sopra steria

BEHIND EVERY SOVEREIGN DECISION

DÉFENSE, SÉCURITÉ & SPATIAL

Cahier de tendances

NEXT PERSPECTIVES

Ce cahier de tendances a été réalisé en partenariat avec CS Group et 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

Notre équipe et nos experts Défense, Sécurité et Spatial

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

Équipe éditoriale

Alain DURAND, Marine CASSOU, Boris LAURENT, Charles MARTY

Contributeurs internes

Général d'armée (2S) Manuel ALVAREZ, Général de division (2S) Bruno COURTOIS, Contre-amiral (2S) Christophe EUGÈNE, Général de division (2S) Jean-Jacques PELLERIN, Frode LILLEDAHL, Louise MONJO, Charles PRAUD, François GRIME, Oana Alina SUCIU, Philippe SERAFIN, Florian MEHATS, Josepha RASAMUEL, Julien MONTROZIER

INTRO DUCTION

Le retour brutal de la puissance

L'Histoire s'est rappelée à nous. Pendant trois décennies, l'Europe a cru évoluer dans un environnement stabilisé, régi par le droit et des alliances solides, et porté par l'illusion d'une mondialisation pacifiée. Cette parenthèse se referme brutalement. Le monde redevient conflictuel, fragmenté, imprévisible. La guerre n'est plus un horizon lointain : elle redevient une constante.
Nous assistons à un basculement d'époque, mais le vieil adage de Végèce « *Si vis pacem, para bellum*[1] » (« Si tu veux la paix, prépare la guerre ») est toujours d'actualité, tout comme la pensée de Thucydide, qui avait déjà compris qu'« *il est dans la nature de l'homme d'opprimer ceux qui cèdent et de respecter ceux qui résistent*[2] ».

Si la guerre ne change pas de nature, elle se caractérise désormais par un nouveau modèle de supériorité stratégique reposant sur une quadruple saturation. Saturation de l'espace avec la multiplication des constellations, saturation cognitive sous l'effet des campagnes de désinformation et des deepfakes, saturation du champ de bataille avec la prolifération des drones, saturation, enfin, des données, issues d'une explosion de capteurs et de flux informationnels.

La guerre en Ukraine et le conflit en Iran le rappellent avec force : la saturation épuise, désorganise, submerge. Elle frappe les stocks, désarticule les chaînes logistiques et met à l'épreuve la résilience industrielle. La supériorité technologique seule ne suffit plus ; elle doit s'inscrire dans la durée et dans la masse. L'amiral Vandier[3] a prévenu : « *Nous devons nous préparer, sinon nous subirons ce que les pays du Golfe sont en train de subir.* (...) *L'enjeu n'est donc plus de faire davantage de ce que nous*

(1) Végèce, *De re militari.*

(2) Thucydide, *Histoire de la guerre du Péloponnèse,* 431-411 avant notre ère, trad. Jacqueline de Romilly, Robert Laffont éditeur, coll. Bouquins, 1990.

(3) Commandant suprême allié pour la transformation de l'OTAN.

faisions hier. Il s'agit dorénavant de trouver des réponses aux défis que posent la Russie ou l'Iran dans leur manière de faire la guerre, sur le plan de la masse des armes et leur vitesse d'évolution.[4] »

Or, dans ce contexte, la souveraineté n'est plus une ambition, mais une condition d'action. L'autonomie stratégique nous donne la capacité à décider et à agir sans subir, dans un environnement où chaque dépendance peut devenir une vulnérabilité.

Dans ce nouveau cadre stratégique et géopolitique, la supériorité ne repose plus uniquement sur des systèmes coûteux, jugés indestructibles, prévus sur le temps long, mais bien sur la capacité à absorber cette saturation et sur la masse. À mesure que les systèmes se multiplient et se banalisent, la valeur bascule : elle ne réside plus dans les plateformes elles-mêmes, mais dans le logiciel qui les rend intelligentes, interconnectées et capables de produire de l'effet.

Les tendances présentées dans ce document s'appuient sur ces constats. Elles décrivent un système de forces cohérent, au service d'un objectif unique : conserver la liberté d'action dans un monde contesté et saturé, tout en garantissant l'autonomie stratégique de l'Europe.

Face au basculement en cours, elles s'inscrivent dans trois impératifs qui structurent désormais l'action :

- ↘ **Surveiller et digérer la saturation :** maîtriser la connaissance de la situation dans tous les milieux, du spatial au cyber, en passant par les réseaux d'information, grâce au Space Situational Awareness (SSA), aux architectures Commandement et Contrôle (C2) et à la fusion des données ;

- ↘ **Agir plus vite que l'adversaire :** exploiter pleinement l'intelligence artificielle, les data spaces et, demain, les technologies quantiques pour accélérer la décision et conserver l'initiative ;

- ↘ **Construire et régénérer dans la durée :** réindustrialiser, produire à l'échelle, raccourcir les cycles d'innovation et rompre l'asymétrie entre une menace low cost et une défense coûteuse, en misant sur une masse intelligente et abordable.

(4) Amiral Vandier, mars 2026.

Dans ce contexte, Sopra Steria contribue, en tant qu'industriel de défense et de sécurité, à la transformation des capacités opérationnelles européennes. Convaincus que les défis d'aujourd'hui façonnent le futur, nous mobilisons innovation, expertise et approches hybrides pour renforcer la sécurité des États, des systèmes et des données.

Partenaire européen de référence de la souveraineté numérique, nous assurons le continuum de sécurité et nous contribuons à la construction de l'autonomie stratégique européenne. En reliant les systèmes, les données et les acteurs, nous permettons des opérations résilientes et interopérables, du commandement à l'exécution, grâce au C2, à l'IA, à la cybersécurité, aux systèmes autonomes, au cloud sécurisé et à la résilience de la supply chain.

Nous agissons au cœur des capacités opérationnelles : nous maîtrisons, intégrons et couplons les technologies critiques pour éclairer la décision, accélérer l'action et renforcer la résilience sur l'ensemble du spectre opérationnel et informationnel. En reliant systèmes, données et acteurs, nous contribuons directement à l'avantage stratégique.

Benoît CHATELAIN **Pierre LOPEZ**

« Dans un monde où la saturation devient la norme, la question n'est plus de savoir si nous devons nous adapter, mais à quelle vitesse — et avec quelles priorités. »

Surveiller et digérer la saturation

↘

TENDANCE 01.

Gagner la guerre avant la guerre : agir sur le champ informationnel

— P. 8

TENDANCE 02.

Renforcer la défense antiaérienne par la lutte anti-drones

— P. 12

TENDANCE 03.

Doter l'Europe d'une capacité spatiale de défense

— P. 16

TENDANCE 04.

Orchestrer l'action militaire multi-domaines

— P. 20

Agir plus vite que l'adversaire

Construire et régénérer dans la durée

GAGNER LA GUERRE AVANT LA GUERRE : AGIR SUR LE CHAMP INFORMATIONNEL

TENDANCE 01.

Dans les conflits contemporains, la victoire ne se joue pas seulement sur le terrain physique. Elle se décide aussi dans l'espace cognitif et le cyberespace, où la crédibilité des États, la réputation des armées et la confiance dans les alliances deviennent des cibles stratégiques. Les technologies numériques effacent les frontières entre champs physique et informationnel. Réseaux sociaux, plateformes et algorithmes sont des instruments d'influence à part entière.

La lutte informationnelle (LI) vise à préserver la crédibilité stratégique et la cohésion nationale dans la durée. Son volet militaire, la lutte informatique d'influence (L2I), s'inscrit dans le continuum cyber aux côtés de la lutte informatique défensive (LID) et offensive (LIO). Ensemble, elles participent directement à la souveraineté. Amplifiées par l'IA générative, les campagnes numériques produisent des effets stratégiques à coût marginal et sous couvert de déni plausible : deepfakes, micro-ciblage et diffusion massive de contenus saturent l'espace médiatique. Piratage et diffusion sélective de données renforcent ces dynamiques, souvent appuyées par des réseaux automatisés. L'Europe fait ainsi face à des campagnes persistantes : près de 20 000 cas de désinformation pro-Kremlin ont été recensés[5]. L'objectif : affaiblir nos sociétés en créant de multiples ruptures. Or, si les armées gagnent les batailles, ce sont bien les nations qui gagnent les guerres. L'impact financier est également énorme. Selon une étude inédite conduite par Sopra Steria, au niveau mondial, le coût économique de la désinformation est estimé à 417 Md$, soit 15% du PIB français en 2024[6].

« Les technologies numériques effacent les frontières entre champs physique et informationnel. »

Face à l'industrialisation des manipulations informationnelles, Sopra Steria développe une approche de bout en bout intégrée. Éclairé par son think tank sur la lutte contre les menaces informationnelles, le Cercle Pégase fédère un écosystème industriel au cœur des dynamiques informationnelles.

(5) EUvsDISINFO.

(6) Sopra Steria, *L'impact économique mondial de la désinformation.*

Cette démarche se concrétise avec **SENSEE**, une plateforme conçue pour détecter et gérer les agressions informationnelles. Appuyée sur un réseau d'entreprises françaises spécialisées en IA et en analyse de données — dont Visibrain, Magic LEMP, OPSCI.AI, Label4.AI et d'autres —, elle orchestre la collecte, l'analyse et la réponse aux campagnes de désinformation. Veille automatisée, détection des signaux faibles et coordination des actions permettent d'anticiper et de caractériser les attaques.

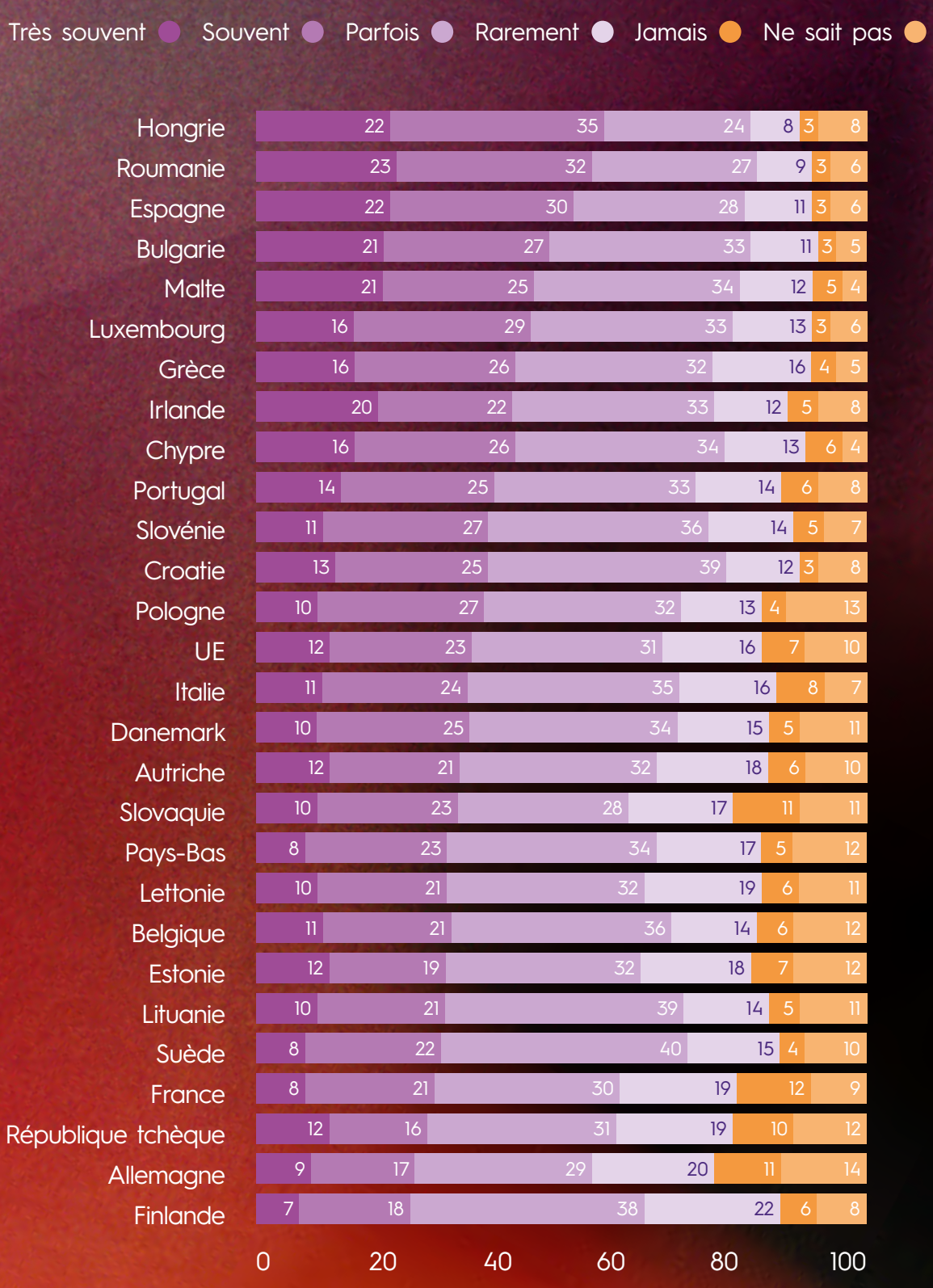
En complément, **Somulator**, outil de simulation développé avec l'Institut norvégien de recherche pour la défense et déployé par Sopra Steria, entraîne les organisations, militaires comme civiles, à gérer les crises informationnelles en recréant des environnements réalistes de réseaux sociaux[7]. La solution est notamment utilisée par les forces armées norvégiennes depuis 2023 lors d'exercices pour simuler des environnements informationnels en périodes de crise.

Enfin, Sopra Steria propose un dispositif d'observatoire informationnel sur des zones géographiques ciblées : analyses régulières, scénarios et recommandations stratégiques. Le groupe apporte ainsi une double expertise : technologique et stratégique. Acculturation aux enjeux de lutte informationnelle, outillage de pointe, proximité relationnelle et mise en relation avec des experts géographiques reconnus constituent des facteurs différenciants fortement appréciés des clients. L'ensemble protège la légitimité et l'efficacité opérationnelle.

La guerre informationnelle est permanente. Elle vise d'abord la légitimité, avant les capacités. Détecter plus tôt, comprendre plus vite, répondre plus précisément : la supériorité informationnelle se construit dans la durée. Sopra Steria accompagne les acteurs de la défense et de la sécurité pour renforcer cette résilience et préserver leur liberté d'action.

(7) Somulator est utilisé par les armées, le secteur public (ministères, mairies), le monde de l'éducation et de la recherche, le secteur de la santé et l'OTAN.

EXPOSITION PERÇUE À LA DÉSINFORMATION (2025)



Source : Euronews, Enquête Eurobaromètre sur les réseaux sociaux 2025 - Pensez-vous avoir été exposé à la désinformation et aux fausses informations au cours des 7 derniers jours ?

RENFORCER LA DÉFENSE ANTIAÉRIENNE **PAR LA LUTTE ANTI-DRONES**

TENDANCE 02.

L'omniprésence des drones au cœur des conflits modernes souligne le besoin d'actualiser la protection de nos forces et sites critiques. Les adversaires de l'Europe adoptent des tactiques de saturation et d'attrition à base de vecteurs mixtes : drones, artillerie, missiles balistiques et de croisières, projectiles hypersoniques, etc. Cette multiplicité des facteurs de menace oblige la réponse à également être multiple.

La massification industrielle des drones et la cadence saturante des salves mixtes dégradent le rapport coût/effets de la défense antiaérienne. Un drone russe Geran-2, produit à plus de 5 000 unités par mois, coûte 30 000 €[8], près de 20 fois moins qu'un missile air-air/sol-air dédié comme le MICA[9] (MBDA), coûtant 600 000 € et à la faible cadence de production[10]. Certains drones sont modernisés pour résister au brouillage – filoguidage, prise en charge multi-constellations ou IA embarquée. Enfin, les missiles d'interception « low cost » et canons DCA modernes, à la portée réduite, nécessitent un maillage très resserré.

La parade ukrainienne est un système de systèmes interopérables : des drones et missiles low cost (Sting, Octopus) en masse, combinés à des solutions décentralisées de guerre électronique (EW) et à des systèmes de fusion de données spécialisés en tracking de drones, permettent un taux d'efficacité au-delà de 90 % face aux effecteurs russes. Le système de défense israélien utilise un couplage similaire, incluant ses batteries « Iron Dome » et des systèmes d'armes à énergie dirigée (AED) « Iron Beam ».

Contrer cette menace requiert d'accomplir la jonction entre défense antiaérienne et lutte anti-drones (LAD), en implémentant plusieurs solutions : d'une part, des détecteurs distribués (radars, caméras multispectrales, capteurs passifs) dans chaque milieu, et une fusion multicapteurs au sein de C2 pouvant suivre des scénarios de lutte anti-essaims. D'autre part, des effecteurs multicouches et interopérables (missiles Aster, outils antimissiles et anti-drones low cost, systèmes d'EW ciblant les liaisons et le C2 des essaims de drones) pouvant

(8) Meta-défense, septembre 2025.
(9) Missile d'Interception, de Combat et d'Auto-défense
(10) *L'Opinion,* mars 2026.

« Pionnier de la lutte anti-drones en France, le groupe développe BOREADES depuis plus de dix ans et ne cesse d'investir et d'innover pour faire évoluer sa solution en permanence et anticiper l'évolution des menaces drones. »

répondre à des attaques saturantes. Le projet European Air Shield au cœur de la Readiness Roadmap de la Commission européenne doit conduire à l'achat de systèmes de défense aérienne jusqu'en 2030.

Sopra Steria répond avec le C2 **BOREADES**, système de fusion de données multicapteurs spécialisé dans la LAD et dans le tracking multicibles, et interopérable avec tout senseur ou effecteur au standard SAPIENT ou avec des systèmes de défenses antiaériennes (SAP, L16). ITAR-free et senseur-agnostique, BOREADES peut orchestrer la chaîne complète de la LAD (de la détection à la neutralisation), en interfaçant divers effecteurs anti-drones ou antimissiles, dont le système AED Helma-P (CILAS) ou des drones intercepteurs.

Opérationnel depuis plus de dix ans et déployable rapidement grâce à des cycles courts de tests et de passage à l'échelle, BOREADES a fait ses preuves au cours des Jeux olympiques 2024 de Paris (au cœur de programmes comme PARADE, MILAD ou RADIANT), et peut être embarqué sur des plateformes terrestres comme les Serval ou les Proteus.

Sopra Steria développe de plus des systèmes optroniques pour l'optimisation de la détection de drones dans des environnements dégradés (contexte urbain, incidence météorologique, etc.).

Enfin, pour assurer une protection efficace contre la menace drone, BOREADES est interopérable avec les systèmes de défense aérienne et les systèmes de sécurité et de protection de sites sensibles via ses solutions CRIMSON et STARLINX. C2 multi-domaines utilisant les dernières technologies des jumeaux numériques, la simulation, la réalité étendue et l'intelligence artificielle, CRIMSON facilite le partage d'informations, la coordination, le commandement et l'aide à la décision. STARLINX est un système autonome ou complémentaire de C2 multi-liaisons de données tactiques pour des opérations conjointes et combinées.

INTEROPÉRABILITÉ DU C2 BOREADES

Le C2 BOREADES est un système ouvert pouvant s'interconnecter avec des systèmes existants via la norme SAPIENT de l'OTAN pour les senseurs et effecteurs et via L16, SAP, etc., pour des C2 de défense antiaérienne.

Source : Sopra Steria

DOTER L'EUROPE D'UNE CAPACITÉ **SPATIALE DE DÉFENSE**

TENDANCE 03.

L'espace est devenu un domaine de conflictualité à part entière. La guerre en Ukraine en a fourni une illustration dès ses prémices, avec l'attaque russe contre les terminaux au sol du satellite KA-SAT, visant à perturber les communications militaires. Depuis, les menaces se sont diversifiées : brouillage, aveuglement, cyberattaques, armes antisatellites ou encore capacités orbitales offensives. Ces attaques dépassent largement le cadre militaire et peuvent affecter directement les économies. À titre d'exemple, près de 20 % du PIB du Royaume-Uni est lié aux services satellitaires, et une interruption du GPS coûterait environ 1 Md£ par jour à son économie[11].

Dans ce contexte, le secteur spatial connaît donc une mutation rapide et profonde, marquée par une militarisation croissante et un recentrage sur les enjeux de défense et de sécurité[12]. L'Europe affiche ainsi sa volonté d'autonomie stratégique, en développant ses propres services d'observation, de positionnement et de communications sécurisées, sans recourir à des systèmes non européens. Concernant les communications, l'Europe investit environ 200 M€ dans les études initiales d'IRIS² et en parallèle l'Allemagne accélère fortement avec son projet SATCOMBw, doté d'un investissement massif de 8 à 10 Md€.

Le programme ERS (European Resilience from Space), porté par l'ESA, s'inscrit dans cette ambition. Doté d'un budget d'environ 1,2 Md€, il vise à fédérer les capacités nationales et à coordonner les systèmes à usage dual. Son lancement opérationnel est envisagé autour de 2028, ce qui s'aligne avec le prochain cadre financier pluriannuel (MFF)[13] de l'Union européenne et montre que l'ERS s'inscrit dans une vision moyen terme de la souveraineté spatiale européenne.

Cependant disposer de capacités spatiales ne suffit pas si celles-ci ne sont pas protégées. Face à des adversaires capables de brouillage ou d'actions offensives dans l'espace, la sécurisation des actifs devient essentielle.

(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).

Le projet de bouclier spatial européen vise ainsi, à horizon 2030 et dans la continuité directe de l'ERS, à fournir aux États membres un service de protection des actifs et services spatiaux. Il s'appuiera, là aussi, sur les capacités spatiales à double usage de l'UE et favorisera le développement de capacités de défense nationales interopérables, notamment autour de Galileo et de la surveillance de l'espace.

Dans ce cadre, la connaissance de la situation spatiale (SSA) devient un enjeu central. L'augmentation du nombre de satellites et le développement des constellations accentuent les risques de collision et complexifient la gestion du trafic spatial.

Face à ces défis, Sopra Steria intervient à différents niveaux :

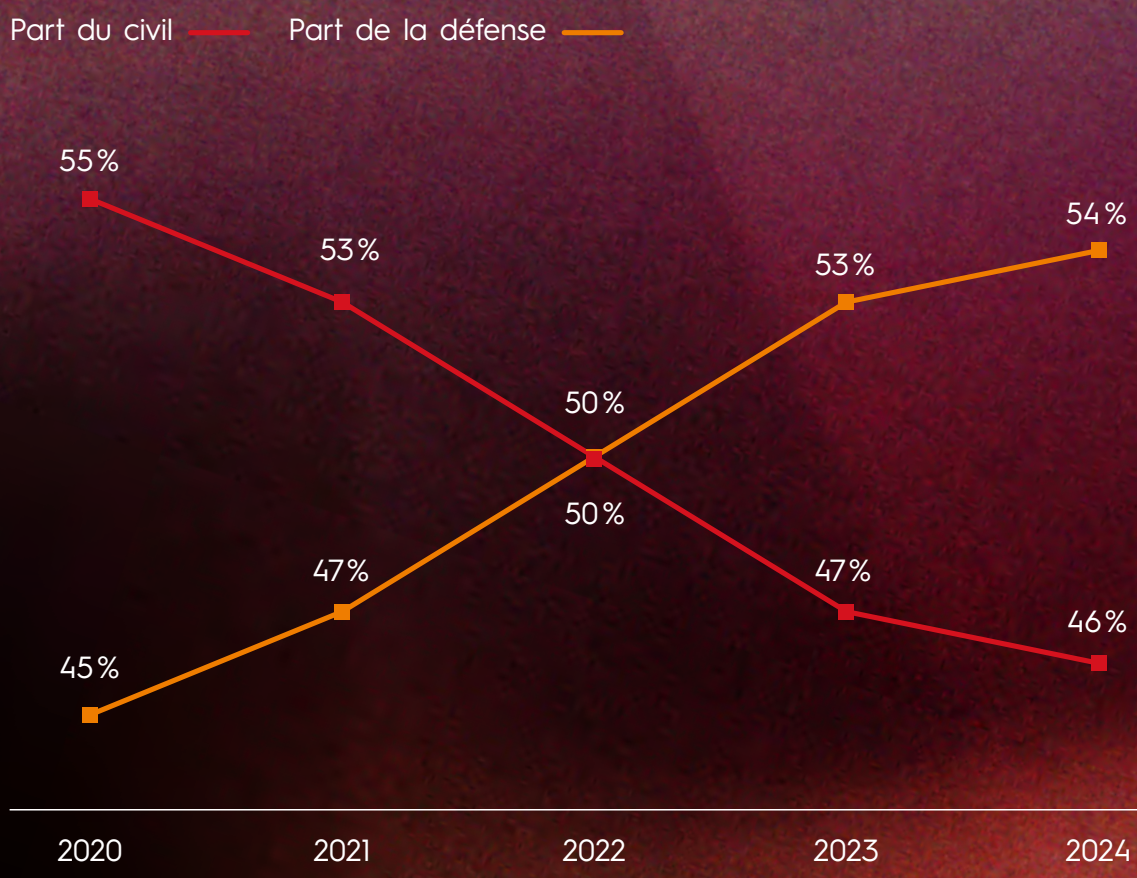
↘ **En développant le concept de constellation virtuelle, basé sur la ligne de produits segment sol GOSMIC.**
Une constellation virtuelle n'est pas un système satellitaire physique unique, mais un ensemble coordonné de missions et de capteurs opérés indépendamment par différents pays et organisations. L'objectif est d'améliorer la disponibilité et l'accessibilité des données en tirant parti de multiples missions satellitaires opérées par diverses agences et entreprises spatiales.

« La connaissance de la situation spatiale (SSA) devient un enjeu central. »

↘ **En concevant et exploitant, pour le CNES,** le nouveau système national de gestion du trafic spatial **STREAMS** (Space Traffic Evaluation and Management System), qui repose sur un catalogue national des objets spatiaux, un service permanent de détection et de gestion des risques de collision et une plateforme agile permettant d'intégrer rapidement des innovations issues de l'écosystème de la surveillance.

BUDGETS SPATIAUX CIVILS ET DE DÉFENSE

Évolution de la répartition entre les budgets spatiaux civils et de défense à l'échelle mondiale (2020-2024)



Source : European Space Agency

ORCHESTRER L'ACTION MILITAIRE MULTI-DOMAINES

TENDANCE 04.

Le retour des conflits symétriques s'appuyant sur des opérations multi-domaines (MDO)[14] change la donne. En plus des cinq milieux de confrontation principaux (terre, mer, air, cyber, espace), les champs transverses (électromagnétique, informationnel) et espaces communs (très haute altitude, fonds marins) sont désormais contestés. Les MDO mobilisent simultanément des capacités (capteurs et effecteurs) dans plusieurs de ces domaines pour obtenir un effet et s'appuient sur l'évolution rapide des moyens de communication pour l'échange de données, accélérant le tempo opérationnel et réduisant la boucle décisionnelle. L'objectif est de préserver la supériorité opérationnelle, ce qui requiert de maîtriser le flux des données, mais aussi d'assurer la synchronicité des effets dans un laps de temps toujours plus réduit.

Plusieurs innovations numériques contribuent à la mise en œuvre du MDO par les forces armées : l'automatisation par IA avancée du cycle captation-traitement-diffusion de la donnée tactique multisource et multiformat ; l'usage de constellations de satellites pour accélérer et fiabiliser l'accès et la transmission de la donnée ; la maturation des plateformes de combat collaboratif par la mise en œuvre de cloud de combat ; l'interopérabilité des systèmes d'armes de chaque milieu. Ces innovations permettent de réduire la charge cognitive liée au traitement massif d'informations tactiques sur un laps de temps court, indispensable à la bonne conduite d'opérations MDO.

Les résultats sont observables sur le terrain en Ukraine comme en Iran : kill chains ultra-courtes (identification par drones, tirs d'artillerie, évaluation de dommages et retask en quelques minutes), manœuvres tactiques conduites grâce au maillage de moyens multi-domaines (ISR[15] issu de satellites commerciaux, brouillage, frappes par drones kamikazes), etc. La décentralisation des moyens et capacités (brouilleurs tactiques, micro-drones, etc.) fluidifie la chaîne décisionnelle et permet des boucles OODA[16] très courtes. Cette nouvelle agilité dépend en particulier de la

(14) Multi-Domain Operations.
(15) Intelligence, Surveillance, Reconnaissance.
(16) Observer-Orienter-Décider-Agir.

capacité d'accès aux données par les forces du niveau tactique. Il est donc essentiel de garantir la sécurité et la maîtrise des flux des infrastructures numériques (datacenters, câbles sous-marins), désormais considérées comme cibles privilégiées, comme le démontrent les frappes iraniennes sur des sites d'AWS début 2026.

Ces opérations trouvent ainsi leurs limites dans la fiabilité d'accès et de gestion de la donnée. La destruction d'infrastructures de service, un brouillage ou une cyberattaque peuvent affaiblir la chaîne opérationnelle de transmission et forcer un retour à des procédés dégradés – dans ce cas, la charge cognitive trop importante pour l'opérateur peut remettre en cause la mise en œuvre du MDO.

Dans ce cadre, des systèmes de commandement et contrôle (C2) interopérables, orchestrant de multiples capteurs de données duales sont indispensables.

Afin de coordonner les actions interarmées et interalliées, Sopra Steria avance aux côtés des forces armées avec la solution **CENTERIS**, système d'hypervision compatible avec les standards de l'OTAN (L16),

« La destruction d'infrastructures de service, un brouillage ou une cyberattaque peuvent affaiblir la chaîne opérationnelle de transmission. »

hautement modulaire et adaptatif et capable d'intégrer des applications métiers et des innovations tierces dont celles de la planification 2D et de la logistique terrestre (solutions Sopsight.ai[17]). CENTERIS est basé sur la solution CRIMSON Defence apportant les capacités de SITAC et de jumeau numérique du théâtre des opérations ainsi que les capacités ISR, de gestion de systèmes robotisés, ainsi que d'aide au commandement à l'aide de l'intelligence artificielle. Basée sur une architecture intégrant la sécurité data-centrée (DCS) CENTERIS apporte une vision nouvelle et data-centrée du commandement des opérations multi-domaines associant moyens militaires et infrastructures duales.

(17) Solutions d'IA multimodales, explicables et souveraines, contribuant à la supériorité opérationnelle multi-domaines.


SECRET OPERATION
OPERATION STATISTIC
sub procedure sendBit()
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
sub procedure sendBit2(dim
boolean)
if (b
SECRET INFORMATION

BÂTIR UNE IA DE DÉFENSE SOUVERAINE, **SÉCURISÉE ET DE CONFIANCE**

TENDANCE 05.

La montée en puissance de l'intelligence artificielle transforme le combat traditionnel et renforce les stratégies hybrides – qui mêlent entre autres actions militaires, cyber, informationnelles. L'IA devient un levier stratégique, mais aussi une source d'instabilité. Alors que les États-Unis et la Chine investissent massivement dans les technologies avancées de défense, l'Europe doit impérativement rester compétitive et investir dans le développement de solutions d'intelligence artificielle fiables, robustes et souveraines pour ses capacités de défense.

Les investissements prennent forme. Des agences gouvernementales dédiées à l'IA de défense sont créées : le DAIC[18] au Royaume-Uni et l'AMIAD[19] en France, dotée d'un financement annoncé de 2 Md€ à l'horizon 2030[20]. Les grands industriels soutiennent les start-up du secteur – Saab avec Helsing (plus de 1,5 Md€ levés), Dassault Aviation avec Harmattan AI (environ 200 M€ levés). Parallèlement, la coopération industrielle s'intensifie pour concevoir des solutions d'IA adaptées aux systèmes critiques dans tous les domaines. Par exemple, Dassault Aviation et Naval Group collaborent avec Thales au sein de l'accélérateur cortAIx, qui conçoit des outils d'IA pour la détection, la classification et l'identification des menaces.

Aide à la décision pour le commandement, assistance au ciblage et à la conduite des frappes, sécurisation des infrastructures critiques : l'IA de défense multiplie les usages. Grâce à sa capacité à traiter rapidement et massivement des données, l'IA devient un véritable démultiplicateur des performances opérationnelles. Toutefois, déployer l'intelligence artificielle dans le domaine militaire présente de nombreux défis. Les standards de fiabilité, de sécurité et de transparence sont particulièrement élevés. Les solutions développées doivent fonctionner dans les centres de commandement stratégique, en edge sur les sites opérationnels, et en far edge pour les systèmes embarqués.

(18) Defence Artificial Intelligence Centre.
(19) Agence ministérielle pour l'intelligence artificielle de défense.
(20) Ministère des Armées et des Anciens Combattants, mars 2024.

Renforcer l'explicabilité et la transparence des systèmes d'IA impose de standardiser les points de mesure des modèles et d'intégrer les composants d'explicabilité tout au long de la chaîne de conception. Sécurité et souveraineté exigent un environnement fermé : conception et déploiement doivent reposer sur des infrastructures dédiées. L'intégration d'IA embarquée impose la réduction de la complexité calculatoire et une optimisation des phases d'apprentissage pour concevoir des modèles plus petits. La rapidité de réentraînement des modèles pour faire face aux adaptations de l'ennemi est également clé – et ce, en garantissant la non-régression de leurs performances acquises. Enfin, pour garantir une IA de confiance dans la défense, l'IA doit proposer, tandis que l'humain conserve l'entière responsabilité des actions.

Sopra Steria s'engage pour répondre à ces enjeux à travers sa participation à des écosystèmes d'IA de confiance, comme ANITI et l'ETA[21] – dont Sopra Steria est membre fondateur aux côtés de l'IRT SystemX et de Thales.

« La rapidité de réentraînement des modèles pour faire face aux adaptations de l'ennemi est également clé. »

Sopra Steria propose une **infrastructure d'IA souveraine et de confiance,** combinant la plateforme MLOps **InnerData** pour l'industrialisation de l'ensemble du cycle de vie des projets IA et la solution **IAKa,** dédiée à l'IA générative et agentique, et conçue pour les environnements critiques.

Architecte de solutions pour de multiples cas d'usage, Sopra Steria maîtrise la chaîne d'industrialisation et de confiance des solutions numériques d'IA autonomes et des solutions intégrées dans les systèmes d'armes. À l'échelle européenne, la conception de modèles d'IA mutualisés exige des infrastructures de partage de données entre alliés. Sopra Steria contribue activement à l'élaboration d'un data space européen pour la défense.

(21) European Trustworthy AI Association.

ETA – EUROPEAN TRUSTWORTHY AI ASSOCIATION

Industrialiser et diffuser la méthodologie et les composants d'une IA de confiance :
- Maturation des composants clés pour la robustesse, les données et la traçabilité ;
- Accompagnement des organisations dans leur transformation IA.

Sopra Steria est à la fois fondateur et fournisseur technologique de l'ETA afin d'accompagner ses membres sur nos principaux domaines d'expertise :
- Les plateformes ;
- La maturation technique.

NIVEAU D'ADHÉSION

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

Source : European Trustworthy AI Association.

PARTAGER ET EXPLOITER LES DONNÉES EN OPÉRATION

TENDANCE 06.

Le renforcement des opérations multi-domaines et interalliées ainsi que l'accélération de la prise de décision via l'intelligence artificielle et les techniques avancées d'analytique de données reposent sur une intégration fluide des réseaux, plateformes, systèmes d'armes, capteurs et données. Cloud et connectivité doivent ainsi être pleinement intégrés aux plateformes et systèmes de défense, afin d'exploiter tout le potentiel technologique au service de la supériorité opérationnelle.

Pour garantir un partage sécurisé d'informations sur le champ de bataille et entre alliés, les États européens doivent assurer la souveraineté de la gestion et du stockage des données. Les États préserveront ainsi leur capacité d'analyse, de compréhension et de protection des données critiques. Plusieurs initiatives émergent : depuis juillet 2025, 12 pays de l'OTAN[22] participent au programme de logiciels interalliés pour services cloud et edge (programme ACE[23]), visant à accélérer et faciliter le partage et le stockage d'informations classifiées dans tous les milieux d'opération.

Parallèlement, l'Agence européenne de défense (AED) pose les bases d'un espace européen de partage de données (projet DAIDS[24]). Ces deux dispositifs devraient être opérationnels d'ici 2030.

Le développement d'un cloud militaire souverain permettra de réduire les vulnérabilités et la dépendance potentielle aux solutions extra-européennes. Un data space européen de défense s'appuyant sur une architecture fédérée et décentralisée – et respectant les standards de l'OTAN – où chaque donnée reste sous l'autorité de son propriétaire, permet d'envisager un partage de données transfrontalier tout en préservant la souveraineté de chacun. Au-delà du stockage, la qualification des données sera clé, notamment pour alimenter efficacement les modèles d'IA. L'IA pourra d'ailleurs elle-même être mise au service de la mise en qualité des données.

(22) Belgique, Canada, Allemagne, Danemark, Espagne, États-Unis, Finlande, France, Grèce, Italie, Luxembourg, Norvège, Pays-Bas, Roumanie, Royaume-Uni et Suède – et le Commandement allié Opérations.

(23) Allied Software for Cloud and Edge Services.

(24) Defense Artificial Intelligence Data Space.

Selon le rapport 2025 de l'ENISA[25], les infrastructures et services digitaux constituent la principale cible du cybercrime en Europe, avec 13,7% des incidents recensés. Plus spécifiquement, 27,7% des incidents de violations de données touchent les infrastructures et services digitaux. Assurer la sécurité des données de défense dans les espaces de stockage et de partage sera donc clé. Au-delà de la protection des réseaux et des infrastructures, la sécurité se recentre aujourd'hui sur la donnée elle-même, grâce à l'approche de « data-centric security ». Chaque donnée est protégée individuellement, notamment via le chiffrement, le contrôle strict des accès (authentification multifactorielle, application du moindre privilège), la traçabilité des actions (journalisation), et des mécanismes robustes de sauvegarde et de réplication.

Sopra Steria introduit les principes de **data centric security** dans le cadre du projet de **data space européen de défense** porté par l'AED aux côtés du CEA et du Cloud Data Engine.

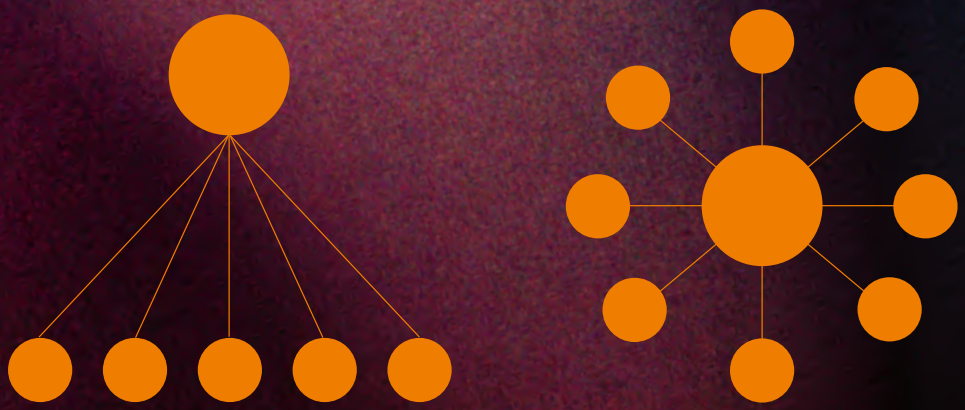
« Les infrastructures et services digitaux constituent la principale cible du cybercrime en Europe, avec 13,7% des incidents recensés. »

Fort de son positionnement unique, entre acteur souverain du numérique et acteur de la défense, Sopra Steria transpose les meilleures pratiques civiles dans le domaine militaire. Son expertise dans la conception de data spaces s'appuie sur son engagement dans les projets Data4NuclearX (nucléaire) et Decade-X (aéronautique) et sur son rôle de leader du consortium InfrateX[26]. Enfin, Sopra Steria joue un rôle central dans le développement du **Secure Cloud** en Europe.
Par exemple, le groupe figure parmi les premiers intégrateurs européens de l'On-Prem Cloud Platform (OPCP) d'OVHcloud : une solution européenne permettant de déployer une infrastructure cloud complète, sécurisée et souveraine, directement sur site, y compris dans des environnements isolés (air-gap).

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

(26) Le consortium InfrateX est responsable de l'implémentation du programme Simpl pour la DG Connect de la Commission européenne.

ÉCHANGE DE DONNÉES : PLATEFORMES TRADITIONNELLES VS DATA SPACES



PLATEFORMES DATA TRADITIONNELLES

- Opérations centralisées
- Cadres commercial et technique définis par le propriétaire de la plateforme
- Échanges gérés par la plateforme
- Données (souvent) utilisées par les fournisseurs à des fins commerciales

DATA SPACES

- Système décentralisé
- Cadre de gouvernance partagé par data space
- Autonomie des participants
- Échanges traçables et transparents entre les participants
- Contrôle de l'utilisation des données spécifique au data space mais basé sur des référentiels communs
- Interopérabilité des data spaces

Source : Gaia-X Hub France.

PASSER DE L'EXPLORATION À L'ACTION AVEC LE QUANTIQUE

TENDANCE 07.

Technologie de rupture, le quantique ouvre la perspective d'une connaissance presque instantanée du champ de bataille : navigation sans GPS, détection d'une précision inédite, simulation accélérée et sécurisation avancée des communications. Faut-il y voir la fin du *« brouillard de la guerre »* décrit par Carl von Clausewitz ? Ou seulement son déplacement, tant la guerre reste soumise aux frictions – erreurs humaines, complexité, hasard, adversité ? Le débat demeure ouvert.

L'European Armament Technological Roadmap[27] identifie l'IA et le quantique comme des priorités stratégiques : leur maîtrise conditionne l'autonomie européenne. Mais cette révolution est ambivalente. Les futurs ordinateurs quantiques pourraient fragiliser les systèmes de chiffrement actuels et nourrir le « harvest now, decrypt later ». L'enjeu est clair : protéger les communications, renforcer la résilience et préserver la crédibilité opérationnelle.

La compétition mondiale s'intensifie. États-Unis et Chine investissent massivement, tandis que l'Europe cherche à préserver sa souveraineté. Les technologies progressent rapidement : qubits supraconducteurs, ions piégés, photons. Des approches hybrides émergent, combinant calcul classique et quantique. Le caractère dual accélère la dynamique, les usages civils soutenant indirectement les capacités militaires. La France, de son côté, « *est bien dans la course*[28] ». « *Le quantique doit être regardé non comme un sujet théorique, mais comme un sujet stratégique, concret et désormais pleinement opérationnel.*[29] » La France triple ainsi son effort en ajoutant 200 M€ aux 120 M€ sur la période 2024-2030.

Le quantique repose sur trois piliers : calcul, capteurs, réseaux. Le calcul ouvre des perspectives en cryptanalyse, simulation et optimisation. Les capteurs – gravimètres, horloges atomiques,

(27) Commission européenne, *White paper for European defence - Readiness 2030.*

(28) Ingénieur général de l'armement Patrick Aufort, Directeur de l'agence de l'innovation de défense, avril 2026.

(29) Catherine Vautrin, ministre des Armées, avril 2026.

navigation sans GPS – promettent des gains majeurs. Le magnétomètre quantique pourrait transformer la détection des sous-marins en révélant les variations du champ magnétique, remettant en question l'invisibilité des composantes de dissuasion. Les réseaux quantiques sécurisent les communications via la distribution de clés.

Sopra Steria inscrit le quantique dans une logique opérationnelle expérimentant des cas d'usage concrets pour la défense, en lien avec un écosystème de partenaires de référence, dont Quandela, Pasqal et CryptoNext, via le fonds Quantonation. Deux axes structurants se dégagent : la résilience des réseaux critiques face aux attaques ou défaillances, et l'optimisation logistique dans des environnements complexes.

Dans le spatial, le projet QC4GEO explore l'apport du quantique pour la classification d'images satellitaires, avec un double objectif de précision et de rapidité. Dans la simulation, des travaux sur le modèle Lattice Boltzmann ouvrent la voie à des performances accrues.

« Faut-il y voir avec le quantique la fin du *"brouillard de la guerre"* décrit par Clausewitz ? »

Parallèlement, des réseaux de neurones quantiques sont développés pour traiter des volumes massifs de données.

Enfin, la cybersécurité est au cœur des enjeux. Sopra Steria intègre la cryptographie post-quantique dans sa solution **Datasphere** afin d'anticiper l'obsolescence des standards actuels et garantir une protection durable des données sensibles. Cette solution est conforme aux recommandations de l'ANSSI en matière de transition vers des schémas de chiffrement hybrides post-quantiques, et interopérable avec les standards de sécurité internationaux (OTAN, NIST).

Le quantique n'est plus un horizon lointain. Il devient un levier opérationnel. Anticiper, tester, intégrer.

UN MARCHÉ EN FORTE ACCÉLÉRATION

Le marché des technologies quantiques de défense reste émergent, mais en forte accélération.

10 MD$

À HORIZON 2030-2035

Selon les périmètres retenus, il se situe aujourd'hui entre 1 et 3 Md$, avec des projections allant de 3 à plus de 10 Md$ à horizon 2030-2035[30], soit des taux de croissance annuels compris entre 15% et 25%[31].

Parallèlement, les investissements publics se structurent à grande échelle : plus de 1,8 Md€ en France[32], 2,5 Md£ au Royaume-Uni[32] et plusieurs centaines de millions d'euros en Allemagne, dont une part croissante dédiée aux applications de défense et de sécurité.

1,8 MD€

EN FRANCE

(30) Custom Market Insights, Quantum Warfare Market 2025-2034 ; Fortune Business Insights, Quantum Warfare Market 2026-2034.
(31) Insight Monk, Quantum Warfare Market 2024-2035.
(32) LaREF, mars 2025.
(33) JDN, juin 2025.

RETROUVER LA **PROFONDEUR STRATÉGIQUE**

TENDANCE 08.

Le retour des guerres de haute intensité et des conflits d'attrition, qui mobilisent massivement hommes et ressources, redéfinit les exigences stratégiques. Au-delà de la supériorité technique, la profondeur logistique et la masse deviennent déterminantes. Le plan Readiness 2030 de la Commission européenne évalue d'ailleurs les besoins capacitaires à 800 Md€[34]. Les États européens sont appelés non seulement à moderniser leurs forces armées, mais aussi à renforcer leur résilience et leur capacité à soutenir l'effort dans la durée. L'heure est au réarmement massif.

En France, la Loi de programmation militaire 2024-2030 prévoit 413 Md€ pour les armées[35], un budget susceptible d'être réévalué à la hausse. L'Allemagne, de son côté, prévoit plus de 100 Md€ de dépenses rien qu'en 2026[36]. Si l'effort budgétaire est bien réel, la dépendance persistante aux équipements de défense non européens et la question de la capacité industrielle à monter en puissance demeurent. Garantir l'autonomie stratégique impose de renforcer la compétitivité et la réactivité de la base industrielle et technologique de défense.

L'objectif est sans équivoque : il s'agit de produire à la fois des systèmes toujours plus complexes et d'autres plus simples et en masse, dans des délais resserrés, tout en maintenant des exigences élevées de qualité et de performance. Ce mouvement est déjà amorcé. KNDS, par exemple, a triplé sa production mensuelle de canons CAESAR, passant de deux unités avant le conflit ukrainien à six en 2024[37]. Dans le même temps, les nouveaux entrants démontrent leur capacité d'innovation et d'accélération industrielle : Harmattan AI, créée en 2024, vise la production de 10 000 drones par mois dès cette année[38], tandis qu'Exail Technologies est devenue en quatre ans le leader européen des drones de déminage sous-marin.

Innover vite, tester vite, déployer vite. Pour passer de cycles longs et de petites séries à une économie de stocks, les usines et processus doivent se transformer. La réduction des cycles

(34) Commission européenne.
(35) Ministère des Armées et des Anciens Combattants.
(36) *La Tribune,* janvier 2026.
(37) *Capital,* mars 2025.
(38) *L'Usine Digitale,* janvier 2026.

de conception impose de moderniser les systèmes d'information, en intégrant outils collaboratifs, modélisation, simulation, etc. L'accélération des cadences dépendra en partie de l'adoption des nouvelles technologies, notamment de l'intelligence artificielle. Résumés d'instructions d'assemblage complexes, détection et gestion des non-conformités, assistance technique : les cas d'usage sont nombreux.

Le renforcement de la continuité digitale entre les différents métiers (ingénierie, production, support) et au sein de l'entreprise étendue, incluant filiales et fournisseurs, est indispensable. Produire plus, et plus vite, requiert non seulement de sécuriser les chaînes d'approvisionnement, mais aussi de fournir aux sous-traitants les moyens financiers et technologiques nécessaires pour soutenir la montée en puissance.

Avec la plateforme **BluejaySecureCollaboration,** Sopra Steria garantit une collaboration sécurisée entre acteurs de défense, et participe ainsi à accélérer la livraison des programmes critiques. Sopra Steria participe également au projet de data space porté par l'Agence européenne de défense aux côtés du CEA et du Cloud Data Engine.

Avec les suites logicielles de **Connectiv-IT,** Sopra Steria répond aux enjeux de digitalisation de la supply chain et des services de MCO du secteur. Sa solution **SCR²M**[39] permet aux industriels de détecter et valoriser financièrement les risques de ruptures d'approvisionnement, permettant ainsi d'agir en amont pour éviter des retards ou pénalités contractuelles.

Sopra Steria mobilise aussi un écosystème de partenaires spécialisés, tels que Picomto, expert de la digitalisation des processus critiques de maintenance et de production. Enfin, Sopra Steria déploie des dispositifs de développement des compétences et de conduite du changement pour garantir l'adoption de nouvelles solutions.

(39) Supply Chain Risk and Resilience Management.

« Au-delà de la supériorité technique, la profondeur logistique et la masse deviennent déterminantes. »

INTÉGRER LES DRONES **EN MASSE AU COMBAT**

TENDANCE 09.

Simple outil ISR jusqu'en 2019[40], le drone connaît aujourd'hui un usage transformatif sur des théâtres d'opérations contemporains dans tous les milieux : terre, mer et air. Si le drone lourd MALE était prééminent jusqu'au conflit en Ukraine, l'effet d'échelle permis par les petits systèmes rend ces derniers incontournables : modèles civils détournés, munitions rôdeuses, drones en essaim, etc.

Les évolutions dans l'IA embarquée, la latence ultra-basse permise par les déploiements 5G et satellitaires ainsi que la chute du coût des capteurs radar, multi-spectral et LiDAR entraînent une croissance rapide du secteur des UxV[41]. La démocratisation de petits modèles moins onéreux que les outils de défense classiques, comme le Shahed-136 iranien, multiplie les usages : patrouille, leurrage, frappe, appui au contact, etc. L'usage d'ISR transmis par drones aériens pour des frappes par drones de surface contre des cibles russes en mer Noire démontre le changement de paradigme créé par l'usage combiné de drones multi-milieux, et par le recours à des tactiques de saturation des défenses par essaims. Ainsi, en Ukraine, les drones causent 70 % à 80 % des pertes sur le front[42].

Les instances publiques pivotent pour intégrer ces capacités : la loi de programmation militaire française 2024-2030 consacre 5 Md€ à l'achat de drones et à la maîtrise du vol en essaim en 2030[43]. Londres a annoncé investir 4,6 Md€ pour équiper ses forces en systèmes autonomes[44], et la Readiness Roadmap 2030 de la Commission européenne prévoit un investissement prioritaire dans des capacités de frappes de précision par drones d'ici 2027. Le secteur privé n'est pas en reste : Helsing et Stark Defence ont sécurisé 1 Md€ chacun pour équiper la Bundeswehr de drones kamikazes[45], Harmattan.AI a levé 171 M€ pour passer sa production de drones à l'échelle[46], et Arquus et Renault se sont associés pour concevoir des drones terrestres.

(40) Les MQ-9 Reaper de l'Armée de l'air et de l'espace française n'ont été équipés d'armement qu'en décembre 2019.
(41) Unmanned extended Vehicles (drones aériens, maritimes, terrestres).
(42) US Army War College.
(43) Ministère des Armées et des Anciens Combattants.
(44) Gouvernement britannique.
(45) *Les Echos,* février 2026.
(46) *L'Usine Digitale,* janvier 2026.

Répondre à cet enjeu nécessite de déployer des architectures robustes de fusion de données et de gestion centralisée de multiples vecteurs semi-autonomes. La fiabilisation de la connectivité dans tous les milieux et le recours à des outils de mise en réseau et de gestion fine de drones en masse sont indispensables au maintien de la supériorité de nos forces. Faciliter cette mise en œuvre et intégrer de nouveaux modèles appelle une forte interopérabilité des systèmes : l'agnosticité d'achat et d'usage de drones repose sur une standardisation des interfaces d'utilisation. Enfin, le recours massif aux UxV en opérations de longue durée requiert d'intégrer l'alimentation énergétique à la logistique opérationnelle, et de mettre en place des systèmes de gestion fine de l'énergie au niveau tactique.

C'est à ces besoins que répond Sopra Steria. Son expérience de l'accompagnement des forces le positionne comme un leader européen de la fusion de données et de

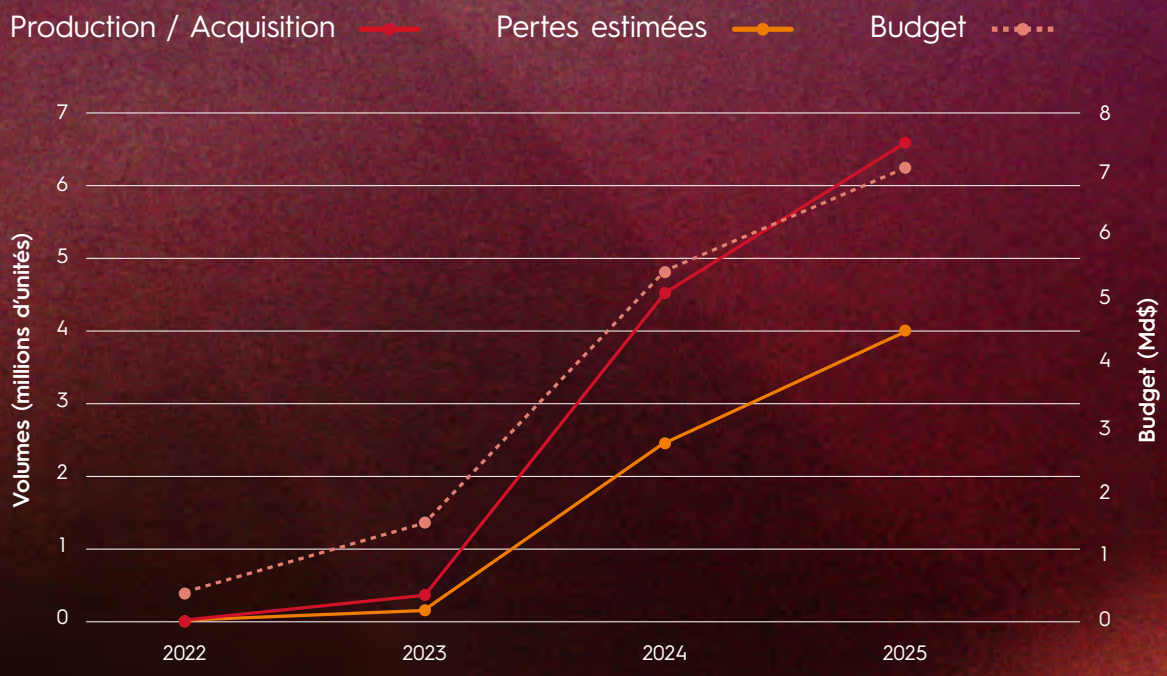
« La Readiness Roadmap 2030 de la Commission européenne prévoit un investissement prioritaire dans des capacités de frappes de précision par drones d'ici 2027. »

l'intégration de l'IA au sein de systèmes autonomes pour la vision, la navigation et la coordination de multiples vecteurs et groupes tactiques multi-milieux. Sopra Steria assure l'intégration des UxV avec son système **CRIMSON** multi-domaines et interopérable, basé sur une architecture ouverte et data-centrée sécurisée (DCS). De plus, CS Group a été retenu par l'AMIAD[47] pour le projet **PENDRAGON**, afin de fournir des composants de son C2 CRIMSON pour intégration au C2 PENDRAGON, et capitalise sur son implication dans des projets de robotique duaux, tels que le projet **CARMA** de développement de robots de réponse et de gestion de crise. Enfin, Sopra Steria travaille aux côtés d'organismes de recherche et d'industriels européens au projet **SENTINEL** sur l'optimisation des moyens énergétiques dans les camps militaires.

(47) Agence ministérielle pour l'Intelligence artificielle de défense.

PROGRESSION DES ACHATS, DE L'UTILISATION ET DES PERTES DE DRONES EN UKRAINE DE 2022 À 2025

Le drone est devenu depuis 2022 une munition consommable, qui structure intégralement l'économie militaire de son utilisateur. Les pertes mensuelles de drones en Ukraine dépassent désormais la production annuelle de la majorité des pays occidentaux, et le coût associé à ces pertes est négligeable comparé aux dégâts infligés à l'adversaire.



Source : Sopra Steria d'après IHEDN, US Army War College, Royal United Services Institute et presse

STRUCTURER LES NOUVEAUX MODÈLES **D'INNOVATION DE DÉFENSE**

TENDANCE 10.

La guerre en Ukraine a profondément transformé la manière de penser l'innovation militaire en Europe. Elle a mis en évidence les limites d'un modèle d'acquisition des armements construit pour des cycles de développement longs, parfois étalés sur vingt ans. Le retour d'expérience de ce conflit montre, au contraire, que la supériorité opérationnelle dépend désormais de la capacité à adapter en continu, parfois en quelques semaines, les équipements aux réalités du terrain. Les forces ukrainiennes modifient en permanence leurs dispositifs en fonction des contre-mesures adverses.

Cette dynamique impose aux armées et aux industriels de repenser leurs cycles de développement : il ne s'agit plus seulement de concevoir des plateformes majeures sur le temps long, mais de disposer d'une capacité industrielle capable d'intégrer en permanence les retours du champ de bataille et d'itérer rapidement. Or, les grands groupes de défense ont construit leur modèle autour de programmes complexes, longs, fortement planifiés et nécessitant des investissements colossaux.

Si cette organisation reste indispensable pour certains systèmes majeurs, elle apparaît moins adaptée à des technologies évoluant rapidement, notamment dans les domaines du logiciel, de l'intelligence artificielle, de l'autonomie ou de la guerre électronique. C'est dans cet espace que s'imposent de nouveaux entrants. Start-up, entreprises duales et acteurs du numérique introduisent des cycles courts, du prototypage rapide et une logique d'amélioration continue directement inspirée du monde de la tech. Des structures comme l'Agence de l'innovation de défense en France ou l'Innovation Board of Belgian Defence illustrent cette volonté d'accélérer et de structurer cet écosystème au sein des armées.

Cette transformation industrielle s'accompagne d'une mutation profonde des modes de financement. Longtemps dominé par la commande publique et les grands programmes étatiques, le secteur de la défense attire désormais de nouveaux investisseurs. Les fonds de capital-risque s'intéressent de plus en plus

aux technologies dites « dual-use », c'est-à-dire susceptibles d'avoir à la fois des applications civiles et militaires : intelligence artificielle, spatial, cybersécurité, robotique ou infrastructures de communication.

Autour des industriels historiques et des budgets nationaux se constitue progressivement un écosystème financier inédit associant investisseurs privés, fonds spécialisés, dispositifs européens[48] et parfois fonds souverains. Ce mouvement reflète une évolution plus large : la sécurité et la souveraineté technologique deviennent des enjeux stratégiques pour les États comme pour les investisseurs.

Au croisement de ces dynamiques se dessine un nouveau paysage pour l'innovation militaire européenne. Les grands programmes d'armement continueront de structurer la puissance militaire sur le temps long, mais ils devront désormais cohabiter avec des cycles d'innovation beaucoup plus courts. L'enjeu pour les États européens sera de réussir à articuler ces deux temporalités : préserver les capacités industrielles lourdes tout en permettant l'émergence d'un écosystème agile, capable de transformer rapidement les innovations technologiques en capacités opérationnelles.

Sopra Steria structure l'innovation de défense via ses dispositifs d'open innovation, en connectant start-up, industriels et acteurs publics pour accélérer l'identification et l'intégration de technologies dual-use. Son expertise en transformation digitale permet de passer rapidement du prototype au déploiement opérationnel dans des environnements complexes et souverains. En complément, ses initiatives en venture capital renforcent sa capacité à détecter, financer et accompagner les technologies stratégiques.

(48) La Tribune, mars 2026.

CONCLUSION

Agir pour préserver notre liberté d'action et garantir notre autonomie stratégique

Un basculement stratégique durable
La conflictualité s'installe dans la durée. Tous les conflits qui se déroulent sous nos yeux le prouvent. Hybride, multi-domaines, permanente, elle cible autant les capacités que la cohésion, la décision et la volonté de l'adversaire. La maîtrise des technologies clés et la résilience industrielle deviennent dès lors les fondements de la puissance.

Dix tendances, un même enjeu : la liberté d'action
Intelligence artificielle, quantique, cyber, lutte informationnelle et d'influence, espace, systèmes autonomes, défense intégrée, souveraineté des données, réarmement industriel… Ces dynamiques ne sont pas isolées : elles convergent vers un objectif unique — conserver l'initiative et la supériorité dans tous les milieux.

Trois leviers indissociables :

↘ **Surveiller et digérer la saturation :** maîtriser la connaissance de la situation dans tous les milieux, du spatial au cyber, en passant par les réseaux d'information, grâce au SSA, aux architectures C2 et à la fusion des données ;

↘ **Agir plus vite que l'adversaire :** simuler pour anticiper et solidifier en modélisant les engagements, en confrontant les modes d'action amis et adverses, en révélant les points de rupture et en testant la résilience des systèmes. La simulation devient un outil clé pour s'entraîner, décider et préparer les opérations avant qu'elles ne se produisent. Exploiter pleinement l'intelligence artificielle, les data spaces et, demain, les technologies quantiques pour accélérer la décision et conserver l'initiative ;

↘ **Construire et régénérer dans la durée :** réindustrialiser, produire à l'échelle, raccourcir les cycles d'innovation et reconstituer une profondeur industrielle et logistique adaptée aux conflits de haute intensité.

C'est bien la combinaison de ces trois leviers qui conditionne l'efficacité militaire et la crédibilité stratégique.

Par ailleurs, la question de la souveraineté et de l'autonomie stratégique européenne comme impératif opérationnel est majeure. Dépendances technologiques, fragilité des chaînes d'approvisionnement, pression informationnelle : chaque vulnérabilité peut être exploitée. L'autonomie stratégique n'est plus un horizon, c'est une exigence immédiate et chaque décision souveraine la façonne.

Dans ce contexte en tension et aux développements incertains, Sopra Steria est un partenaire au cœur de la supériorité informationnelle, technologique et opérationnelle européenne :

- ↘ Un acteur européen indépendant et de référence, engagé au service des forces armées, de la sécurité et du spatial ;
- ↘ Un industriel de défense d'un nouveau genre, acteur hybride – industriel du secteur et ESN – au sein de la Base industrielle et technologique de défense, de l'espace et de la sécurité européenne, qui conçoit des solutions, intègre des systèmes avec ses partenaires et relie données, plateformes et acteurs au cœur de l'interopérabilité.
- ↘ Un catalyseur de transformation opérationnelle, au croisement du C2, de l'IA, de la cybersécurité, du cloud souverain et des systèmes autonomes ;
- ↘ Un architecte de résilience, contribuant à sécuriser les infrastructures critiques, protéger l'information et garantir la continuité des opérations ;
- ↘ Un partenaire de confiance, ancré dans les écosystèmes nationaux et européens, au service de l'autonomie stratégique, capable de faire émerger, structurer et accélérer les acteurs innovants.

Mais il est nécessaire d'agir maintenant :

↘ **Anticiper plutôt que subir :** identifier dès aujourd'hui les ruptures technologiques et leurs impacts opérationnels ;

↘ **Accélérer la transformation au cœur de l'interopérabilité :** moderniser les systèmes, intégrer l'IA, sécuriser les architectures et préparer le post-quantique ;

↘ **Renforcer la résilience :** protéger les données, les infrastructures et les chaînes critiques ;

↘ **Construire des capacités souveraines :** réduire les dépendances et maîtriser les technologies clés.

« Avec Sopra Steria, transformez les ambitions stratégiques européennes en capacités opérationnelles. Dans un environnement de confrontation durable, l'avantage se construit dès maintenant. »


The world is how we shape it*
sopra steria
* Le monde est tel que nous le façonnons