tools, small models such as the Iranian Shahed-136, meeting widespread adoption, have an expanding range of uses: patrol, decoy, strike, close air support, etc. The use of ISR data transmitted by aerial drones to guide surface drone strikes against Russian targets in the Black Sea demonstrates the paradigm shift brought about by the combined use of multi-domain drones and the deployment of swarm tactics to overwhelm defences. Consequently, in Ukraine, drones are responsible for 70 to 80 per cent of casualties on the front line.[41]

Public authorities are shifting their focus to incorporate these capabilities: France's 2024–2030 Military Programming Law allocates €5 billion to the procurement of drones and the development of swarm flight capabilities by 2030.[42] London has announced a €4.6 billion investment to equip its forces with autonomous systems,[43] and the European Commission's Readiness Roadmap 2030 prioritises investment in precision strike capabilities using drones by 2027. The private sector is not to be outdone: Helsing and Stark Defence have each secured €1 billion to equip the Bundeswehr with kamikaze drones,[44] Harmattan.AI has raised €171 million to scale up its drone production,[45] and Arquus and Renault have joined forces to design ground-based drones.

(40) Unmanned Extended Vehicles (air, maritime and land drones).
(41) US Army War College.
(42) French Ministry of Armed Forces and Veterans.
(43) British Government.
(44) *Les Echos,* February 2026.
(45) *L'Usine Digitale*, January 2026.

Addressing this challenge requires the deployment of robust architectures for data fusion and centralised management of multiple semi-autonomous platforms. Ensuring reliable connectivity in all environments, and allowing the use of tools for networking and fine-grained management of large numbers of drones, are essential to maintaining the superiority of our forces. Strong system interoperability is required to facilitate this implementation and integrate new models: the freedom to purchase and use drones of any make depends on the standardisation of user interfaces. In addition, the widespread use of UxVs in long-duration operations requires the integration of power supply into operational logistics, and the implementation of detailed energy management systems at the tactical level.

Sopra Steria meets these needs. Its experience in supporting the armed forces positions it as a European leader in data fusion and the integration of AI into autonomous systems for vision, navigation and

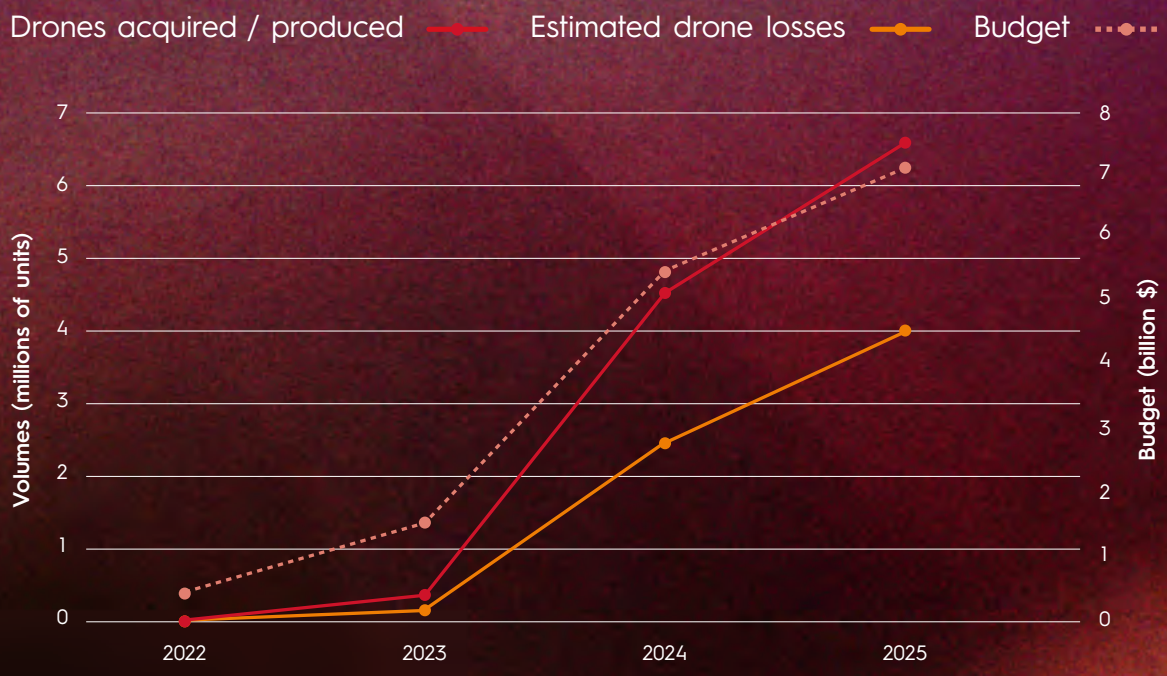
"The European Commission's Readiness Roadmap 2030 prioritises investment in precision strike capabilities using drones by 2027."

the coordination of multiple vehicles and multi-environment tactical groups. Sopra Steria ensures the integration of UxVs through its multi-domain, interoperable **CENTERIS** system, based on a secure, open, data-centric architecture (DCS), of which the CRIMSON solution is a key component. Furthermore, CS Group has been selected by AMIAD[46] for the **PENDRAGON** project to provide components of its CRIMSON C2 system for integration into the PENDRAGON C2. This builds on the company's involvement in dual-use robotics initiatives, such as the **CARMA** project aimed at developing crisis response and management robots. Finally, Sopra Steria is working alongside European research organisations and industrial partners on the **SENTINEL** project to optimise energy resources in military camps.

(46) French Ministerial Agency for Defence Artificial Intelligence.

TREND IN DRONE PURCHASES, USAGE AND LOSSES IN UKRAINE FROM 2022 TO 2025

Since 2022, drones have become consumable munitions, which fundamentally reshapes the military economy of its user. Ukraine's monthly drone losses now exceed the annual production of most Western countries, and the cost associated with these losses is negligible compared to the damage inflicted on the adversary.



Source: Sopra Steria, based on data from IHEDN, the US Army War College, the Royal United Services Institute and the press.

STRUCTURING NEW DEFENCE **INNOVATION MODELS**

TREND 10.

The war in Ukraine has profoundly transformed the way military innovation is conceived in Europe. It has highlighted the limitations of an arms procurement model designed for long development cycles, sometimes spanning 20 years. Feedback from this conflict shows that operational superiority now depends on the ability to continuously adapt equipment to the realities on the ground, sometimes within a matter of weeks. Ukrainian forces are constantly modifying their systems in response to enemy countermeasures.

This dynamic requires the armed forces and industry to rethink their development cycles: it is no longer simply a matter of designing major platforms over the long term, but of having an industrial capacity capable of continuously integrating feedback from the battlefield and iterating rapidly. However, major defence groups have built their model around complex, lengthy, highly planned programmes requiring colossal investments.

Whilst this organisational structure remains essential for certain major systems, it appears less suited to rapidly evolving technologies, particularly in the fields of software, artificial intelligence, autonomy and electronic warfare. It is in this space that new entrants are making their mark. Start-ups, dual-use companies and digital players are introducing short cycles, rapid prototyping and a culture of continuous improvement directly inspired by the tech sector. Organisations such as the French Defence Innovation Agency or the Innovation Board of Belgian Defence illustrate this drive to accelerate and structure this ecosystem within the armed forces.

This industrial transformation is accompanied by a profound shift in funding models. Long dominated by public procurement and major state programmes, the defence sector is now attracting new investors. Venture capital funds are showing increasing interest in so-called "dual-use" technologies, i.e. those likely to have both civilian and military applications: artificial intelligence, space, cybersecurity, robotics and communications infrastructure.

A new financial ecosystem is gradually taking shape around established manufacturers and national budgets, bringing together private investors, specialised funds, European schemes,[47] and sometimes sovereign wealth funds. This trend reflects a broader shift: security and technological sovereignty are becoming strategic priorities for both states and investors.

At the intersection of these dynamics, a new landscape for European military innovation is taking shape. Major armaments programmes will continue to shape military power over the long term, but they will now have to coexist with much shorter innovation cycles. The challenge for European nations will be to successfully reconcile these two timeframes: preserving heavy industrial capabilities whilst enabling the emergence of an agile ecosystem capable of rapidly transforming technological innovations into operational capabilities.

Sopra Steria structures defence innovation through its open innovation initiatives, connecting start-ups, manufacturers and public sector bodies to accelerate the identification and integration of dual-use technologies. Its expertise in digital transformation enables a rapid transition from prototype to operational deployment in complex and sovereign environments. Furthermore, its venture capital initiatives strengthen its ability to identify, fund and support strategic technologies.

(47) *La Tribune,* March 2026.

CONCLUSION

Taking action to preserve our freedom of action and guarantee our strategic autonomy

A lasting strategic shift
Conflict is becoming a long-term reality. All the conflicts unfolding before our eyes prove this. Hybrid, multi-domain and ongoing, they target not only capabilities but also the adversary's cohesion, decision-making and resolve. Mastery of key technologies and industrial resilience are therefore becoming the foundations of power.

Ten trends, one common challenge: freedom of action
Artificial intelligence, quantum computing, cyber, information and influence warfare, space, autonomous systems, integrated defence, data sovereignty, industrial rearmament. These dynamics are not isolated: they converge towards a single objective — maintaining the initiative and superiority in all domains.

Three inseparable levers:

↘ **Monitoring and processing information overload:** maintaining situational awareness across all domains, from space to cyberspace and information networks, through SSA, C2 architectures and data fusion;

↘ **Acting faster than the adversary:** using simulation to anticipate and strengthen positions by modelling engagements, comparing friendly and adversarial courses of action, identifying points of failure and testing the resilience of systems. Simulation is becoming a key tool for training, decision-making and preparing for operations before they take place. Fully exploiting artificial intelligence, data spaces and, in the future, quantum technologies to speed up decision-making and retain the initiative;

↘ **Build and regenerate over the long term:** reindustrialise, produce at scale, shorten innovation cycles and rebuild industrial and logistical depth suited to high-intensity conflicts.

It is indeed the combination of these three levers that determines military effectiveness and strategic credibility.

Furthermore, the issue of European sovereignty and strategic autonomy as an operational imperative is of paramount importance. Technological dependencies, fragile supply chains, information pressure: every vulnerability can be exploited. Strategic autonomy is no longer a distant goal; it is an immediate requirement, and every sovereign decision shapes it.

In this tense context, with its uncertain developments, Sopra Steria is a partner at the heart of European information, technological and operational superiority:

- **An independent European leader,** committed to serving the armed forces, security and the space sector;
- **A new breed of defence contractor, a hybrid player** — both an industry player and an IT services provider — within the European Defence, Space and Security Industrial and Technological Base, which designs solutions, integrates systems with its partners and connects data, platforms and stakeholders at the heart of interoperability.
- **A catalyst for operational transformation,** at the intersection of C2, AI, cybersecurity, sovereign cloud and autonomous systems;
- **An architect of resilience,** helping to secure critical infrastructure, protect information and ensure business continuity;
- **A trusted partner,** rooted in national and European ecosystems, serving strategic autonomy, capable of fostering, structuring and accelerating innovative players.

But we must act now:

↘ **Anticipate rather than react:** identify technological disruptions and their operational impacts today.

↘ **Accelerate transformation at the heart of interoperability:** modernise systems, integrate AI, secure architectures and prepare for the post-quantum era.

↘ **Strengthen resilience:** protect data, infrastructure and critical chains.

↘ **Build sovereign capabilities:** reduce dependencies and master key technologies.

"With Sopra Steria, turn European strategic ambitions into operational capabilities. In an environment of ongoing competition, the advantage is being built right now."

DESIGN: Angie PHOTO CREDITS: © GETTY IMAGES.


The world is how we shape it
sopra steria