The world is how we shape it

sopra steria

Vision paper Défense & Sécurité

Bâtir ensemble la défense & la sécurité européennes de demain

« Bâtir ensemble la défense et la sécurité européennes de demain » : sur la base de cette mission, Sopra Steria souhaite contribuer au façonnement d'une Europe plus forte, c'est-à-dire en mesure de faire face aux défis et aux dangers qui s'imposent à elle, plus protectrice et plus juste pour l'ensemble de ses citoyens, et souveraine pour défendre les fondements de nos démocraties.

Dans un monde pétri de tensions et d'incertitudes qui voit parallèlement l'avènement de nouvelles technologies de rupture, nous sommes bien plus qu'une ESN de la transformation numérique dans le secteur Espace, Défense & Sécurité. Nous sommes un acteur majeur qui aide à répondre aux grands enjeux sécuritaires d'aujourd'hui et de demain. Adressant les ministères régaliens des Armées, de l'Intérieur et de la Justice et présent dans plus de 14 pays européens, notre position est celle d'un **industriel du numérique Défense & Sécurité souverain et européen**. Nous proposons à nos clients des offres complètes en tirant parti de l'innovation dans le numérique et les domaines métiers. En France, près de 1 000 collaborateurs contribuent déjà au renforcement de la sécurité des biens, des personnes et du territoire national et européen tout en répondant aux enjeux de souveraineté, de confiance et d'éthique.

Ce document part d'un constat : le monde est en plein bouleversement et grâce à notre expertise dans les technologies de rupture, les systèmes critiques et nos savoir-faire métiers dans de nombreux domaines, nous préparons les armées, les forces de sécurité intérieure et la Justice à répondre aux défis auxquels elles font face.

Par ce vision paper, nous réaffirmons notre engagement et notre contribution à la défense et à la sécurité européennes, présentes et futures. Forts de nos atouts, nous anticipons le monde de demain et nous le construisons avec les acteurs défense et sécurité, en étant conscients des risques qui pèsent sur l'Europe et au-delà, tout en ayant pleinement confiance en l'avenir.

Laurent GIOVACHINI
Directeur Général Adjoint Sopra Steria

[1] Sécurité publique & identité, command and control, cyberdéfense, maintenance et logistique, soutien général aux opérations et spatial militaire.

Sommaire

01. 5 - 6

Accompagner les transformations technologiques de la Défense pour faire face à un monde en plein bouleversement

02. 7 - 10

Maîtriser le multi-milieux, multi-champs (M2MC) et accélérer la transformation numérique du secteur de la Défense et de la Sécurité

03. 11 - 12

Les fondements de notre vision

04. 13 - 15

Nos trois piliers au service de nos clients

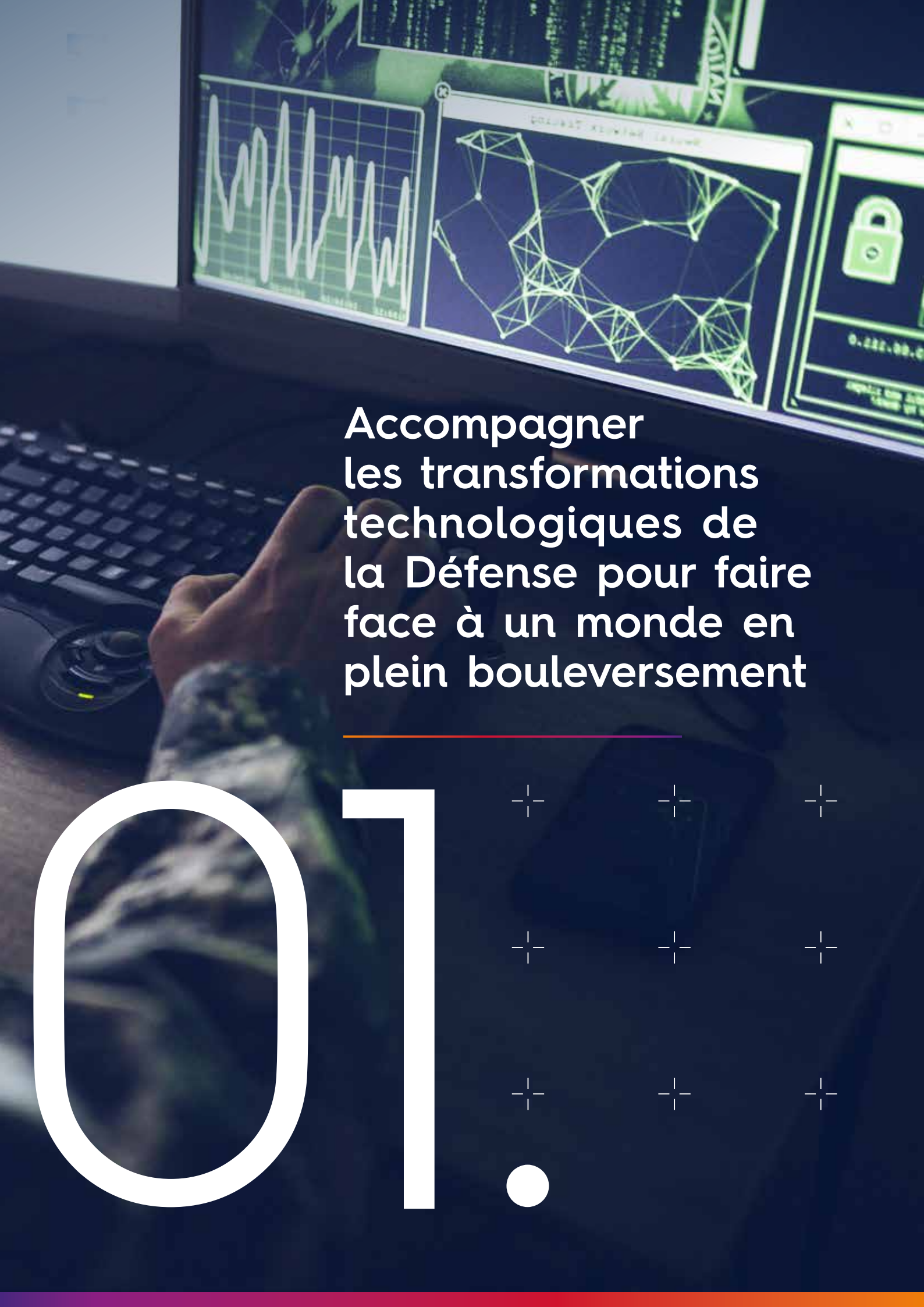
05. 16 - 17

Les nouvelles technologies au service de la Défense et de la Sécurité

- Intelligence artificielle 18 - 23
- Quantique 24 - 29
- Cloud souverain de combat 30 - 31
- Jumeaux numérique 32 - 36
- Réalité étendue 37 - 38

06. 39 - 40

Nous bâtissons avec nos partenaires la défense et la sécurité européennes de demain



Accompagner les transformations technologiques de la Défense pour faire face à un monde en plein bouleversement

01.

Nous passons de l'ère des crises à l'ère des chocs

L'amiral Vandier, major général des armées, indiquait récemment que nous quittons l'ère des crises pour entrer dans celle des chocs marqués par des environnements nouveaux et plus que jamais incertains[2]. Le monde est en effet confronté au renouveau de compétitions stratégiques dans tous les domaines. De la zone indopacifique à l'Europe, en passant par l'Afrique et le Moyen-Orient, un arc de tension se constitue. En Europe, la guerre a fait un retour fracassant en février 2022. L'invasion de l'Ukraine est un glissement stratégique qui fait surgir de nombreuses notions : risque nucléaire, retour d'une stratégie globale et d'actions hybrides, conflit de haute intensité, retour de la guerre symétrique multi-milieux et multi-champs, utilisation de technologies duales comme la constellation de satellites Starlink, utilisation de l'intelligence artificielle, et enfin « dronisation » du champ de bataille.

L'attaque du Hamas contre Israël révèle quant à elle les grands traits de la guerre dite « asymétrique » et l'importance cruciale du renseignement. Elle prouve que le rapport du faible au fort est en mesure de changer grâce à l'appui d'États tiers, souvent tapis dans l'ombre : opérations terrestres, maritimes et aériennes simultanées et minutieusement préparées depuis des mois, tirs de roquettes, infiltration de combattants par les airs, etc.

Enfin, et ce n'est pas le moindre des problèmes, le dérèglement climatique a des conséquences géopolitiques majeures avec les déplacements de populations, le risque de disparition d'États, les crises alimentaires, l'instabilité et la sécurité internationale, le terrorisme, la criminalité internationale, l'intensification des crises migratoires et les ruptures dans les chaînes d'approvisionnement.

Affronter le présent et préparer le futur

Tous ces bouleversements ont des conséquences capitales pour nos clients. La pandémie de Covid-19 comme la guerre en Ukraine et les tensions internationales ont provoqué des changements majeurs. Dès le mois d'avril 2022, la croissance de l'industrie a marqué le pas, principalement en raison de la guerre en Ukraine et des mesures de confinement en Chine. Dès lors, sont apparues de fortes tensions sur les approvisionnements en Europe. De plus, la guerre en Ukraine et la crise de l'énergie qui a suivi ont mis en lumière le double phénomène de dépendance à la Russie pour le gaz et donc de l'électricité produite par ce biais, et d'interdépendance très forte entre les différents acteurs. Les chaînes d'approvisionnement ne parviennent pas à tenir la cadence imposée par les grands groupes. Safran a, par exemple, connu des problèmes avec ses sous-traitants qui lui fournissent 65% des pièces qui entrent dans la fabrication des moteurs Leap fabriqués par CFM, société commune entre GE et Safran.

Pour l'Union européenne, la guerre en Ukraine confirme sa grande dépendance vis-à-vis de la Chine notamment pour ce qui concerne les matières premières critiques et les terres rares. Les bouleversements provoqués par les crises et les chocs ne sont pas seulement matériels. Ils touchent aussi l'organisation et le personnel, les forces morales et la lutte informationnelle, le maintien en condition opérationnelle des matériels, la sécurité des réseaux et la protection des données. Or, toutes les organisations n'ont pas les moyens humains ou technologiques d'affronter ces difficultés. Y faire face aujourd'hui, tout en préparant le futur, est la mission que Sopra Steria s'est fixée pour tous les acteurs du monde de la défense (entreprises, industries, ministères, organisations internationales telles l'OTAN, l'Union européenne). Le renouvellement de leur confiance est gage de notre réussite.

[2] Discours d'ouverture du CEMM lors du colloque « Naval de défense », salon Euronaval 2022.

Maîtriser le multi-milieux, multi-champs (M2MC) et accélérer la transformation numérique du secteur de la défense et de la sécurité

02.

Sopra Steria est un acteur mondial de la transformation numérique et un membre actif de la BITD européenne, fort de plus de 40 ans d'expérience dans le secteur Défense & Sécurité. Nous avons une très bonne maîtrise et connaissance du secteur et des marchés de nos clients, quels qu'ils soient (ministère des Armées, Union européenne, OTAN). C'est un atout capital pour les aider à faire face aux nouveaux enjeux qui apparaissent.

Maîtriser le multi-milieux – multi-champs

L'ÉLARGISSEMENT DU SPECTRE DES DOMAINES

Le contexte international est marqué par de fortes tensions. Des conflits entre acteurs régionaux soutenus par des puissances plus importantes émergent. Pour sa part, la guerre en Ukraine illustre la réapparition de la guerre interétatique et des engagements symétriques. Les espaces ou champs conflictuels ont changé, ils se sont agrandis pour englober désormais le champ immatériel et les espaces dans lesquels les règles n'étaient pas ou insuffisamment définies (haute mer et espace). Il ne s'agit plus seulement de la terre, de la mer et des airs. Les conflits se jouent aussi dans le cyberespace, l'espace et dans les champs informationnel et électromagnétique. C'est le multi-milieux – multi-champs (M2MC) appelé aussi multidomaines aux États-Unis.

Les opérations multi-milieux – multi-champs nécessitent l'intégration et la synergie des nouveaux domaines du combat (informationnel, cyber et spatial) dans les opérations interarmes et interarmées (terre, mer et air) avec une boucle décisionnelle plus rapide « afin de surprendre, saturer ou déstructurer l'adversaire[3]. » Dans ce contexte, les technologies numériques jouent un rôle majeur avec notamment le cloud, l'intelligence artificielle, la réalité étendue et bientôt les technologies quantiques.

CYBERESPACE ET L2I

Un grand nombre d'activités sont présentes dans le cyberespace. Ce domaine attise toutes les convoitises : espionnage, criminalité, sabotage, influence. Au cours des dernières années, les cyberattaques se sont multipliées, contre les hôpitaux, des industries de défense stratégiques, des institutions publiques sans qu'il soit possible d'en repérer les auteurs. En France, entre janvier 2022 et juin 2023, l'ANSSI a traité en moyenne 10 attaques par mois concernant une collectivité territoriale, cela se traduit par 42 départements touchés sur 101 et 12 régions attaquées sur 18.

Face à ces menaces la lutte informatique d'influence (L2I), qui offre de multiples modes d'action efficaces, a pris également une place très importante dans les modes d'action de nos adversaires, avec des actions hostiles menées à l'encontre de nos intérêts, que ce soit sur certains théâtres d'opérations (notamment le Sahel) ou sur le territoire national. La L2I qui désigne les opérations militaires conduites dans le domaine informationnel au sein du cyberespace, vise à détecter, caractériser, identifier et réagir face à ces attaques massives et variées.

[3] Étienne Faury, « Les opérations multidomaines : une révolution militaire », Revue Défense Nationale, 2020 : chocs stratégiques - Regards du CHEM - 69e session.

ESPACE ET TRÈS HAUTE ALTITUDE

• **Espace** : « L'enjeu spatial est fondamental si l'on veut rester dans le club des nations en capacités de conserver des moyens de renseignements ou d'observations souverains » a indiqué le ministre des Armées, Sébastien Lecornu[4]. Observation, renseignement, communication, protection des intérêts nationaux, prévention des risques environnementaux, etc., l'espace joue aujourd'hui un rôle incontournable pour la défense et la sécurité intérieure et civile. En conséquence, ce lieu stratégique devient une zone de tensions et d'enjeux majeurs. Le spectre des actions envisageables est large : brouillage, prise de contrôle voire destruction de satellite, etc., l'espace reflète les perturbations géostratégiques terrestres.

• **Très Haute Altitude** : Entre espace et ciel, l'espace aérien supérieur (EAS), situé entre 20 et 100 kilomètres, est devenu un nouvel enjeu de défense[5]. Cette tranche d'altitude se peuple progressivement de nouveaux objets qui répondent à des besoins très différents, à la fois civils et militaires, tels que les aéronefs suborbitaux, les ballons stratosphériques ou les planeurs hypersoniques. Face aux évolutions majeures, il apparait nécessaire de mettre en place une coopération entre tous les acteurs afin de garantir une utilisation sûre, responsable et équitable de cet espace.

ESPACES MARITIMES ET FONDS MARINS

• **Espaces maritimes** : La France est le deuxième espace maritime mondial avec 11 millions Km^2 d'espace maritime. La Marine nationale y défend les intérêts de la France et y préserve la paix via cinq grandes missions : renseignement, prévention des risques, intervention en zones de conflit, protection des mers et des océans et assistance aux navires, dissuasion grâce à ses SNLE[6].

• **Fonds marins** : Longtemps inaccessibles, ils constituent aujourd'hui un milieu d'intérêt stratégique. L'arrivée de nouveaux drones sous-marins capables de mener des missions militaires transforme ces fonds en nouveaux espaces de conflictualité. En effet, à l'heure des difficultés d'approvisionnement en métaux rares et gaz naturel, les grands fonds marins peuvent désormais susciter un fort intérêt, notamment pour le gaz, les hydrocarbures et le lithium. Enfin, la protection de la biodiversité reste une mission cruciale pour la France et les nations « ultra-marines ». Par ailleurs les câbles sous-marins de communication représentent un enjeu crucial pour le transport de flux d'informations. L'ANSSI souligne d'ailleurs qu'ils forment « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques[7]. » Aujourd'hui, plus de 95% des communications mondiales transitent par les câbles sous-marins.

[4] Objectifs LPM 2024-2030 : maîtriser les nouveaux espaces de conflictualité | Ministère des Armées (defense.gouv.fr).

[5] Agnès d'Heilly, directrice des affaires publiques, Ariane Group, lors du colloque Du ciel à l'espace, nouveaux enjeux opérationnels à très haute altitude, École militaire, janvier 2023.

[6] Les missions de la Marine : Missions et organisation / Marine Nationale - www.lamarinerecrute.fr

[7] ANSSI 2011, rapport Défense et sécurité des systèmes d'information Stratégie de la France (Consulté le 05/04/2022.

Accélérer la transformation numérique du secteur de la défense et sécurité

Atteindre les objectifs capacitaires pour répondre aux nombreux défis auxquels sont confrontés nos clients ne peut se faire sans une transformation numérique au long court. C'est l'enjeu de ce niveau opérationnel. Cela concerne les systèmes d'information et de communication des armées en opérations, mais aussi la cybersécurité, la maîtrise et la protection des données l'interopérabilité interarmes, interarmées et interalliées.

Cette transformation numérique ne se résume pas à la seule Défense. La numérisation du ministère de l'Intérieur constitue un défi majeur. En France, la Loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) traduit la nécessité d'investir dans le domaine technologique et la transformation numérique. Cela signifie une meilleure prise en compte du numérique dans les politiques publiques et il garantit la préparation des grands événements sportifs (renforcement de la cybersécurité), la facilitation du quotidien des usagers du service public (refonte des parcours de plaintes, identité numérique), la transformation des modes de travail numériques (proximité des forces de l'ordre avec la population dans l'espace public).

DES SOLUTIONS POUR LA SÉCURITÉ CIVILE

En Allemagne, Sopra Steria a développé la solution IGNIS-Plus spécifiquement pour les services d'incendie et de secours. L'évolutivité et la grande adaptabilité du système constituent la base d'applications possibles dans l'ensemble du secteur des autorités et des organisations ayant des tâches de sécurité ainsi que des pompiers d'usine. IGNIS-Plus est utilisée avec succès par différents centres de lutte contre l'incendie et de secours dans plusieurs régions métropolitaine et agglomérations allemandes en tant que système de contrôle des opérations et garantit une fiabilité maximale, même en cas de pics de charge élevés. En tant que combinaison logicielle et matérielle, IGNIS-Plus répond aux diverses exigences et permet d'obtenir les temps de réponse rapides nécessaires à l'ensemble de la gestion du déploiement des opérations.

La numérisation de la justice doit aussi permettre plus d'efficacité en simplifiant les procédures et en développant la collaboration entre tous les acteurs notamment de la chaîne pénale. Magistrats et acteurs de la justice doivent disposer d'outils performants, les justiciables doivent avoir la possibilité de déposer des demandes d'aide juridictionnelle et de saisir la justice et de suivre leurs affaires en ligne. D'autre part, l'orientation des détenus doit être facilitée. Enfin, les mineurs pris en charge par la protection judiciaire de la jeunesse doivent être suivis plus efficacement.

Les fondements de notre vision prospective : innovation et mutualisation des expertises

03.

La vision prospective : intégrer l'incertitude

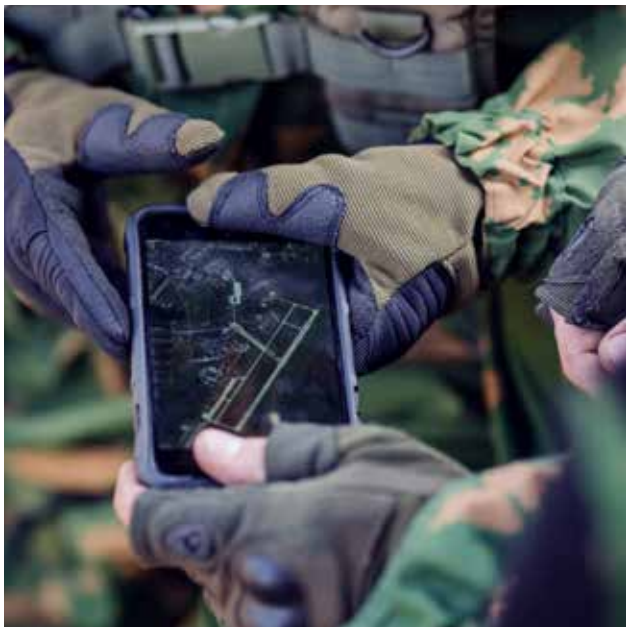
« Demain ne sera pas comme hier. Il sera nouveau et dépendra de nous. Il est moins à découvrir qu'à inventer. » Sopra Steria souscrit pleinement à l'assertion de Gaston Berger, l'inventeur du terme « prospective ».

Pour consolider leur capacité d'innovation, leur processus métiers et la résilience de leur organisation, nos clients doivent élaborer des stratégies solides. Pour cela, ils doivent analyser le monde tel qu'il est, c'est-à-dire pétri d'incertitudes et de ruptures, mais aussi préparer le futur grâce à la prospective.

L'innovation : une démarche d'ensemble pour intégrer les technologies de rupture

L'environnement défense et sécurité de plus en plus complexe nécessite une vue d'ensemble et une démarche d'innovation technologique forte pour une adaptation constante des services aux contraintes évolutives caractéristiques de ce secteur stratégique. Dans ce contexte, deux grandes technologies s'imposent : l'intelligence artificielle et le quantique.

Nos clients pensent que l'IA sera incontournable dans le futur. Ils ont raison. L'IA est moins associée aux robots futuristes qu'aux outils de productivité, de prédiction (maintenance avec la convergence des IoT et de l'IA mais aussi grâce au métaverse et aux jumeaux numériques), d'aide à la décision (combat collaboratif) avec l'intelligence augmentée, d'amélioration des conditions de vie et de travail, de gestion, etc... Nous aidons nos clients à gérer les défis liés à l'introduction de l'IA dans leur organisation. De la même manière, « Les technologies quantiques sont à un moment charnière », souligne le physicien Julien Bobroff. Ces technologies quantiques ne se résument pas à la cyberdéfense (attaque et défense) et aux réseaux de communication ou à la cryptographie. Elles couvrent en réalité un bien plus large spectre de domaines défense. Le quantique concerne trois grands domaines d'applications : la cryptographie, les capteurs et l'ordinateur (optimisation et simulation). Dans ces trois segments, des applications défense sont possibles : spatial militaire et télécommunication, localisation ou furtivité des sous-marins, détection d'armes chimiques et biologiques, santé, nouveaux matériaux, etc.



L'accompagnement et la mutualisation des expertises

Sopra Steria accompagne ses clients sur le terrain pour leur proposer des solutions globales et un service optimal, porteurs d'innovations technologiques.

Les organisations - gouvernements, ministères et organismes privés - sont aujourd'hui confrontées à des défis multiples en termes de défense et de sécurité. Un meilleur contrôle des données et des informations est primordial pour minimiser les risques et assurer une autonomie numérique stratégique et puissante.

Chez Sopra Steria, nous sommes convaincus que mutualiser les expertises et les informations permet d'être plus efficient et de garantir la sécurité des personnes et des données.

Nos trois piliers au service de nos clients

04.

Être un Tiers de confiance au cœur de l'innovation

Qu'est-ce qu'être un Tiers de confiance quand on est une entreprise de la Tech européenne et souveraine ? C'est porter les enjeux de la confiance politique (Sopra Steria est tourné vers le service des intérêts des États et des entreprises critiques européennes), de la confiance numérique (sécurité) et de la confiance économique (les technologies critiques doivent rester européennes).

Dans un monde de plus en plus complexe et tendu, autant que dans un univers économique de plus en plus concurrentiel caractérisé par une clientèle informée et exigeante, innover c'est conserver une supériorité technologique sur les adversaires de la France et de l'Union européenne, garantir notre sécurité, et garder une longueur d'avance sur les concurrents.

Sopra Steria imagine avec ses clients des solutions sur mesure mettant le numérique au service de l'humain. La relation que nous entretenons avec nos clients repose depuis plus de 40 ans sur la confiance et la fiabilité.

S'engager dans la technologie éthique

Intelligence artificielle, cloud, quantique, métaverse industriel, impression 3D, etc., notre monde est entré dans une nouvelle phase d'accélération technologique qui offre plus d'efficience dans la production et l'organisation pour les industriels. Pour les armées, les forces de l'ordre et le personnel du ministère de la Justice, les technologies offrent l'efficacité opérationnelle, l'accessibilité et la transparence.

Cette numérisation pose néanmoins de nombreuses questions : données personnelles, transparence des plateformes, traçabilité des algorithmes, place de l'homme dans la décision, etc. Comment dès lors imaginer demain, la digitalisation de notre économie, de notre vie sociale, de nos comportements privés ou professionnels, de nos armées et des pouvoirs publics, sans tenir compte d'un cadre éthique ? Le développement économique des entreprises, comme le déploiement opérationnel des armées et des forces de l'ordre mais aussi la numérisation de la Justice, ne peut plus se construire sans prendre en compte les impacts sociaux et environnementaux.

« L'éthique du numérique englobe l'ensemble des principes et valeurs qui s'appliquent à la conception, la réalisation, la commercialisation, la promotion, l'exploitation et la prise en compte ainsi que la gestion de l'ensemble des effets induits par les technologies numériques et de leurs éléments constitutifs ou nécessaires à leur fonctionnement. Sont notamment visés les impacts sociaux et environnementaux, la protection des données personnelles et du libre arbitre des individus, le principe de non-discrimination. Ni béquille, ni étape supplémentaire, elle s'impose comme un moyen de l'action, comme un ciment de la confiance[8]. »

Sopra Steria s'engage sur l'éthique numérique afin de promouvoir des stratégies de transformation digitale responsables, humaines et durables. Nous avons par ailleurs créé un Concours d'éloquence sur l'éthique numérique et lancé un prix de l'entreprise éthique. Mais au-delà de ces aspects officiels, nous intégrons l'éthique numérique dans chaque étape de la transformation, que ce soit dans le conseil ou l'intégration.

> Si une approche éthique n'est pas adoptée, les entreprises peuvent en effet, et par mégarde, s'exposer à plus de risques que d'avantages. Elles peuvent ne pas suffisamment identifier et mettre en œuvre les bons garde-fous pour gérer ou atténuer ces risques.
>
> **Kevin Macnish**
> Consulting Manager in Digital Ethics, Sopra Steria UK

[8] Floran Vadillo, Directeur conseil, Éthique & Souveraineté, Éthique numérique : quels choix pour une action dans la confiance ? L'Exploratoire, Sopra Steria Next.

Être un acteur souverain au service de clients partout en Europe

Sopra Steria est un acteur français, souverain, au cœur de l'Union européenne et au service de clients basés dans quatorze pays qui nous font confiance dans des domaines variés. Or, dans une époque post-Covid marquée par la guerre en Ukraine et de vives tensions internationales, la question de la souveraineté est redevenue un enjeu majeur. Nous disposons ainsi d'un positionnement unique d'industriel du numérique au cœur de la BITD européenne.

> Nous voyons le futur cloud de combat comme un réseau maillé, global, pour la redistribution des données et le partage de l'information aux niveaux stratégique, opératif et tactique. Le cloud est un accélérateur et un vecteur de transformations et d'efficience opérationnelles mais aussi logistiques.
>
> **Hugues Valentin**
> Cloud Center of Excellence, Sopra Steria

05.

Les nouvelles technologies au service de la défense et de la sécurité

Sopra Steria est un partenaire de référence de la souveraineté numérique. En travaillant avec une vision long terme au profit des ministères régaliens, en France et en Europe, nous sommes reconnus dans la transformation et pour nos offres industrielles sur les six grands domaines métiers :

• **Opérations & Soutien général** : combats asymétriques, retour du conflit de haute intensité, nos armées sont confrontées à des menaces multiformes. Le cloud souverain de combat est un outil indispensable pour les préparer en toutes circonstances et dans différents types d'affrontements. Le cloud, c'est également le Soutien général avec le travail des ressources humaines et le paiement des soldes, en France mais aussi au Royaume-Uni.

• **Command & Control** : un ensemble d'attributs et de processus organisationnels et techniques utilisant des ressources humaines, physiques et informationnelles permettent d'accomplir des missions, d'exécuter des tâches (C2) et de rendre compte.

• **Cyberdéfense** : le cyberspace est complexe et comprend plusieurs domaines dont la lutte informationnelle, la cryptographie post-quantique et la cybersécurité des systèmes, et de l'intelligence artificielle.

• **Sécurité publique & identité** : l'État, via ses ministères de l'Intérieur et de la Justice est garant de l'ordre public et de la sécurité visant à protéger la population et à lui garantir une justice équitable, transparente et efficace.

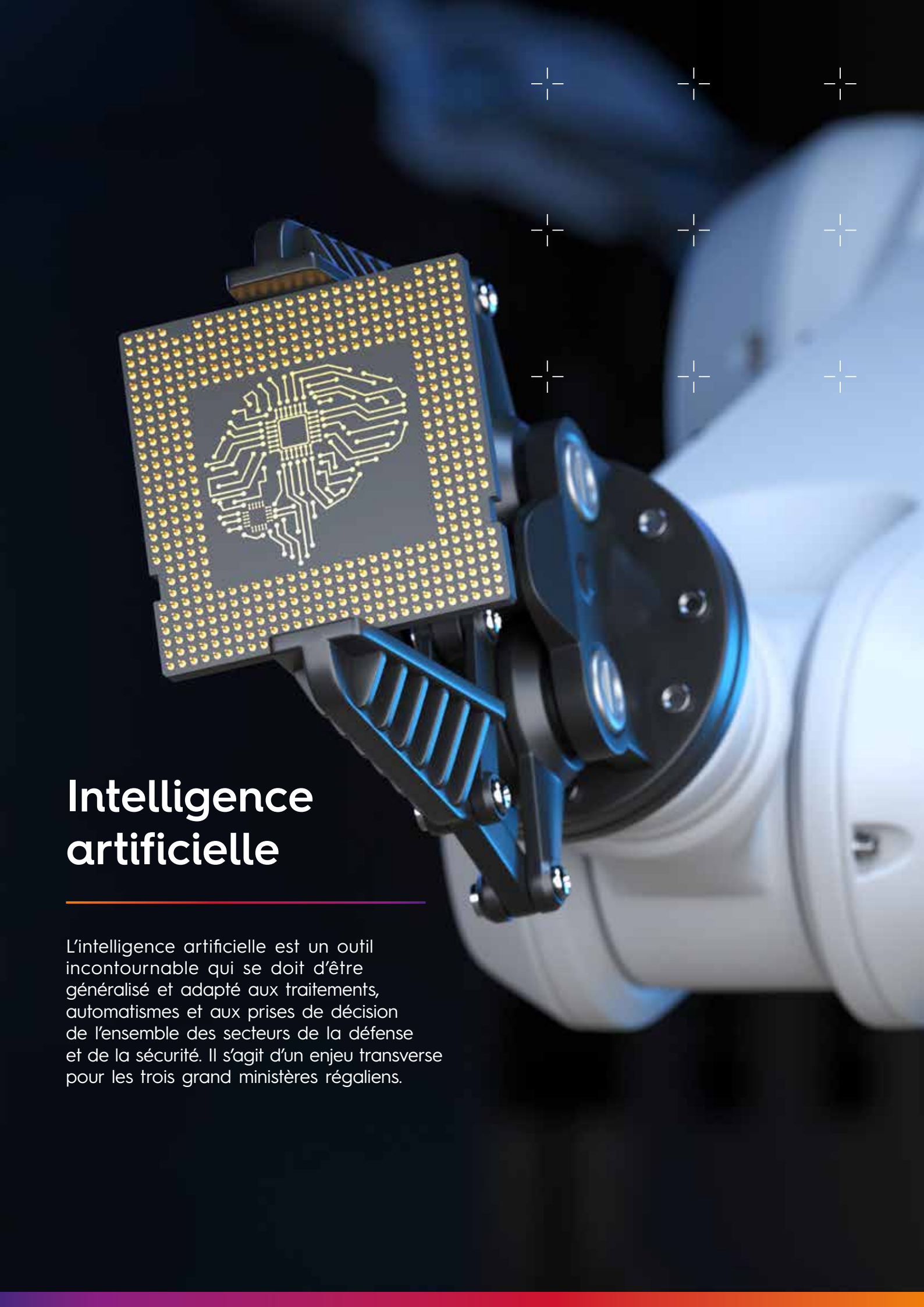
• **Maintenance & logistique** : l'efficacité opérationnelle des forces est conditionnée par l'efficience et la qualité des soutiens comme le maintien en condition opérationnelle et la logistique.

• **Spatial militaire** : par spatial militaire, nous entendons d'abord les opérations et les « combats » orbitaux, c'est-à-dire des actions passives et actives menées par un État dans l'espace pour garantir l'intégrité des capacités et des services spatiaux nationaux et pour conserver sa liberté d'action dans ce milieu. La guerre spatiale inclut également des actions sur les systèmes au sol (station de réception, système de commandement et de contrôle, etc.).

Intégration multi-milieux – multi-champs : les technologies dans les domaines métier

Cyber défense	Soutien général aux opérations	Maintenance & logistique	Command & Control	Sécurité publique & identité	Spatial militaire
IA	Cloud de confiance	Quantique	IA	IA	Quantique
Quantique	Jumeau numérique	Jumeau numérique	Quantique	Jumeau numérique	IA
Jumeau numérique	IA	IA	Jumeau numérique	Cloud de confiance	Jumeau numérique
	Réalité étendue		Réalité étendue	Réalité étendue	

L'environnement Défense & Sécurité dans un contexte multi-milieux – multi-champs nécessite une excellente adéquation entre les technologies que nous maîtrisons et les domaines métier pour lesquelles nous sommes reconnus. Notre vue d'ensemble et nos savoir-faire permettent à nos partenaires de s'adapter aux contraintes en constante évolution de la défense et de la sécurité.



Intelligence artificielle

L'intelligence artificielle est un outil incontournable qui se doit d'être généralisé et adapté aux traitements, automatismes et aux prises de décision de l'ensemble des secteurs de la défense et de la sécurité. Il s'agit d'un enjeu transverse pour les trois grand ministères régaliens.

Command & Control

Le numérique irrigue totalement les concepts de Command & Control des opérations militaires. Parallèlement, l'intelligence artificielle est devenue incontournable au sein des armées. La guerre en Ukraine a ouvert une fenêtre sur l'IA appliquée au niveau tactique qui s'étendra aux commandements des niveaux opératifs et stratégiques qui doivent détenir une vision la plus réaliste possible du théâtre d'opérations pour élaborer les ordres, selon la bonne temporalité. Avoir une vision réaliste est une chose. L'obtenir au meilleur moment et de manière la plus exhaustive possible pour bien comprendre le contexte et surtout pouvoir s'assurer de la véracité des informations en est une autre.

Dans ce contexte, la maîtrise de l'IA offre un avantage déterminant aux combattants.

« Car aujourd'hui, face à des ennemis et des dangers multiformes qui frappent sans distinction civils et militaires, dans un environnement multidomaines complexe et dual, le C2 doit permettre de s'assurer et de conserver l'initiative et l'avantage informationnel et donc décisionnel sur l'ennemi. Cela exige des progrès dans les technologies et une adaptation de l'IA.[9] »

En 2021, Sopra Steria et CS ont pris une part essentielle dans la fourniture d'une solution de protection des sites militaires sensibles qui devrait équiper 28 emprises à l'horizon 2025, réparties entre l'armée de l'Air et de l'Espace et la Marine nationale. Cette solution innovante jette les prémices de ce que devraient être les solutions de protection multidomaines car elle fédère les composantes « sûreté » (actions malveillantes depuis l'extérieur) et « sécurité » (accidents au sein de l'emprise) autour d'un système C2 unique. Conçu par CS, CRIMSON devrait être le socle des futures solutions de Sopra Steria s'agissant des opérations multidomaines. L'ambition de cette offre est de permettre aux Armées d'obtenir et de maintenir la supériorité informationnelle. Cette dernière est la clef de la réussite pour les opérations.

CS travaille ainsi sur un projet innovant avec de nouvelles approches d'intelligence artificielle pour la détection et l'identification automatique de menaces positionnées sur la frange côtière et la lutte anti-drones, à la rupture de milieu mer-terre. Ce projet (TIAMAT) complète l'offre globale de CS pour la surveillance et la protection maritime couvrant un espace étendu, depuis les zones portuaires jusqu'aux limites de la zone économique exclusive (ZEE). Grâce au projet TIAMAT, CS propose des solutions algorithmiques basées sur l'intelligence artificielle pour l'aide à la décision en milieu maritime.

VISION SSG

Dans ce contexte, et forts du succès de nos programmes CRIMSON et rAIse[10] (centré sur l'IA), notre vision repose sur la compréhension de l'IA, pas seulement comme une finalité, mais aussi comme un formidable outil d'ingénierie. Renforcé par CS, Sopra Steria s'inscrit totalement dans ce schéma global d'IA défense et sécurité, en témoigne le programme CRIMSON dans lequel l'intelligence artificielle est en cours d'intégration.

Notre ambition est de déceler et collecter l'information utile et validée pour obtenir la supériorité informationnelle et aider le Commandement Stratégique ou tout autre centre de commandement militaire, civil ou dual, à prendre une décision en évitant la saturation cognitive.

À terme, l'objectif est bien de disposer d'une IA de confiance aux niveaux opératif et stratégique, c'est-à-dire décisionnel. La machine étant capable de produire des analyses erronées à partir de données erronées, l'IA de confiance est bien au cœur de nos préoccupations.

Plus globalement, nous imaginons un système d'opération nouvelle génération, robuste aux attaques cyber, groupé dans une constellation de systèmes de commandement et de contrôle, inter-opérant au sein d'un Cloud, adaptés à un domaine (opérations terrestres, opérations navales, lutte anti-drones, etc.) ou en couvrant plusieurs pour obtenir des résultats synchronisés. Ils seront multidomaines, renforcés et résilients grâce à l'intelligence artificielle.

« Nous sommes persuadés que de nouveaux algorithmes ultra puissants permettront de proposer des scénarios prospectifs pour les opérations extérieures, en suggérant par exemple l'itinéraire jugé optimal pour un convoi ou en proposant la meilleure zone de largage pour une opération aéroportée.[11] »

Grâce au LLM (Large Language Model ou grand modèle de langage), il sera possible de planifier, de réaliser les RETEX et de bâtir des scénarios grâce à la valorisation des connaissances des missions. On peut dès lors imaginer les avantages d'un système d'information des armées avec de l'intelligence artificielle générative pour la restitution du fantassin après une mission, par exemple, avec les possibilités de reporting et de notes. Associé à l'IA, le jumeau numérique améliorera les simulations et les analyses basées sur les RETEX et sur la prospective grâce à des représentations virtuelles dynamiques des missions en cours. Le C2 multidomaines ouvre en réalité une voie à explorer pour créer la double rupture, technologique et stratégique. Techniquement, cet outil est à portée de main et Sopra Steria et sa filiale CS se sont résolument engagés sur cette voie à la croisée de leurs domaines d'expertise.

[9] Philippe Loviconi, conseiller opérationnel, Protection multi-domaines.
[10] Lancé dès le 1er semestre 2023, rAIse est un grand programme interne d'adoption de l'intelligence artificielle générative. Il touche à la fois l'ensemble des forces de conseil métiers, les outils de développement internes et la stratégie de partenariats de Sopra Steria.
[11] Nicolas Martin, Sales Manager, Sopra Steria Group, Défense & Sécurité Commandement.

Cyberdéfense

Le cyberespace est bien le cinquième milieu du combat. Chez Sopra Steria, nous avons complètement intégré l'espace cyber dans les grands enjeux présents et futurs, en France comme en Europe. C'est notamment le cas en Allemagne, avec la Bundeswehr pour laquelle nous travaillons dans le domaine de la cybersécurité pour la disponibilité, la confidentialité et l'intégrité des données.

D'autre part, Sopra Steria et CS accompagnent un acteur dans le domaine du nucléaire pour la refonte complète de son système d'information de niveau Diffusion Restreinte. Ce système d'information ambitieux et innovant met en œuvre des innovations technologiques françaises comme la mise en place d'un cloud sécurisé et surtout l'utilisation d'un poste de travail durci bi-niveau. Ce poste de travail basé sur la solution SEDUCS UNIFYER, innovation de rupture conçue et développée par CS GROUP, permet sur un seul poste physique d'avoir deux environnements de sensibilités différentes tout en renforçant au quotidien le niveau de sécurité global du système d'information, en améliorant l'expérience utilisateur, tout en restant conforme aux exigences règlementaires.

La cybersécurité et la protection de la donnée sont au cœur de nos savoir-faire défense et sécurité. Ainsi, nous travaillons sur l'interopérabilité et l'interconnexion entre les armées et nous sommes convaincus que la DCS – Data Centric Security – contribuera à terme à réduire l'existence de nombreux réseaux pour ne constituer qu'un seul et unique réseau qui facilitera les échanges, le partage et la consommation de données avec une défense centrée sur les données optimale. Nous développons d'ailleurs une brique DCS répondant aux exigences des standards de l'OTAN.

VISION SSG

Dans ce contexte cyber en tension, l'intelligence artificielle est incontournable. Nous travaillons depuis trois ans sur l'IA de confiance, c'est-à-dire protégée contre les cyberattaques et respectueuse des règles éthiques (équité, vie privée, non-discrimination, etc.).

« Car l'intelligence artificielle est partout, dans les mains de tout le monde. Si elle n'est pas de confiance, cette technologie n'a aucune valeur.[12] » L'IA de confiance est la seule véritablement utilisable car elle guide nos actions. Les données d'apprentissage, les algorithmes et l'architecture doivent être transparents, sans biais. Notre vision repose sur des cas d'usage utiles qui renforce la sécurité des réseaux, des matériels et donc des personnes engagées. Sopra Steria est un membre actif du collectif français « Confiance.ai » qui conçoit et industrialise des systèmes à base d'intelligence artificielle de confiance et rassemble près de 50 partenaires incluant des industriels, des PME, des académiques et des start-ups. L'un de ses grands objectifs est précisément de proposer cet ensemble d'outils permettant non seulement de concevoir, mais également de valider, de certifier et d'expliquer. C'est l'objectif même de l'environnement de confiance que Sopra Steria fournit. Dépassant le cadre national, « Confiance.ai » collabore avec le consortium allemand conduit par VD pour réaliser un Memorandum of Cooperation qui vise à soutenir le règlement européen sur l'IA (AI Act) avec la création d'un label commun franco-allemand sur l'IA de confiance et responsable. Cette coopération ambitionne de fournir les lignes directrices et spécifications pour les applications d'IA et de préparer les écosystèmes à se mettre en ordre de marche en vue du respect de l'AI Act. Concrètement, ces acteurs clés en France et en Allemagne proposeront un référentiel commun sur l'IA de confiance. À terme, cela accélérera le time-to-market, notamment en faveur des PME et ETI qui disposeront de solutions qu'elles n'auraient pas pu développer toutes seules.

> La maitrise et les possibilités offertes par l'IA créent des capacités de supériorités militaires majeures. La question de l'autonomie stratégique et de la dépendance par rapport à des acteurs tiers est tout aussi importante que celle liée à l'autonomie dans le cadre de la dissuasion nucléaire.
>
> **Simon Marsol**
> European Business Coordination Defence & Security

[12] Jean-Luc Gibernon, Directeur développement, Campus Cyber, Sopra Steria.

Lutte informationnelle

« La grande force de Sopra Steria est de traiter le cyber dans l'infiniment grand et l'infiniment petit. Cela se traduit par exemple par la mise en place de centres opérationnels des sécurité cyber au profit de grands groupes industriels, qui nous confient leur sécurité mais aussi la réalisation d'outils spécifiques en série limitée. Dans ce cadre, le croisement des compétences entre experts du conseil et ingénieurs informatiques représente l'atout majeur et natif de Sopra Steria.[13] »

Acteurs du Pôle d'excellence cyber, nous avons contribué en mai dernier à la parution d'un document de référence sur la lutte contre la manipulation de l'information en collaboration avec le ministère des Armées, de multiples entreprises du numérique, des chercheurs et des enseignants et étudiants de grandes écoles. Jean-Yves Le Drian, ancien ministre de la Défense et ancien ministre de l'Europe et des Affaires étrangères rappelle que « l'espace informationnel est l'un des champs d'action privilégiés des puissances qui, dans le dessein de pousser leur avantage et de faire valoir leur propre modèle, entendent saper les fondements de nos sociétés démocratiques, entraver notre influence dans le monde et détruire les conditions mêmes de l'action collective internationale, pourtant indispensable face aux grands bouleversements écologiques, technologiques et humains du XXIe siècle.[14] »

Nous avons également créé un « cercle d'étude », embryon de think tank dénommé PEGASE, sur la lutte informationnelle avec pour objectif de contribuer à la résilience de la Nation dans ce domaine, de faire avancer la réflexion sur ce sujet (méthodes, menaces, expériences, perspectives). Ces réflexions permettront de générer des idées sur cette menace très actuelle, concevoir des outils, des techniques et des réponses technologiques et humaines pour faire face à ces défis majeurs.

Nous sommes également membre fondateur du conseil d'administration du campus cyber mis en place à l'initiative du président de la République et de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Nous sommes également membre actif de l'European Cyber Security Organisation (ESCO) depuis 2020 et nous contribuons enfin à la Chaire cyber de l'IHEDN (Institut des hautes études en défense nationale).

VISION SSG

Aujourd'hui, nous appréhendons la cybersécurité en termes de vulnérabilité des systèmes d'informations, de virus informatiques, d'espionnage et de cybercriminalité. Toutefois, l'omniprésence de la lutte informationnelle, associée à la lutte contre les manipulations de l'information et la lutte informatique d'influence (L2I) est devenue un enjeu majeur pour notre pays. En effet, des attaques informationnelles sont menées régulièrement pour dénigrer un État ou une entreprise mais aussi pour saper les fondements même de nos démocraties. Or, dans ce contexte, l'intelligence artificielle représente un risque notamment dans le cadre des *deep fakes*, mais elle est aussi un outil remarquable de lutte contre l'IA malveillante.

Sopra Steria a pour ambition de devenir un acteur de référence de la lutte informationnelle et de la L2I. Nous sommes persuadés que dans 10 ans, la lutte informationnelle aura l'importance de la cyberdéfense et de la cybersécurité aujourd'hui. Les travaux actuels en cybersécurité, notamment l'étude des modes opératoires des attaquants et leur identification, pourront être adaptés aux contraintes de la lutte informationnelle pour anticiper et identifier les attaques informationnelles mais aussi pour riposter. Par ailleurs, nous sommes convaincus que « le stockage intelligent », le tri et la valorisation de la donnée mais aussi l'automatisation des processus d'identification et de réponse constitueront autant d'atouts de premier plan pour faire face cette menace croissante. Dans le domaine spatial, par exemple, nous travaillons sur l'intégrité de la donnée tout en vérifiant qu'une donnée orbitale n'a pas été transformée à l'insu du capteur et/ou du système de traitement puis renvoyé comme une donnée réelle métier vers un système C2 ou décisionnel stratégique.

Sopra Steria Benelux joue un rôle crucial dans le secteur de la défense et de la sécurité en fournissant des solutions innovantes et des services spécialisés. Ses activités englobent divers domaines stratégiques, contribuant ainsi à renforcer les capacités opérationnelles et la résilience des institutions gouvernementales et des forces de sécurité.

Didier Gilbert

Aerospace, Defense & Security Business Unit Director

[13] Bruno Courtois, conseiller Défense et Cyber, Sopra Steria.

[14] La lutte contre les manipulations de l'information (pole-excellence-cyber.org)

Sécurité publique

Les nouvelles technologies, comme l'intelligence artificielle et la data transforment les services de sécurité. Ils jouent également un rôle de plus en plus prégnant au sein du ministère de la Justice. Ce dernier s'est d'ailleurs engagé dans un plan sans précédent de transformation digitale, ce qui aura pour conséquence un changement profond de ses modes de fonctionnement. Nous travaillons d'ores et déjà sur la Procédure pénale numérique dans la perspective d'une dématérialisation imminente des procédures civiles occasionnant une évolution profonde des systèmes d'information de l'administration pénitentiaire et de la protection judiciaire de la jeunesse.

Au sein des forces de l'ordre, dans lesquelles la technologie s'intègre déjà :

« la proximité reste la clef et les technologies permettent de répondre à l'enjeu de sécurité. Par ailleurs, celui-ci n'est plus seulement national, mais européen, avec l'interopérabilité entre les différents pays, la réglementation européenne, etc. Or, Sopra Steria opère déjà des systèmes d'information interopérables en France et en Europe, avec notamment le contrôle aux frontières.[15]».

Cela est d'autant plus important que la situation migratoire européenne va se durcir et l'IA peut adresser ce défi majeur pour notre continent.

Par ailleurs, la multiplicité des capteurs ainsi que l'usage des images satellites permets de créer des sources multiples à fusionner pour mieux gérer les différentes menaces. Globalement, l'IA peut répondre aux enjeux sécuritaires en Europe, qui rappelons-le, est frappée par une criminalité organisée désinhibée. En 2019, les recettes d'origine criminelle représentaient 130 milliards d'euros, soit 1% du PIB de l'Union européenne[16].

Nous avons déjà développé SELFIM, dont l'IA aide à repérer les fraudes aux plaques d'immatriculation. Le succès est incontestable avec l'implémentation des démarches DevOps et Cloud, renforçant la collaboration entre les équipes et accélérant la mise en œuvre de solutions innovantes complétant l'approche déterministe déjà implémentée.

En Belgique, Sopra Steria accompagne la Police Intégrée belge (Police Fédérale et Police locale) dans la transformation numérique des services de police en fournissant des outils et des plateformes modernes. Cela englobe l'automatisation des processus, l'intégration de technologies de pointe telles que l'intelligence artificielle et l'analyse de données pour améliorer la prise de décision et l'efficacité opérationnelle.

Enfin, n'oublions pas que le climat est un enjeu incontournable avec des épisodes catastrophiques de plus en plus réguliers. Avec CS, nous travaillons déjà dans le domaine de la prévention des feux. Ainsi, la plateforme CRIMSON est utilisée par de nombreux SDIS (Services départementaux d'incendie et de secours) pour la supervision de la lutte contre les incendies ainsi que par le département des Alpes-Maritimes pour la surveillance des feux de forêts sur l'ensemble de son territoire.

On comprend ainsi que ce sont bien tous les domaines qui vont être impactés, dans l'ensemble des pays européens.

VISION SSG

Demain, il s'agira d'accélérer dans l'IA pour l'ensemble des forces de sécurité et pour tous les cas d'usage (contrôle aux frontières, enquêtes criminelles, biométrie, analyse de données criminelles, gestion de crise, analyse d'images de drones, etc.).

Dans le cas de l'immigration et du contrôle aux frontières, nous souhaitons faire évoluer les outils d'identification biométriques comme la prise d'empreinte sans contact, véritable sujet pour les 10 années à venir. L'analyse d'images et des comportements, le renseignement, les antécédents judiciaires, le partage d'informations biométriques, mais aussi la communication et les outils de traduction intelligente, etc., sont autant de sujets capitaux, alors que l'Europe fait face à des flux migratoires de plus en plus importants.

Face aux défis climatiques, l'IA jouera une rôle clé pour la sécurité civile. Demain, des modèles climatiques et environnementaux identifieront des schémas de catastrophes et analyseront les impacts d'événements climatiques difficiles pour mieux comprendre et anticiper les menaces. Fort du succès de CRIMSOM, nous sommes prêts à relever cet immense défi.

[15] Étienne Loth, Directeur Marché Sécurité intérieure, Sopra Steria.

[16] L'action de l'UE contre la criminalité organisée - Consilium (europa.eu)

Maintenance & logistique

La maintenance est un enjeu crucial pour les armées. Innover pour optimiser les processus et rendre disponibles plus rapidement et plus largement les matériels est une nécessité. Cette innovation passe par l'analyse de données historiques, par le développement de HUMS (Health and Usage Monitoring Systems), d'outils d'aide à la décision, de l'assistance à distance grâce aux lunettes connectées. La maintenance prédictive et la fabrication additive grâce à l'impression 3D permettent déjà d'alléger la logistique en opération et d'optimiser la chaîne d'approvisionnement.

VISION SSG

Notre quotidien est très impacté par le fait que dans tous les secteurs d'activité (énergie, transports, industrie, télécommunications, finance et assurance, ...), il existe une multitude de problèmes d'optimisation que nous ne savons pas résoudre. Le quantique devrait permettre de résoudre totalement et de manière quasi-instantanée une grande partie de ces problèmes. Il constituera donc en soi une véritable révolution.

« Sachant que l'IA pourra également être optimisée de manière beaucoup plus efficace grâce au quantique, nous avons la conviction que cette révolution promet d'être grandement décuplée par cette association de l'IA et du quantique.[17] »

2023 a marqué l'avènement des IA génératives mais celles-ci sont basées sur des technologies qui ne sont pas nouvelles (notamment celles des Transformers) et que nous avions déjà intégrées. En fait, ces technologies peuvent être utilisées non seulement de manière générative mais aussi de manière dite discriminative ou extractive. D'ailleurs, même si en tant qu'utilisateur on ne voit que leur partie générative, les applications d'IA génératives les plus connues (ChatGPT, Bard, ...) combinent souvent des IA extractives et des IA génératives, les IA extractives étant généralement meilleures pour extraire les informations pertinentes et les IA génératives étant meilleures pour synthétiser ces informations. Grâce à l'intelligence artificielle, la maintenance pourra être menée à distance pour des évaluations plus rapides, avec moins d'expertises locales et plus de maintenance prédictive.

En 2021 et 2022, nous avons utilisés avec succès des IA extractives de type Perceivers (une variante des Transformers) pour deux projets :

- Dans un projet de Naval Group pour détecter et classifier les dysfonctionnements de pompes de sous-marins à partir des signaux très instationnaires et très bruités d'un capteur vibratoire échantillonné à plus de 25 kHz ;
- Dans un POC pour prédire les pannes d'une flotte de camions à partir des informations remontées de manière asynchrone sur plusieurs semaines ou plusieurs mois par leur système de supervision embarqué.

[17] Michel Poujol, CTO, programme intelligence artificielle, Sopra Steria.

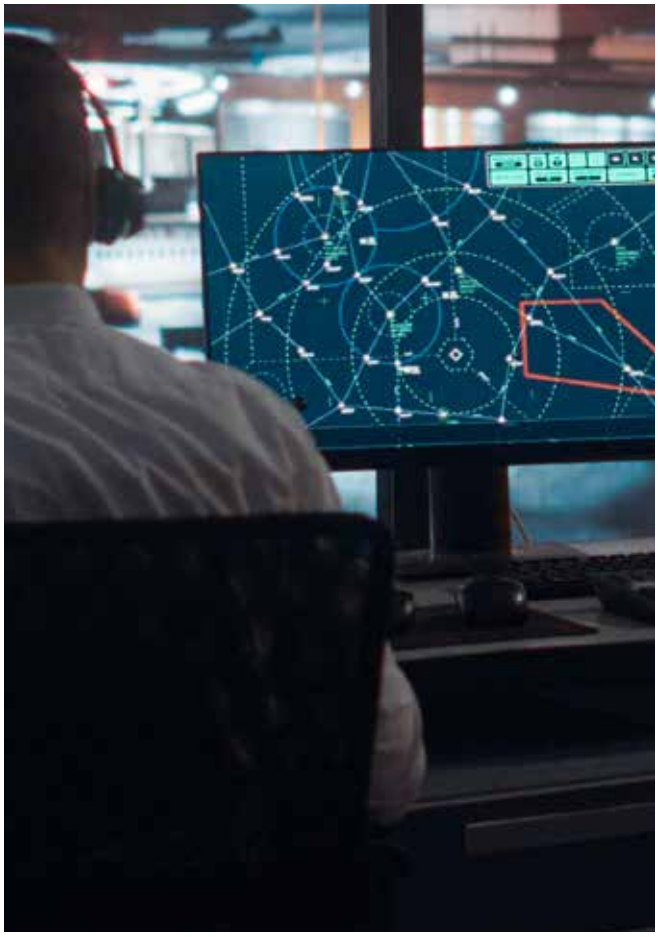
Quantique

La technologie quantique de seconde génération n'en est qu'à ses débuts, mais déjà États, armées, industriels de la défense et start up voient l'immense champ des possibles qui s'ouvrent à eux. La course au quantique a bien débuté dans le secteur Défense car elle ouvre une nouvelle dimension d'anticipation et de calculs. Elle permet également d'accroître la précision des senseurs et offre des moyens supplémentaires de sécuriser les communications ou de casser les données encryptées. Nous nous engageons dès à présent dans cette technologie de rupture pour les décennies à venir.

Command & Control

Depuis 2022, le ministère des Armées place beaucoup d'espoirs dans les technologies de calcul quantique. Cette capacité de calcul phénoménale sera un véritable atout au profit des travaux de simulation extrêmement sensibles menés dans le domaine de la dissusion par la Direction des applications militaires du Commissariat à l'énergie atomique. Cependant, cette capacité est autant attendue au profit des capacités d'analyse que crainte dans le domaine plus spécifique de la cryptographie. La technologie quantique peut être exploitée dans de très nombreux domaines : navigation, ISTAR (renseignement, surveillance, acquisition d'objectifs et reconnaissance), guerre électronique, radar et lidar quantiques, guerre sous-marine, simulation biologique et chimique, design de nouveaux matériaux, interface homme-machine, etc. Cette technologie de rupture va s'imposer dans la guerre de demain car elle permettra l'adaptabilité instantanée du milieu à la menace. Elle doit aussi nous faire réfléchir sur les moyens de protéger nos données et nos échanges, car si cette technologie est prometteuse, elle sera partagée et utilisées par nos adversaires potentiels.

« Nous sommes prêts maintenant pour répondre aux défis dans 10 ans. Telle est notre vision dans les domaines clefs de la cryptographie, des capteurs et du calcul quantique.[18] »



INA représente bien plus qu'une simple avancée dans l'analyse des réseaux mobiles. C'est une belle démonstration de la manière dont la co-construction avec nos partenaires, autour de technologies innovantes, génère un impact positif et quantifiable dans l'industrie des télécommunications. En collaborant avec Telefonica, nous avons créé une solution inédite qui conjugue à la fois performance, efficacité opérationnelle et durabilité des réseaux. Nous sommes extrêmement fiers de cette réussite commune qui illustre notre engagement en faveur d'un numérique plus responsable, et redéfinit les normes de nos industries respectives

Sven Wissman
Global Industry Lead Telecommunications de Sopra Steria

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

VISION SSG

Sopra Steria s'inscrit dans le nouveau paradigme qu'impose la technologie quantique pour de nombreuses applications. Le quantique n'offrira pas seulement des améliorations et de nouvelles capacités, mais imposera également de faire évoluer les doctrines et les concepts d'emploi du niveau tactique au niveau stratégique.

Les capteurs quantiques sont par exemple des instruments de mesure d'une précision inégalée notamment pour les domaines du C2, de la guerre électronique et de l'imagerie.

« À l'horizon 2035, les capteurs quantiques permettront d'obtenir une précision si fine, qu'il sera possible, grâce à des micro-vibrations et à la corrélation de micro-signaux, de parfaitement identifier des véhicules sur de longues distances. Pour les armées, il s'agit d'un outil extraordinaire.[19] »

Également, le calcul quantique qui vise à utiliser les propriétés quantiques de la matière (superposition, intrication, etc.) pour effectuer des opérations massives sur des données va révolutionner le renseignement et le ciblage avec des boucles décisionnelles extrêmement courtes. Rappelons-nous de l'assertion de Guilio Douhet[20] :

« La victoire sourit à ceux qui anticipent l'évolution du caractère de la guerre, pas à ceux qui s'y adaptent une fois que le changement est intervenu. »

Conscient de cet enjeu majeur, Sopra Steria a depuis plusieurs années mis en place une veille technologique et travaille avec des partenaires intégrés au fond Quantonation qui explore des domaines tels que la conception moléculaire, le calcul haute performance, la cybersécurité ou la détection ultra-précise. Pragmatiques, nous sélectionnons le cas d'usage avant d'exprimer mathématiquement le problème. Nous cherchons à développer un algorithme fournissant la meilleure solution.

« La technologie pour la technologie ne nous intéresse pas. Nous ne sommes pas là pour survendre la technologie, mais pour poser une vision pragmatique, afin d'accompagner la stratégie d'une organisation ; c'est notre savoir-faire.[21] »

En étroite collaboration avec Telefonica, Sopra Steria révolutionne la gestion et la planification des réseaux en lançant l'Analyse Intelligente de réseau (INA, Intelligent Network Analysis). Cette solution de jumeau numérique explore la manière dont les technologies quantiques afin d'offrir une meilleure connectivité et une efficacité énergétique accrue du réseau mobile.

En s'appuyant sur la solution Azure Quantum, Sopra Steria et Telefonica expérimentent les dernières avancées des technologies quantiques afin d'améliorer la capacité des réseaux et de réduire l'empreinte énergétique des infrastructures déployées en Allemagne. Ce déploiement illustre la manière dont les technologies quantiques apportent une amélioration des performances, tout en gagnant en efficacité énergétique et en durabilité.

Cette simulation quantique mise en œuvre avec succès sur le réseau de données mobiles de Telefonica, combine une cartographie en temps réel et la gestion dynamique du trafic au sein d'un même système. Elle permet d'optimiser la planification des infrastructures, jusque-là effectuée sans support numérique par des opérateurs. Avec des millions de combinaisons possibles, la cartographie du réseau constituait un réel défi pour les ordinateurs classiques et nécessitait des temps de calcul considérables. Le quantique offre une analyse en temps réel des capacités du réseau pour fluidifier l'écoulement du trafic IP. Le volet quantique d'INA va également permettre de mieux absorber les pics de trafic sans avoir à surdimensionner les infrastructures. En identifiant les connexions potentiellement superflues et en réallouant la charge sur différentes parties du réseau, INA permet d'exploiter toutes les capacités du réseau, et ce sans nécessiter de mise à niveau matérielle ou d'extensions.

Telefonica en Allemagne, expérimente le calcul quantique de manière à réduire significativement son empreinte énergétique et environnementale, pour un réseau plus durable, tout en améliorant la qualité de service de ses utilisateurs mobiles.

[19] Guillaume Roy, Head of IoT, Industry 4.0, Directeur Conseil Centre d'expertise digitale, Sopra Steria.

[20] Stratège italien de l'aéronautique et théoricien du bombardement stratégique.

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

Cyberdéfense : la cryptographie post-quantique

L'ANSSI met en garde, relayée par de nombreux think-tank : les cyberattaques quantiques menacent de bouleverser les pays de l'Union européenne durant les prochaines années. Les progrès dans l'informatique quantique vont rendre obsolètes les systèmes de cryptage actuels. Il convient de se préparer dès maintenant. La protection des données doit être prévue au-delà de 2030. Il est donc nécessaire de préparer les moyens d'une migration des mécanismes cryptographiques.

La technologie quantique n'est pas encore opérationnelle mais nous savons que le calculateur quantique aura bientôt une vraie valeur. Grâce à sa capacité de calcul massive, il sera en mesure de casser des codes cryptés, de casser des clés en parallèle très rapidement pour faire sauter des algorithmes inviolables aujourd'hui. Il faut donc agir dès maintenant pour être en mesure d'être prêts dans quelques années.

À court terme, il faut donc changer tous les algorithmes symétriques et les chiffrements asymétriques. Les États-Unis ont en effet développé le concept de « store now, decrypt later », c'est-à-dire stocker les données maintenant pour les décrypter plus tard, lorsque la technologie sera arrivée à maturité. Il est donc capital d'effectuer des chiffrements post-quantique qui résisteront aux calculateurs quantiques. Or, le domaine cyber revêt un caractère géopolitique très fort avec la question incontournable de la souveraineté. Cet enjeu est d'autant plus grand dans un contexte international tendu, avec, comme sujet principal, la compétition entre la Chine et les États-Unis.

VISION SSG

La cryptographie post-quantique vise à développer de nouveaux systèmes cryptographiques capables de se protéger contre une attaque quantique car le calcul quantique peut être utilisé pour craquer les protections numériques. Avec CS, nous augmentons le niveau de confiance des services cryptographiques avec la génération de clés, la signature et la vérification de signatures avec une cryptographie post-quantique résistante aux attaques des ordinateurs quantiques.

Le vaste projet de renouvellement cryptographique est très lourd et concerne de nombreux secteurs, les grands ministères des Armées, de l'Intérieur et de la Justice, mais aussi les secteurs bancaires et financiers. Sopra Steria et CS anticipent et travaillent déjà sur ce sujet sensible et stratégique, et offrent des solutions de migration vers la cryptographie post-quantique. Avec Cryptonext Security qui fait partie du fond Quantonation, nous proposons des plans de migration et nous aidons nos partenaires à faire les bons choix technologiques. Notre force est ainsi à la fois interne et externe.

Spatial militaire

Tout comme le milieu aérien et la cyberdéfense avant lui, l'espace devient un champ de confrontation entre des puissances et, bientôt peut-être, des acteurs privés. Le secteur spatial connait une vague d'innovation sans précédent : le *New Space*. Le développement de moyens spatiaux nouveaux a rendu les technologies spatiales accessibles à un plus grand nombre d'acteurs et de nations : l'arsenalisation de l'espace est en cours suivant des techniques communes aux autres domaines.

La guerre en Ukraine est riche d'enseignements immédiats. L'espace n'échappe pas à cette règle : rôle de premier plan des capacités spatiales commerciales, guerre « symétrique » entre deux États disposant de capacités spatiales et d'alliés, rôle des start-ups, etc.

Le *New Space* fait partie intégrante de la guerre en Ukraine. Le cas Starlink le prouve. En coupant son système aux Ukrainiens, Elon Musk a empêché une attaque de drones de grande ampleur contre le port militaire russe de Sébastopol. Cet épisode sans précédent nous interroge aussi sur le monopole technologique et l'intervention directe de groupes privés dans un conflit.

Dans le contexte du New Space, le quantique pourrait là aussi révolutionner une multitude de secteurs. L'Europe avec son initiative EuroQCI lancée en juin 2019, a pour objectif de construire une infrastructure de communication quantique sécurisée qui couvrira l'ensemble de l'Union européenne, y compris ses territoires d'outre-mer, d'ici 2027, avec l'aide de la constellation européenne de satellite IRIS2. L'EuroQCI protégera les données sensibles et les infrastructures critiques en intégrant des systèmes quantiques dans les infrastructures de communication existantes, fournissant ainsi une couche de sécurité supplémentaire basée sur la physique quantique. Elle renforcera la protection des institutions gouvernementales européennes, de leurs centres de données, des hôpitaux, des réseaux d'énergie, etc.

VISION SSG

Lorsqu'on parle de spatial militaire, il s'agit d'abord de guerre orbitale (Orbital Warfare) et de guerre sur la donnée *(Space Situational Awareness Warfare)*. Mais la guerre spatiale se livre aussi sur Terre, avec le déploiement de moyens capables d'atteindre les capacités spatiales d'un adversaire via des cyberattaques et des frappes contre les infrastructures au sol.

Dans ce contexte, le quantique dessine lentement l'horizon : liaison entre satellites, chiffrage, solutions et capacités de calcul, sécurisation à tous les niveaux, camouflage et furtivité. Les technologies quantiques vont aider à sécuriser les actions militaires spatiales, à protéger l'espace et nos satellites qui y évoluent de manière défensive mais aussi offensive.

D'abord, car le quantique est un démultiplicateur de technologies. Nous pensons qu'associé aux jumeaux numériques, le quantique va aider à lier l'environnement quantique de calcul à la réalité. La réplique digitale au sol de l'objet en orbite et de sa mission permettra d'anticiper les effets militaires hostiles et intentionnels contre nos intérêts, allant par exemple du brouillage à la neutralisation de panneaux solaires pour rendre inopérant le satellite. Nous estimons que le jumeau numérique est un catalyseur d'intelligence pour faire comprendre la situation en temps réel à l'opérateur et au satellite pour une prise de décision optimale. Celui qui aura la donnée la plus juste pour prendre la décision en temps réel l'emportera. Par ailleurs, cette technologie de rupture permettra au satellite d'optimiser ses capteurs et effecteurs en les adaptant à chaque situation pour par exemple trouver le meilleur angle d'attaque avec l'utilisation du laser afin de neutraliser les panneaux solaires d'un satellite hostile. L'effet que nous recherchons est bien l'autonomie du satellite dans l'optimisation de sa mission, le rendre décisionnel dans son périmètre de mission, avec une intelligence maîtrisée pour des actions de protection. À long terme, il s'agira d'accroître ses capacités d'autodéfense, puis, avec l'autorisation du politique, de développer des capacités offensives.

Le quantique ouvre le champ des possibles avec de nouveaux matériaux pour le camouflage des satellites. La furtivité en orbite est un objectif à atteindre autant sur la non « détection » physique du satellite que sur les actions qu'il pourra mener. L'optimisation de l'allocation de ressources rares dans le spatial est un autre exemple d'application sur laquelle nos équipes travaillent déjà.

Enfin, le maillage de satellites permettra, grâce au quantique, d'organiser encore plus efficacement la défense en orbite et de faire communiquer les satellites entre eux sans passer par la Terre. Il autorisera le partage de l'information en temps réel mais en continu, partout et pour toutes les forces pour des actions simultanées et coordonnées. Demain, maîtriser le tir par l'utilisation du laser dans l'espace sera peut-être nécessaire.

« Le quantique va apporter des changements majeurs en permettant la prise de décision avant qu'il ne soit plus possible d'agir en orbite, tout en augmentant et en sécurisant les débits d'informations. L'anticipation est l'atout-maître ; le quantique la fiabilisera.[22] »

Cette technologie permettra aussi d'atteindre « l'intelligence décisionnelle », c'est-à-dire l'autonomie des satellites. Pour cette raison, nous nous positionnons clairement dans le domaine des capteurs et du calcul quantique pour l'optimisation des systèmes, notamment critiques.

[22] Nicolas Sauvage, expert C2 et opérations spatiales, Sopra Steria.

Cloud souverain de combat

Acteurs de la souveraineté numérique, forts de notre participation à l'alliance européenne Gaia-X et membre de l'alliance pour les données industrielles Edge et Cloud qui vise à favoriser le développement d'un cloud de nouvelle génération, nous anticipons pour donner forme au futur cloud de combat.

Soutien général aux opérations

La guerre en Ukraine révèle les grands traits de la guerre de haute intensité d'aujourd'hui mais aussi de demain. Parmi eux, la numérisation est devenue incontournable et le cloud en est l'un des outils essentiels. La capacité de traitement de l'information est ainsi devenue un enjeu clé. Le programme américain *Joint Warfighting Cloud Capability* le prouve.

Les technologies cloud ont démontré leurs bénéfices dans les usages civils pour croiser et partager les données hétérogènes. Les armées ont des ambitions similaires : lever le brouillard de guerre, accélérer leur boucle de décision, détecter les changements, se signaler les dangers et se réarticuler, assurer la logistique du ravitaillement, gagner la supériorité informationnelle en exploitant au maximum toutes les sources possibles, le tout en disposant d'une infrastructure sans dépendance, économiquement et énergétiquement viable et capable de résister aux attaques. S'il est un défi opérationnel, le cloud défense est un impératif stratégique autant qu'un enjeu de souveraineté[23].

VISION SSG

« Nous pensons que demain le cloud offrira de larges capacités de calculs, de stockage et de traitement de l'information, notamment en local (on premise) grâce à l'intelligence artificielle, de manière ultra-sécurisée.[24] »

Car notre vision repose sur l'efficience de l'interopérabilité, le partage de plateformes et d'applications entre les armées françaises, mais aussi européennes ou au sein de l'Alliance atlantique. Nous sommes en effet un interlocuteur naturel des institutions européennes et acteur des initiatives majeures en matière de souveraineté numérique. Nous sommes par ailleurs membre de l'Alliance européenne pour les données industrielles Edge et Cloud pour le cloud de nouvelle génération. Aussi, transformer la manière de collaborer entre alliés, pour le renseignement, le raccourcissement du traitement de l'information et des prises de décisions grâce aux échanges entre les systèmes de commandement, sont au cœur de nos réflexions sur les technologies mais aussi sur l'accompagnement dont bénéficient déjà nos clients, comme le gouvernement britannique qui dispose de la solution BlueJaySecureCollaboration grâce à Sopra Steria Royaume-Uni, un cloud privé performant qui offre un accès évolutif et sécurisé à tous les utilisateurs tout en répondant à des exigences strictes en matière de sécurité et d'accès aux données.

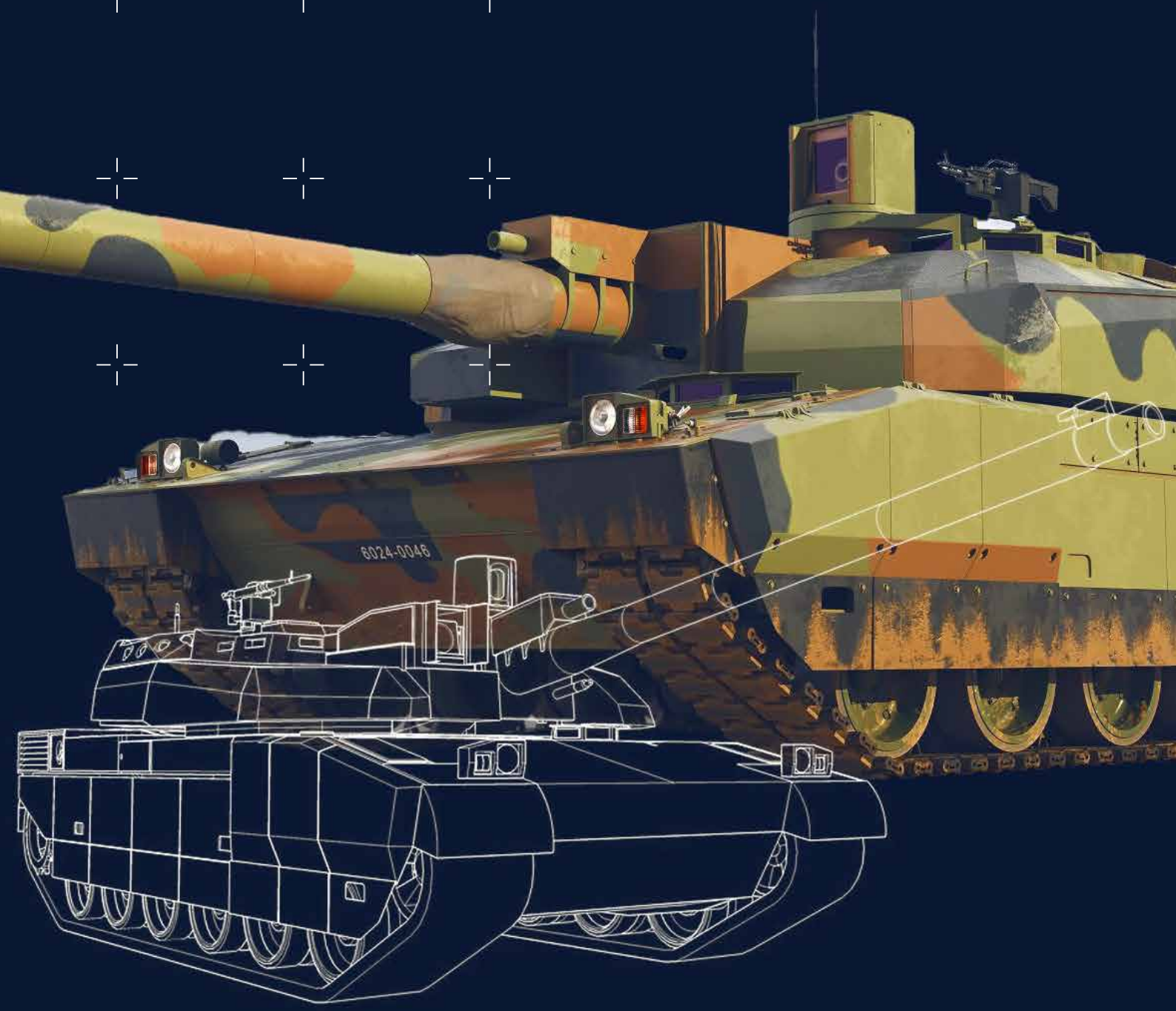
Faire en sorte que nos armées soient prêtes en tout temps grâce à un taux élevé de disponibilité des matériels est un enjeu majeur. Or, le cloud est un outil qui va révolutionner le maintien en condition opérationnelle (MCO) avec la maintenance prédictive et intelligente soutenues par la valorisation de la donnée, son partage dans une chaîne composée de l'ensemble des sous-traitants. La mise à jour d'aéronefs en vol, les arrêts techniques majeurs des navires, des porte-avions et des sous-marins ainsi que les programmes de modernisation sont déjà possibles grâce au cloud. À l'horizon 2035, le partage de données multi-armées et multi-nations sera possible afin de tirer parti de traitement massif en Cloud, distribué jusqu'au *far edge* permettant de garantir une supériorité d'abord tactique, puis stratégique.

Or, la logistique, l'interopérabilité et les opérations ne peuvent se penser sans sécurité. Le cloud, en proposant des technologies déconnectées, va permettre à l'edge computing un chiffrement au plus près de la donnée et donc une cybersécurité renforcée. Car le conflit en Ukraine met en lumière la guerre des données et leur migration vers le cloud . Cette guerre est aussi un véritable changement de paradigme en France et en Europe dans la mesure où les questions de la souveraineté (numérique, de défense, énergétique) et d'autonomie (stratégique) sont revenues au premier plan. Notre vision repose sur un cloud souverain et autonome afin de ne pas être dépendant des hyperscalers et de leurs data centers. Le ministère des Armées a développé une stratégie cloud sur plusieurs niveaux, central, edge et far edge avec, pour les deux derniers, une capacité de cloud opérationnel permettant l'autonomie lorsque les réseaux ne sont plus disponibles. Bientôt, une nouvelle étape dans le cloud de combat multidomaines devra être franchie. Telle est notre cible à l'horizon 2035. L'objectif est de créer un cloud de combat, décentralisé, protégé des cyberattaques, collaboratif et partagé entre tous les domaines (terre, air, mer, espace et cyber). Toutes les forces seront donc connectées et les différentes plateformes hétérogènes seront intégrées pour l'échange de l'information en temps réel et de manière continue pour les armées.

Nous voyons le futur cloud de combat comme un réseau maillé, global, pour la redistribution des données et le partage de l'information aux niveaux stratégique, opérationnel et tactique. Le cloud est un accélérateur et un vecteur de transformations et d'efficience opérationnelles mais aussi logistiques.

[23] Étude de l'IFRI, Le cloud défense. Défi opérationnel, impératif stratégique et enjeu de souveraineté

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



Jumeaux numériques

Expert dans le domaine du métaverse et donc des jumeaux numériques grâce à son Centre d'expertise digitale, Sopra Steria a pris le chemin de l'industrie 5.0 et de l'efficience opérationnelle. Dans un contexte tendu de retour de la guerre de haute intensité, le multidomaines, le Command & Control et la sécurisation de la maintenance et de la logistique sont de véritables défis pour nos armées et les armées européennes. Notre maîtrise de la technologie des jumeaux numériques est ainsi un atout de taille.

Command & Control

L'utilisation du jumelage numérique à des fins militaires, voire à double usage, en rapprochant les mondes physique et numérique grâce à une connectivité robuste et au moyen de l'intelligence artificielle et des technologies de simulation, change la donne. Il permettra aux décideurs et aux commandants de mieux maîtriser leur environnement et donc de prendre les décisions appropriées en cas de besoin. Le jumeau numérique aidera les commandants d'opération à mieux élaborer leur plan de campagne, à anticiper et à adapter leurs actions et leurs tâches sur la base de données actualisées. Cette capacité appliquée à tous les domaines et aux différents niveaux de commandement (stratégique, théâtre d'opérations et tactique) offrira un avantage extraordinaire, car elle suggérera une action/décision éclairée, fondée sur des données de haute qualité en temps opportun. Le jumeau fournira des recommandations sur l'optimisation des ressources dans différents scénarios. L'emploi d'un drone dans différentes configurations en est un bon exemple, et la guerre en Ukraine est un bon rappel de l'optimisation des moyens en fonction de la posture du belligérant. Le jumelage permettra une meilleure compréhension d'une menace et des moyens possibles pour la contrer.

Quant aux commandants dont la responsabilité est de fournir des moyens, de les soutenir et de les entraîner dans le continuum crise, confrontation, conflit, l'utilisation du jumelage numérique apporte également de grands avantages. En effet, un jumeau peut optimiser la gestion d'une infrastructure, qu'elle soit terrestre, aérienne ou navale, peut améliorer l'utilisation de l'énergie, offrir une approche de la sécurité sous un angle différent et faciliter le déploiement de personnes pour répondre au mieux à toute tâche spécifique. Pour que le jumeau numérique change la donne, la confiance dans les données est primordiale Ces deux éléments distincts sont tout aussi fondamentaux l'un que l'autre. En effet, si toute donnée entrant dans le monde jumeau est corrompue ou fausse, le résultat sera catastrophique car elle fournira des informations erronées sur la base desquelles une décision de commandement sera prise.

La création du jumeau est basée sur des données provenant de capteurs déployés sur l'objet réel à jumeler, mais aussi sur des modèles de simulation et l'IA afin de reproduire le comportement et les caractéristiques du jumeau physique pour aider à la prise de décision. C'est grâce aux capteurs que la connexion avec la réalité est établie. La qualité des capteurs et leur capacité à capturer la réalité sont au cœur du concept.

Dans le concept de jumelage numérique, il y a un échange permanent d'informations et de données entre le jumeau physique et le jumeau virtuel. Ce flux doit se produire à intervalles réguliers, en fonction du rythme opérationnel. Cet échange est la clé du succès du concept dans un environnement opérationnel où la décision ou l'information fournie aux décideurs sera basée sur les dernières informations reçues.

Le jumeau numérique est plus qu'une simulation car il apporte la notion de « réalité dynamique » qui permet au décideur d'exiger davantage du jumeau - car il y a un élément de surveillance et d'optimisation de l'objet physique sur la base d'une boucle Observer, Orienter, Décider et Agir numérique.

Jusqu'à présent, le jumelage numérique dans le domaine militaire a été essentiellement considéré sous l'angle de la maintenance et de la logistique. En effet, avoir la capacité de suivre à travers un jumeau numérique l'usure (attrition) d'un rotor d'hélicoptère ou d'un moteur de navire à travers le flux de données en temps réel permet de faire de la maintenance prédictive et corrective selon les besoins et sert donc d'outil d'anticipation et d'optimisation.

Cependant, l'utilité d'un jumeau numérique est bien plus grande si l'on pense aux opérations C2 multidomaines. Il a le potentiel de redéfinir la planification, la conduite et l'exécution d'une opération et, à l'extrême, de fournir une vue d'ensemble stratégique de toutes les opérations. Le jumelage numérique n'est possible que grâce à une connectivité robuste et à une infrastructure informatique capable de collecter, de stocker et d'exploiter des données en temps réel, ce qui permet également d'effectuer des simulations.

Le ministère de la Défense britannique s'appuie sur Sopra Steria pour fournir des services numériques fiables en matière de gestion des stocks et de capacité d'intégration qui permettent une prise de décision efficace grâce à l'accès à des données pertinentes. Maintenir, moderniser et transformer les services de logistique et de soutien de l'armée britannique sont de véritables défis. Chez Sopra Steria, nous tirons parti de nos capacités numériques à l'échelle de l'entreprise en matière de solutions d'ingénierie tout au long de la gestion de la chaîne d'approvisionnement avec des technologies numériques habilitantes, notamment les jumeaux numériques, la blockchain et les environnements de collaboration sécurisés pour faire en sorte que l'armée britannique relève efficacement ces défis.

VISION SSG

Il existe plusieurs cas d'utilisation où le jumeau numérique apportera une valeur ajoutée à la défense et à l'armée en particulier. Un cas d'usage opérationnel forme la partie émergée de l'iceberg et Sopra Steria identifie clairement les opportunités qui existe dans cette technologie et le domaine métier qui lui est lié.

Plusieurs cas d'utilisation qui peuvent être développés dans chacun des domaines (terrestre, maritime, aérien, spatial et cybernétique). Nous pensons que les opérations multidomaines illustrent parfaitement l'utilisation du jumeau numérique dans la planification et l'exécution des missions, dans l'aide à la prise de décision, la formation et dans la simulation à travers un large spectre de fonctions (logistique, opérations, santé...).

En effet, pour planifier une opération, le commandant d'une force déployée sur un théâtre d'opération peut utiliser les capacités du jumeau numérique avec les dernières données disponibles. Cela se traduit, par exemple, par l'identification de la meilleure zone (3D) pour une opération amphibie, des itinéraires de déminages, pour le réapprovisionnement des unités en mer avant l'assaut. En d'autres termes, des plans d'action seront suggérés par le jumelage en fonction du niveau de difficulté du débarquement, de la connaissance du terrain, du fond marin, de la menace, de la capacité à disposer des bonnes informations et des capacités en unités, y compris leur niveau d'entraînement.

Nous croyons que le jumeau numérique agit dans les différents niveaux du combat. Le stratégique qui a sous son commandement d'autres opérations peut anticiper et mieux répartir ses forces. Cette capacité de jumelage permet de faire passer la planification de la prédiction à la décision.

Au niveau tactique, les commandants ont la possibilité grâce au jumeau numérique d'imaginer, de planifier et de reconfigurer leurs forces opérationnelles et leurs moyens afin de les positionner au mieux pour mener à bien une opération. Par exemple, l'utilisation de drones au-dessus d'une zone tactique pour « rafraîchir » les données du jumeau avec des informations actualisées sur le terrain avant un débarquement ou un déploiement de forces, peut s'avérer utile. En effet, le commandant de la force de débarquement pourra réévaluer et revoir ses intentions sur la base des recommandations du jumelage. L'utilisation d'un jumeau numérique implique une confiance absolue dans les données collectées et l'utilisation ultérieure de celles-ci dans des configurations en temps quasi réel par le biais de différents algorithmes et modèles. La question philosophique de la position de l'homme par rapport à la boucle sera très probablement posée dans un tel contexte. En effet, avec un outil aussi performant, on pourrait être tenté de faire totalement confiance au jumeau sans tenir compte du facteur humain. Aujourd'hui, il est recommandé que l'homme reste sur la boucle. Cela a toujours été notre conviction, quelle que soit la technologie. Et cela le restera.

Maintenance & logistique

La première moitié de cette décennie a vécu un bouleversement important des manières de faire au sein de l'écosystème de la défense. Les organisations militaires et les entreprises du secteur défense ont connu des perturbations majeures des chaînes d'approvisionnement provoquées par de multiples facteurs, notamment la pandémie de Covid-19, la guerre en Ukraine, les catastrophes naturelles, des conditions économiques difficiles et plus globalement, des relations internationales en tension. Par ailleurs, les organisations doivent faire face à un éventail de plus en plus large de choix et dans un paysage en évolution rapide de technologies émergentes comme la blockchain, la robotique et l'intelligence artificielle.

L'une des technologies émergentes qui affecte déjà le secteur est celle des jumeaux numériques, en particulier pour l'amélioration de l'adaptabilité des chaînes d'approvisionnement en cas de surprise stratégique. Une combinaison de technologies habilitantes et de capacités analytiques, les jumeaux numériques produisent un modèle virtuel d'un processus, d'un système ou d'un objet, informés par des données en temps réel.

D'une manière générale, l'industrie 4.0 est au cœur de nos savoir-faire, comme en Espagne où Sopra Steria optimise les processus de fabrication du secteur aérospatial grâce à la robotique, l'IoT, le cloud, la réalité virtuelle, l'intelligence artificielle. Chez Sopra Steria, nous contribuons au déploiement de solutions numériques innovantes pour le maintien en condition opérationnelle (MCO).

VISION SSG

Les nouvelles plateformes de jumeaux numériques couplées permettent d'une part la fusion de données réelles issues de scan 3D (dont LIDAR) avec des données de modélisation, et d'autre part d'enrichir ses données avec la génération de données synthétiques qui viennent compléter ou détailler les nuages de points réels. Ces modèles synthétiques enrichis peuvent ensuite servir de modèles d'entrainement pour l'IA, destinés par exemple à l'optimisation de déplacement des robots de production (Zvision et Nvidia Isaac Sim) ou de logistique. L'entrainement d'IA sur les jumeaux numériques permet également d'anticiper les problèmes de corrosion ou de fatigue structurelle à court, moyen et très long terme (au-delà de 30 ans) facilitant ainsi les opérations de maintenance prédictive (simulations de Siemens Energy). Nos savoir-faire dans les domaines du métaverse et donc des jumeaux numériques ne sont plus à démontrer. Nous avons lancé plusieurs programmes de pilotage de l'industrie 4.0 (services, processus, cas d'usage, technologie et modèles organisationnels pérennes et efficaces) avec par exemple la digitalisation de 35 sites au niveau mondial pour Renault. Nous menons également de nombreux projets IoT, avec du conseil en méthodologie et dans le déploiement avec les technologies 5G, l'edge computing, l'IA embarquée pour le contrôle et les commandes d'équipements industriels, le tout avec une cybersécurité associée. Nous travaillons notamment avec Schréder, producteur de bras automatisés, pour l'amélioration de leurs produits à destination de leurs clients.

Nous sommes partenaires de Nvidia pour permettre aux entreprises de développer des pipelines 3D personnalisés, afin de simuler à grande échelle des mondes virtuels physiquement réalistes, afin de développer des simulations virtuelles parfaitement synchronisées avec le monde réel, fidèles à la réalité physique et basées sur l'IA. Cela peut concerner autant la localisation la plus efficace pour une chaîne de production, ou la cartographie d'une zone de combat grâce à la réalité hybride. Cela ouvre la possibilité pour de nouveaux cas d'usage et permet de collaborer autour d'un jumeau numérique au sein d'une entreprise ou d'une unité de l'armée et son écosystème.

« Les avantages du jumeau numérique pour les chaînes d'approvisionnement et le maintien en condition opérationnelle de la défense sont nombreux. Car cette technologie est en réalité le modèle qui tire après lui tous les cas d'usage.[25] »

Le conflit en Ukraine nous impose aujourd'hui d'anticiper demain. Défaut d'un fournisseur, embargo sur des matériaux stratégiques, les cas de ruptures sont légion et le jumeau numérique reconfigure l'écosystème logistique pour plus de résilience, y compris en avance de phase grâce aux vertus de la simulation qu'il permet. Nous tablons depuis longtemps sur la maintenance préventive pour anticiper les ruptures. Mais nous parions sur une optimisation plus grande encore de la phase de maintenance et de la simulation pour un découpage fonctionnel servant au remplacement de pièces ou au changement de matériels (capteurs avec l'impression 3D, écrans plus légers et intuitifs, par exemple) et pour la formation poussée des opérateurs. Les gains de performance se font dès lors aux niveaux technique et financier.

Demain, nous entrerons dans un système de systèmes susceptible d'offrir un solide centre de soutien logistique en OPEX ou sur le territoire, avec des jumeaux numériques capables d'optimiser les machines et les matériels tout en diminuant l'empreinte logistique. Notre conviction est que ce système de systèmes répondra à la forte demande de mutualisation, de collaboration entre les armées au sein de l'Union européenne et de standardisation des jumeaux numériques pour diminuer les facteurs d'indisponibilité des matériels. Par ailleurs, grâce aux scénarios « what if ? », il sera possible d'explorer les actions possibles pour plus de résilience des systèmes ainsi que leur mise en commun entre différents partenaires.

« Couplé à l'IA et d'autres facilitateurs comme les réalités virtuelle et augmentée ou l'internet des objets (IoT), cette technologie mise à jour et partagée, améliorera l'automatisation, l'autonomie, le pilotage à distance des opérations et l'aide à la décision.[26] »

Grâce à l'entretien, la mise à jour et au partage des jumeaux numériques, y compris en temps réel, les limites techniques et technologiques seront repoussées. Ce système de demain ouvrira le champ à la simulation de grande ampleur, avec des impacts bénéfiques aux niveaux tactiques et opérationnels pour les armées. Le jumeau numérique du futur ouvrira de nouveaux champs d'application, une nouvelle vision, complète.

[25] [26] Pierre-Antoine Arrighi, Directeur, Centre d'expertise digitale, Sopra Steria, David Maurange, Directeur conseil, Digital Interaction & Metaverse, Centre d'expertise digitale, Sopra Steria Next.

Réalité étendue

Sopra Steria s'engage pour accompagner les mutations du secteur industriel en proposant des solutions sécurisées, optimisées et novatrices. Le recours à la réalité virtuelle et augmentée dans les secteurs stratégiques de la défense, de la sécurité, de l'aéronautique et de l'aérospatial, contribue à accélérer et à optimiser la conception de nouveaux projets.

Sécurité publique & justice

Imaginer les futurs emplois des forces armées, des forces de l'ordre et de la sécurité civile, conduit à repenser leur formation et la planification de leurs missions. Ainsi, les nouvelles technologies sont amenées à se développer fortement au sein de ces forces. Parmi elles, la réalité étendue ouvre le champ des possibilités.

La notion de réalité étendue fait référence à une combinaison de technologies qui étendent la réalité par des facteurs numériques. Cette réalité, appelée aussi réalité mixte, combine la réalité virtuelle et la réalité augmentée. Beaucoup plus récente, cette technologie propose des objets de synthèse rajoutés au monde réel et visualisables par les individus. Ces objets ressemblent à des hologrammes et interagissent avec le monde réel, tout comme ce dernier coexiste avec eux.

Command & control

La Red Team de l'Agence de l'innovation de défense (AID), a parfaitement compris le rôle que jouent la réalité étendue et les jumeaux numériques pour les armées. Dans son scénario prospectif Chronique d'une mort culturelle annoncée, elle crée le concept de « safe spheres » ou bulles de réalité étendue dans lesquelles sont intégrés des jumeaux numériques qui constituent des doubles virtuels d'objets réels avec lesquels il est possible d'interagir[27]. Les outils numériques permettent déjà d'optimiser la logistique et la maintenance. Ils aident aussi à planifier des opérations militaires grâce à des données analysées par l'intelligence artificielle. Cela offre aux soldats une vision précise de l'espace de bataille.

CS a développé CRIMSON Sentinel, solution d'hypervision dédiée à la gestion centralisée des systèmes de protection et de sécurité et à la conduite des opérations. Elle s'appuie sur un puissant moteur cartographique 2D/3D pour offrir une tenue de situation globale, synthétique et intelligible, et exploiter le jumeau numérique du site à sécuriser.

Crimson Sentinel facilite le partage d'informations, la coordination et l'aide à la décision avec une gestion des droits adaptée au besoin d'en connaître, et un éditeur de règles graphique pour l'automatisation des tâches.

VISION SSG

« Nous pensons que cette technologie sera incontournable pour les forces de sécurité, les forces armées et la sécurité civile. Imaginez la possibilité, pour un pompier en mission, de voir dans son casque et ses lunettes des informations incrustées couplées à un lidar ou une caméra thermique, qui lui donnent des indications sur la température d'une zone, le risque pour son équipe, des analyses sur l'état des matériaux et les risques d'effondrement.[28] »

Cette réalité mixte peut également fournir une cartographie complète des lieux. C'est un sujet technologique d'avenir et nous sommes persuadés que demain, pour les armées (simulations, entraînement, opérations réelles), les forces de sécurité et la sécurité civile, la réalité sera mixte : le soldat, soldat du feu, policier et gendarme aura conscience de son environnement physique, mais prendra aussi en compte de multiples paramètres virtuels pour l'aider à accomplir sa mission.

[27] https://redteamdefense.org/saison-1/chronique-dune-mort-culturelle-annoncee

[28] Étienne Loth, Directeur Marché Sécurité intérieure, Sopra Steria.

Nous bâtissons avec nos partenaires la défense et la sécurité européennes de demain

06.

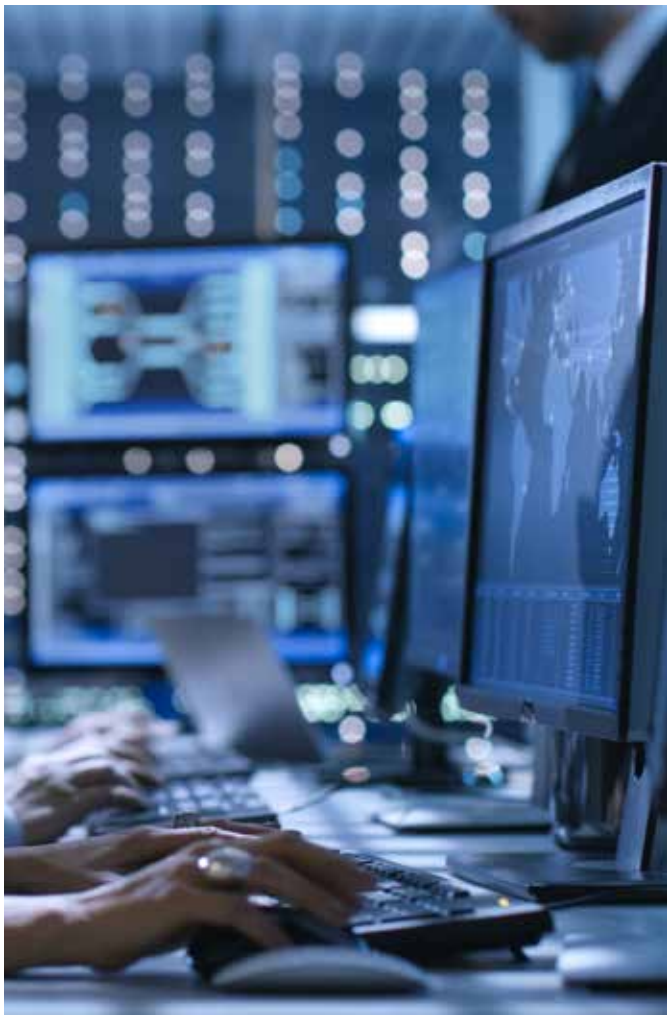
Bâtir aujourd'hui la défense et la sécurité de demain. Nous avons dépassé le stade des crises pour entrer dans celui des chocs. Le monde est en tension, la guerre de haute intensité a fait un retour fracassant alors que le modèle de guerre asymétrique n'a pas disparu, le dérèglement climatique impose ses catastrophes et ses drames et la sécurité est au cœur des préoccupations des citoyens français et européens. Pour une défense et une sécurité efficientes, notre stratégie repose sur la maîtrise des technologies de rupture mais aussi sur nos savoir-faire dans les grands domaines métiers. Cette singularité associée à la connaissance des grands enjeux auxquels sont confrontés les trois grands ministères régaliens – Armées, Intérieur et Justice – nous positionne comme le seul industriel de référence dans le numérique de Défense.

Nous possédons une connaissance approfondie du secteur défense et sécurité mais aussi des grands enjeux internationaux, nous permettant de prendre de la hauteur sur la « tectonique » géopolitique qui transforme le monde.

Forts de plus de 40 ans d'expérience, nous sommes un acteur mondial de la transformation numérique et un membre de la BITD de défense.

Nous travaillons avec des partenaires multiples au service de la défense et de la sécurité, en Europe et à travers le monde. Acteur de référence de la souveraineté numérique, nous développons des expertises dans des domaines majeurs.

Nous sommes convaincus que « la technologie est un outil exceptionnel, véritable levier d'efficacité capable de suggérer de nouvelles modalités d'engagement[29] » mais aussi de renforcer et de sécuriser les chaînes logistiques, de rendre plus efficient le travail des forces de sécurité intérieures et civiles et la justice. Nous n'oublions pas pour autant que l'Homme reste central, décisionnel car bien formé à l'utilisation de la technologie, raison pour laquelle nous insistons tout autant sur les expertises métiers.



[29] Boris Laurent, Manager Défense & Sécurité, Sopra Steria Next, auteur de « Technologie et nouvelle modalité de l'engagement tactique », in La tactique au XXIe siècle. Le retour de la bataille, sous la direction de Thibault Fouillet, Fondation pour la recherche stratégique, Édition du Rocher, octobre 2023.

The world is how we shape it