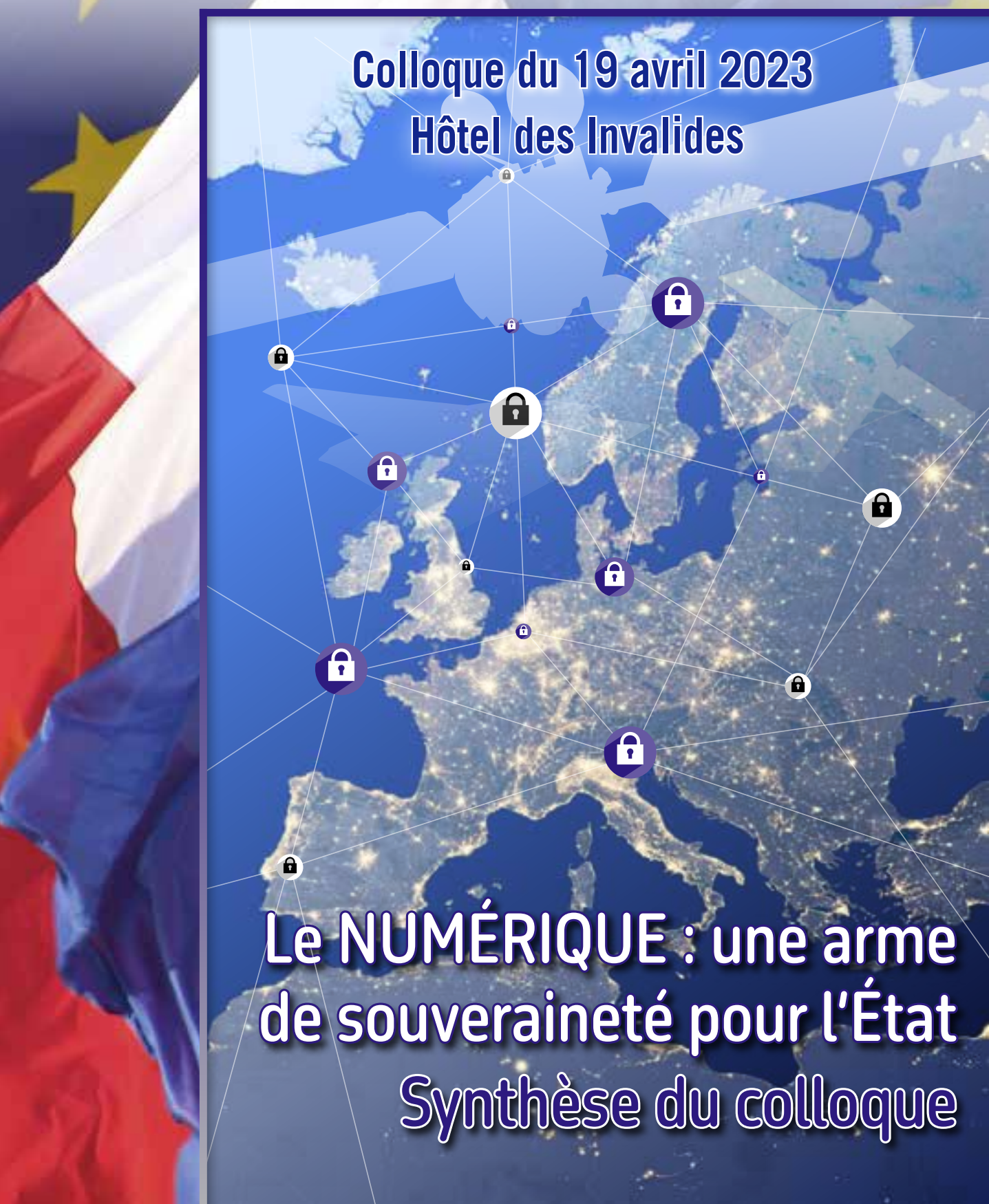
Confédération Amicale
des Ingénieurs de l'Armement

Colloque du 19 avril 2023
Hôtel des Invalides



Le NUMÉRIQUE : une arme de souveraineté pour l'État

Synthèse du colloque

Pourquoi ce colloque ?

Tous les deux ans, la CAIA organise un colloque sur un thème qui résonne avec la raison d'être du corps des ingénieurs de l'armement.

Après l'édition 2021 centrée sur les enjeux de souveraineté (« Reconquérir la souveraineté »), l'édition 2023 du colloque de la CAIA s'est tenue le 19 avril 2023 au sein du prestigieux Hôtel des Invalides sur le thème **« Le numérique, une arme de souveraineté pour l'Etat ».**

L'IGA (2s) Olivier Martin, président de la CAIA, et l'IGA Thierry Carlier, Directeur Général Adjoint de la DGA.

Grâce à la présence d'intervenants de haut niveau, une salle comble (près de 150 personnes en amphithéâtre et 50 personnes à distance), une participation équilibrée (secteurs public/privé), des interactions entre la salle et les speakers, ce colloque fut un grand succès.

Ce colloque s'est achevé par un cocktail qui a réuni l'ensemble des participants, permettant ainsi de poursuivre les nombreux échanges dans une ambiance très conviviale.

Pour ceux qui n'auraient pas eu la possibilité d'y assister, la CAIA a rédigé la présente synthèse des principaux points forts de cet événement.

Bonne lecture !

Mot d'accueil

Olivier Martin, Président de la CAIA

Je suis très heureux de vous accueillir aujourd'hui pour le colloque CAIA 2023 sur le thème : « Le numérique, une arme de souveraineté pour l'Etat ».

Ce thème a été choisi avec soin et se trouve parfaitement en phase avec l'actualité.

Sur le plan international, le récent conflit ukrainien a souligné l'importance des systèmes numériques dans les opérations : emploi de systèmes de communications satellitaires, exploitation du renseignement, communications sécurisées, cyberattaques, désinformation …

Sur le plan national et dans un domaine qui concerne particulièrement les ingénieurs de l'armement, **le gouvernement a confirmé dans sa communication du 23 novembre 2022 au titre de la réforme des grands corps techniques, le rôle important que doivent jouer les grands corps techniques au profit de l'Etat en soulignant notamment que : *« …Cette réforme répond aux besoins de l'État de « réarmer » ses capacités d'expertise technique et scientifique, y compris dans des champs comme le numérique, et de les conserver. »***

Or, **le ministère des armées dispose d'un grand nombre d'experts dans le domaine du numérique, le Corps de l'armement pouvant lui-même s'appuyer sur près de 150 ingénieurs de l'armement très qualifiés.**

C'est donc dans cette perspective que s'inscrit ce colloque, dont les principaux objectifs sont :

- partager le savoir-faire et l'engagement des ingénieurs de l'armement sur un sujet aussi stratégique,
- réunir des personnalités de tous horizons pour échanger sur leurs expériences et connaissances,
- débattre sur les principaux enjeux du ministère des armées dans ce domaine
- et, si possible faire des recommandations utiles au profit de l'Etat.

Nassima Auvray et Isaure de Broglie, co-organisatrices de ce colloque.

Je tiens à remercier l'ensemble des intervenants qui ont bien voulu participer à ce colloque, avec une mention particulière pour l'IGA Thomas Courbe, Directeur Général des entreprises, Vincent Tejedor, Directeur Général du Numérique et des systèmes d'information et de communication et l'IGA Thierry Carlier, Directeur Général Adjoint de la DGA, qui a clôturé nos travaux.

Je tiens également à remercier chaleureusement nos partenaires[1] qui nous ont soutenu lors de l'organisation de ce colloque et ont ainsi permis son succès.

Il est enfin important de remercier **l'équipe d'organisation de ce colloque, Nassima Auvray**, Responsable général, **Isaure de Broglie**, responsable logistique et **l'équipe de jeunes IA²** qui se sont dévoués pour bâtir ce colloque et même l'animer, montrant ainsi leur engagement au profit de la CAIA et plus largement de l'ensemble de notre communauté.

---

1 : Airbus, MBDA, Orange et Thales
2 : Baptiste Chomel de Jarnieu, Gaëtan Doueneau, Pauline Emschwiller, Thibaut Lajoie Mazenc, Lucien Masson et Jean-Baptiste Moiroud.

La CAIA tient à remercier pour leur soutien au Colloque de la CAIA 2023 ses partenaires :

AIRBUS

MBDA

THALES

et

orange

Ouverture

ICA Nassima Auvray, Membre du CA de la CAIA et Responsable du colloque

Ce colloque est le fruit de plusieurs mois de préparation et j'aimerais chaleureusement remercier les intervenants des différentes *keynotes* et tables rondes qui nous ont fait l'honneur d'accorder un peu de leur temps précieux pour partager leur connaissance. J'aimerais également remercier toute l'équipe de jeunes ingénieurs de l'armement ainsi que les membres du bureau de la CAIA qui ont œuvré à l'organisation et à la réussite de ce colloque.

Pourquoi avoir choisi «Le numérique : une arme de souveraineté pour l'Etat» pour thème ? Tout simplement parce que c'est un sujet d'actualité : le numérique est devenu à la fois un instrument de performance dans tous les aspects de notre société mais aussi un nouvel espace de confrontation.

Cyberattaques, multiplication des campagnes de désinformation, risques d'intrusions informatiques dans les infrastructures critiques, exploitation des données à des fins d'espionnage, recours démesuré à l'intelligence artificielle à des fins malveillantes… Ces exemples de risques induits par le numérique sont une réalité aussi bien dans le cadre d'un conflit armé que dans notre vie de tous les jours. Ils illustrent, d'une part, l'importance de la souveraineté numérique pour protéger les intérêts nationaux et garantir la sécurité de l'Etat et, d'autre part, l'enjeu pour notre Etat à mobiliser toutes les compétences dont il dispose pour conserver son autonomie.

Alors que la loi de programmation militaire 2024-2030 a été adoptée par le Parlement, il n'y a aucun doute sur le fait que la supériorité numérique sera un enjeu clé aussi bien pour les milieux Terre, Air, Mer que pour les nouveaux champs de conflictualités que sont l'espace exo-atmosphérique ou encore les fonds marins, sans compter bien évidemment le cyberespace ou l'espace informationnel.

Quelques semaines avant la tenue du colloque, une mystérieuse coupure de câbles sous- dans les environs de Taiwan, avait fortement perturbé l'activité de l'ile si bien que Taiwan a fait le choix d'expérimenter le recours aux satellites en orbite basse pour assurer une continuité d'activité en cas de répétition de ce type d'événements. Cet événement, loin d'être anodin, illustre bien le fait que la souveraineté numérique s'opère en tout lieu, depuis les fonds marins jusqu'aux différentes couches de l'atmosphère.

Ce colloque avait pour objectif de partager le savoir-faire et l'engagement de grands nombres d'acteurs qui œuvrent quotidiennement sur un sujet aussi stratégique et qui soulève de nombreuses questions d'ordre géopolitique, de sécurité, de protection des données, de normes et de réglementation, de garantie des droits fondamentaux mais aussi d'innovation et de compétitivité.

Le programme de ce colloque était ainsi réparti en trois tables rondes et trois interventions et son détail est donné ci-après :

- Keynote **« La souveraineté numérique », IGA Thomas Courbe,** Directeur Général des Entreprises
- Table ronde **- Les technologies du numérique au service des usages opérationnels,** animée par l'**IPA Thibaut Lajoie Mazenc** avec :
  - **IGA Dominique Luzeaux**, Directeur de l'Agence du Numérique de Défense, ministère des Armées
  - **GDA Philippe Dedobbeleer**, Chef de la Division Stratégie Numérique des Armées, ministère des Armées
  - **Hélène Chinal**, Head of Transformation Southern and Central Europe SBU, Capgemini
  - **IGA Thierry Baud**, Directeur Commercial France, Airbus Defence and Space
- Keynote **« Enjeu des compétences dans le numérique »**, **Vincent Tejedor,** Directeur Général du Numérique et des systèmes d'information et de communication, ministère des Armées
- Table Ronde – **L'Intelligence Artificielle de confiance**, animée par **l'IA Baptiste Chomel de Jarnieu** avec :
  - **Guillaume Avrin,** Coordinateur National pour l'Intelligence Artificielle, Direction Générale des Entreprises
  - **Marko Erman,** Chief Scientific Officer SVP, Thalès
  - **Col Jean-Gabriel Herbinet,** Adjoint du Bureau Numérique, EMAT
  - **Yonatan Teboul,** Responsable Groupe du Digital pour les produits et les services, MBDA
- Table Ronde – **Lever le voile sur la Cyber**, animée par l'**IA Pauline Emschwiller** avec :
  - **GDI Aymeric Bonnemaison,** COMCYBER, Ministère des Armées
  - **IGA Bruno Marescaux,** Chargé de mission Cyber auprès du Délégué Général pour l'Armement, DGA
  - **Patrick Radja,** VP Cybersecurity Director, Naval Group
  - **ICA Frédéric Grelot,** Co-Founder, Scientist Lead, GLIMPS
- Clôture par **l'IGA Thierry Carlier**, Directeur Général Adjoint de la DGA

KEYNOTE

la souveraineté numérique

IGA Thomas Courbe

La souveraineté numérique est au croisement de deux grands mouvements : la transition numérique de l'économie, et plus largement de nos sociétés d'une part et, plus récemment, la recherche de l'autonomie stratégique. Ce dernier concept est un des grands acquis de la présidence française de l'Union européenne, cet enjeu étant aujourd'hui acté au niveau européen après beaucoup d'efforts, compte tenu de la doctrine générale de la politique économique européenne.

Cette souveraineté numérique ainsi définie repose sur trois grands piliers indissociablement liés.

Le premier pilier réside dans la construction d'une offre numérique souveraine, française et européenne sur les technologies les plus importantes. Ces dernières sont déterminées par le croisement de la criticité en cas d'absence de la maîtrise de cette technologie, de leur impact économique car les technologies numériques sont transverses et enfin de la présence d'un écosystème en France capable de générer cette offre, condition indispensable pour y parvenir.

Ce raisonnement a permis **d'identifier un certain nombre de technologies numériques pour lesquelles nous concentrons les moyens de soutien importants pour cette offre ciblée : nucléaire, intelligence artificielle, 5G, cloud, semi-conducteur, cybersécurité et quantique.**

Très concrètement, les stratégies que nous déployons depuis quelques années pour faire émerger cette offre souveraine nous amènent à observer des ruptures dans l'offre mise à disposition de nos entreprises et plus globalement de notre économie.

Sur la cybersécurité, par exemple, nous avions des pans entiers de la chaîne de valeur qui manquaient. Nous préparons actuellement avec les entreprises (souvent des start-ups ou des entreprises de taille moyenne), une suite bureautique complète, chiffrée de bout en bout et un système de gestion sécurisée de l'IOT, des outils d'évaluation du risque cyber ou encore des services d'anonymisation sur les réseaux. Aucune offre n'existait en ces domaines il y a quelques années mais certaines sont aujourd'hui en cours de développement afin de répondre le mieux possible à l'ensemble des besoins des entreprises.

De même, en matière de 5G, nous travaillons évidemment à l'ancrage des grands constructeurs certes pas français, mais européens comme Nokia ou Ericsson et nous avons beaucoup progressé ces dernières années en France, notamment en termes de R&D. Nous développons également avec des start-ups des compléments à cette offre au sein de l'IRT BCom dans le cadre d'une initiative public-privé pour développer un cœur de réseau télécom 5G souverain.

Focus sur IRT BCom

Soutenu par le programme Investissements d'Avenir de l'Etat, la Région Bretagne, Rennes Métropole, Lannion Trégor Communauté et Brest Métropole, BCom explore, conçoit et fournit les technologies numériques au service des grandes filières industrielles européennes au croisement de six piliers : connectivité, cybersécurité, jumeau numérique, immersion/interaction, informatique du futur et intelligence artificielle.

Si le volet de l'Intelligence artificielle sera abordé plus longuement lors de ce colloque, notamment pour la partie IA de confiance, l'IA embarquée fait également l'objet de développements très importants, nous permettant de viser de façon crédible 15% de part du marché mondial en 2030. Nous avons ainsi réussi à créer sur ce segment essentiel

1 : Scikit-learn est une bibliothèque libre destinée à l'apprentissage automatique. Elle est développée par de nombreux contributeurs, notamment dans le monde académique par des instituts français d'enseignement supérieur et de recherche comme Inria3. Elle propose dans son framework de nombreuses bibliothèques d'algorithmes à implémenter, clé en main. Ces bibliothèques sont à disposition notamment des data scientists.

une dynamique de construction de l'offre et des travaux combinant recherche publique et privée, comme avec Scikit Learn[1] qui va devenir l'une des principales bibliothèques de machine Learning capable de rivaliser avec celle de Meta ou de Google.

La construction d'une offre souveraine en matière numérique dépend tout d'abord des investissements que l'on peut consentir. A ce titre, au titre du programme France 2030, environ 10 milliards d'euros de financement sont mobilisés pour soutenir le développement de cette offre. Elle dépend également des ressources humaines et des compétences nécessaires pour toutes les entreprises impliquées. Là encore, des réponses très concrètes sont apportées, notamment via la démarche dite « Compétences et métiers d'avenir », dotée de 2,5 milliards d'euros et qui permettra par exemple de former d'ici 2025 9 200 spécialistes de cybersécurité supplémentaires et 3 700 diplômés en IA. En parallèle, des efforts très importants sont menés pour inclure des modules sur l'intelligence artificielle ou sur la cybersécurité au sein de formations généralistes.

Le deuxième pilier porte sur l'environnement réglementaire qui va permettre d'assurer cette souveraineté numérique, visant trois objectifs essentiels.

Le premier objectif porte sur la protection de nos actifs stratégiques. De nombreuses réalisations concrètes ont été mises en place ces dernières années comme la loi sur la sécurité du réseau de télécommunications, permettant une évolution très significative des parts de marché des acteurs européens dans nos réseaux 5G. Les nombreuses réglementations européennes sur la cybersécurité, telles que la directive NIS 2, le Cyber Resilience Act ou le Cyber Security Act vont permettre de renforcer très nettement à la fois les exigences imposées aux acteurs économiques, notamment en termes de sécurité et de cyber sécurité, mais également les exigences vis-à-vis des fabricants, des vendeurs de produits numériques afin de réhausser globalement le niveau de cybersécurité en Europe.

Une démarche analogue est poursuivie sur le Cloud, élément essentiel de la numérisation de l'économie, avec une démarche assez unique en France autour du label SecNumCloud[2]. Ce label permet ainsi d'assurer à la fois un très haut niveau de sécurité et de cyber sécurité du Cloud, mais également une immunité aux lois extraterritoriales, notamment américaine et chinoise. Enfin, la France agit au niveau européen pour que ce label soit adopté et mis en œuvre en Europe.

Cette protection des actifs stratégiques se pratique également au quotidien via la politique de sécurité économique déployée par la France. Cette politique vise à ce que chaque menace par exemple de rachat ou de transfert forcé de technologie sur une entreprise stratégique en France ou sur un laboratoire de recherche appelle immédiatement une réponse. Développée depuis trois ans, cette politique a permis de répondre à 700 alertes de sécurité économique sur nos actifs stratégiques, notamment les actifs numériques avec un très bon résultat en termes de niveau de protection.

Le second objectif de cet effort de régulation est économique afin de permettre de renforcer la concurrence dans le monde numérique, de permettre de limiter, voire d'annuler les effets d'abus de position dominante des grandes plates-formes Internet américaines. Ainsi, adoptés pendant la présidence française de l'Union Européenne, les règlements DMA et DSA permettent désormais à des entreprises françaises ou européennes de développer et proposer des services numériques innovants dans de nombreux domaines où il n'était plus possible de le faire.

Le troisième objectif concerne la protection de nos valeurs. La souveraineté numérique consiste à permettre à l'Union Européenne de faire respecter ses valeurs dans l'espace numérique. A titre d'illustration, le règlement DSA constitue la base de la réglementation sur l'IA, actuellement en cours de négociation.

---

2 : La qualification SecNumCloud de l'ANSSI s'adresse aux prestataires de services cloud souhaitant démontrer un niveau de sécurité parmi les plus élevés du marché. Cette qualification est en phase avec les attentes des Organismes d'Importance Vitale. Liée à un Visa de Sécurité, elle est la prestation d'excellence des services cloud. Basée sur la structure de la norme ISO/IEC 27001, ce référentiel s'inscrit dans la stratégie nationale française pour un cloud de confiance et le Cybersecurity Act de l'Union Européenne (https://certification.afnor.org/numerique/qualification-secnumcloud)

Le troisième pilier de cette souveraineté concerne le déploiement du numérique dans le tissu économique. Ce déploiement constitue clairement un outil de compétitivité pour nos acteurs économiques. Nos objectifs sont importants : ainsi, en matière de cyber sécurité, nous prévoyons de doubler entre 2019 et 2025, le nombre de petites entreprises de moins de 50 salariés qui ont recours à trois systèmes de protection cyber. De plus, notamment dans les secteurs de l'énergie et aérospatial, nous accompagnons plus de 750 PME et ETI parmi les plus menacées dans la mise en œuvre de projets cyber d'envergure. Nous avons également un programme important en matière d'intelligence artificielle : ainsi, un grand nombre de PME peuvent désormais intégrer des solutions d'intelligence artificielle et avoir des applications utiles en matière de 5G. Enfin, pendant le plan de relance, nous avons accompagné un quart de la totalité des PME industrielles françaises dans la numérisation de leur outil de production avec la même conscience du lien très fort entre numérisation et compétitivité et entre compétitivité et souveraineté.

En conclusion, il convient de souligner les importants progrès que nous avons réalisé sur l'ensemble de ces trois piliers avec des résultats très concrets, notamment durant les quatre dernières années, même si, bien entendu, il nous reste évidemment des défis majeurs sur chacun de ces piliers.

Ainsi, en ce qui concerne l'offre numérique, l'actualité nous montre qu'avec GPT4, nous devons sans cesse renouveler nos efforts d'anticipation des ruptures technologiques et d'identification des acteurs porteurs de ces ruptures technologiques et anticiper le soutien pour le développement de leurs offres.

A propos de régulation, des progrès historiques ont été enregistrés au niveau européen, en matière d'autonomie stratégique et de régulation du numérique. Le corpus de régulation du numérique en Europe est sans précédent, unique au monde, même si nous pouvons encore constater des clivages très importants entre les pays du Nord et du Sud de l'Europe sur l'appréciation de la nécessité et l'acceptabilité de ces régulations. Notre effort doit donc être sans cesse renouvelé, d'autant plus que les autorités américaines, elles-mêmes attachées à leur souveraineté numérique, challengent notre légitimité à mettre en œuvre des régulations européennes, par exemple sur le Cloud.

Enfin, le troisième défi porte sur l'intégration de solutions numériques par les entreprises françaises pouvant aboutir à l'émergence d'offres industrielles françaises compétitives. C'est ici à la fois un enjeu de diffusion et un enjeu d'orientation vers l'offre française.

TABLE RONDE 1 :

Les technologies numériques au service des usages opérationnels

Animateur :
Thibaut Lajoie-Mazenc

Intervenants :
IGA Dominique Luzeaux (MINARM/AND), GDA Philippe Dedobbeleer (EMA), Hélène Chinal (CAP Gemini), IGA Thierry Baud (Airbus Defense & Space)

La continuité numérique

L'enjeu principal du numérique au service des usages opérationnels est celui de la continuité, qui se décline en quatre volets.

1. La continuité verticale : dans une opération militaire, les ordres descendent du niveau politique et sont progressivement déclinés aux niveaux stratégique puis opératif avant d'être exécutés au niveau tactique. Les systèmes numériques doivent servir de socle commun à ces différents niveaux pour passer efficacement d'un niveau à l'autre.

2. La continuité horizontale : les affrontements se déroulent aujourd'hui en "multi-milieu multi-champ" (M2MC), c'est-à-dire qu'ils ont lieu sur terre, dans les airs, sur la mer, dans l'espace et le spectre électromagnétique, mais également dans les champs cyber et informationnel. Les systèmes numériques doivent également aider à coordonner les actions dans les différents milieux et champs, y compris avec les alliés dans les opérations en coalition ou avec les autres services de sécurité dans les opérations sur le territoire national.

3. La continuité d'usages : qu'il soit en métropole, en outre-mer ou à l'étranger, tout opérateur doit disposer d'outils similaires pour réaliser son métier, le numérique devant être une aide et non une contrainte. Les systèmes numériques doivent donc gérer la complexité liée à la différence d'infrastructure : ainsi, le raccordement aux réseaux du ministère des Armées est très différent selon que l'on se trouve à Paris, Kourou ou en opérations extérieures, mais SIA (le Système d'Information des Armées) permet à ses utilisateurs de travailler sur la même interface dans les trois cas.

4. La continuité de maîtrise technologique : de la production d'une donnée à son exploitation, il est nécessaire de comprendre et maîtriser la chaîne complète de l'information pour maximiser son utilité. Ainsi, la chaîne image de la constellation Pléiades Néo offre des images satellites d'une très grande précision grâce à une connaissance approfondie du capteur et des différents systèmes de transmission permettant d'acheminer les images jusqu'aux opérateurs.

GDA Philippe Dedobbeleer (MINARM/EMA) et IGA Dominique Luzeaux (MINARM/AND).

La combinaison de ces quatre volets permet d'acquérir la supériorité informationnelle sur l'adversaire, c'est-à-dire pour que notre boucle décisionnelle OODA (observation, orientation, décision, action) soit plus rapide et efficace que celle de l'adversaire. Cela fait partie des éléments clés pour la victoire dans un affrontement.

Les spécificités du domaine militaire

Hélène Chinal, Head of Transformation Southern and Central Europe SBU, Capgemini.

Le numérique militaire a quelques spécificités qui le différencient du numérique civil grand public. Historiquement, chaque niveau hiérarchique avait besoin de ses propres outils ; c'est de moins en moins vrai, principalement grâce à la prise en compte du **besoin de continuité verticale** et à l'amélioration des composants permettant de **réaliser de nombreux traitements au niveau du combattant**, qu'il soit débarqué ou dans un avion de chasse. Cependant, les contraintes d'environnement (volume, surface, chaleur, énergie) demeurent : un fantassin ou un avion ne pourront pas embarquer les mêmes systèmes qu'un poste de commandement en métropole.

Par ailleurs, la doctrine, les très nombreuses interfaces spécifiques et les habitudes des opérateurs entrainent deux conséquences. Premièrement, **l'adaptabilité des systèmes et l'injection de nouvelles technologies sont des sujets indispensables mais non triviaux**. Ainsi, SAER, système de renseignement déployé depuis de très nombreuses années, évolue encore régulièrement en termes de fonctions et de briques technologiques pour continuer de répondre au besoin des forces : à titre d'illustration, plusieurs équipes travaillent actuellement à trouver la place de la 5G dans les opérations. **Ensuite, la montée en compétence d'un nouvel acteur industriel dans le domaine est complexe, et ceux déjà installés s'appuient sur des équipes largement dédiées au monde de la défense.**

IGA Thierry Baud, Directeur Commercial France, Airbus Defence and Space.

La souveraineté

La souveraineté consiste à choisir ses indépendances et à accepter ses dépendances. **Une cible raisonnable pour la France est de bâtir sa souveraineté numérique à l'échelle européenne** : il semble impossible de rivaliser seul sur l'ensemble du spectre numérique avec les États-Unis quand les GAFAM investissent chacun de l'ordre de 10 milliards de dollars par an. Pour cela, la France dispose de partenaires sérieux : l'Italie, l'Allemagne, le Royaume-Uni qui, malgré le Brexit, reste un allié crédible et de longue date.

Le numérique souverain, comme l'agriculture biologique, coûte nécessairement plus cher que son homologue conventionnel. Son surcoût doit cependant rester raisonnable pour que l'investissement soit envisageable : en termes financiers, il doit rester inférieur à 10%, sans quoi il devient rédhibitoire. Ensuite, les performances et l'intégration doivent être au rendez-vous : ce point constitue l'un des succès des suites Office et Google. Un acheteur ne doit pas avoir à se poser de questions sur la capacité à faire fonctionner ensemble des briques distinctes, et il sera difficile de demander à des agents habitués aux outils numériques de travailler sur des versions trop dégradées pour répondre à l'objectif de souveraineté.

Enfin, **une fois le choix de la souveraineté réalisé, il est nécessaire de l'assumer** : les investissements doivent être réalisés de manière conséquente et pérenne, et des directives d'utilisation doivent être déclinées dans les différents organismes publics concernés : cela vaut pour le ministère des Armées, mais également pour l'ensemble des autres ministères, régaliens ou non.

Hervé Guillou, Président d'Exail, Ancien Vice-Président du CGARM

KEYNOTE
« Enjeu de compétences dans le numérique au sein de l'Etat »
Vincent Tejedor

Les constats :

Le numérique est omniprésent dans l'État, en tant que moyen et en tant qu'outil de politique publique. De plus, les besoins RH sont en augmentation aussi bien en quantité (évolution des usages, transformation des organisations) et en qualité (renouvellement rapide des technologies). Or, la dépréciation des compétences est rapide et le flux de formation peu élastique : le stock disponible est donc limité. Enfin, ces ressources sont très convoitées au même moment par le secteur privé (France et international) et public (autres ministère et MinArm). En synthèse, le prix de ces ressources augmente car elles sont rares et recherchées.

La stratégie du MINARM est dérivée du rapport CGE-IGF[1] sur les compétences numériques de l'État.

Attractivité et fidélisation

Il convient donc de développer une image de marque du « Numérique des armées » afin de favoriser l'attractivité. Ainsi, pour les contractuels, les salaires du public sont faibles par rapport au privé. En réponse, nous appliquons la grille DINUM (56 métiers) pour le recrutement ou lors des renouvellements de contrats afin d'éviter la concurrence au sein du secteur public.

Pour les militaires, une prime de compétences spécifiques militaires (PCS MIL) « Supériorité opérationnelle numérique » est à l'étude. Le personnel civil titulaire aura un traitement équivalent au travers d'une indemnité de fonction, de sujétion et d'expertise (IFSE) complémentaire.

Recrutement

Plusieurs leviers sont actuellement en cours de mise en œuvre. Il est prévu de développer une réserve opérationnelle numérique, pouvant devenir par la suite un nouveau vivier de recrutement, d'élargir le recours aux commissionnés (militaire recruté par contrat pour satisfaire des besoins immédiats et occuper des emplois de spécialistes à caractère scientifique, technique ou pédagogique qui ne sont pas pourvus par les autres modes de recrutement et de formation). De plus, un effort particulier est en cours pour le recrutement de 3 000 apprentis au sein du MINARM, mais il convient de constater que peu signent ensuite un contrat. En réponse, la DRH-MD a lancé des actions visant à proposer une embauche ferme aux apprentis de la famille professionnelle SIC, 6 mois avant la fin de l'apprentissage.

Enfin, nous prévoyons de définir les compétences associées en matière de nouvelles technologies (IA, quantique…) afin de bien identifier les nouvelles cibles de recrutement.

Formation continue et reconversion (« reskilling »)

Un outil spécifique PIX (auto évaluation/certification) est en cours de déploiement au sein du MinArm de l'outil afin de bien détecter nos talents. En parallèle, une Académie du numérique (ADN) propose plusieurs offres pour permettre la formation continue et offrir des cursus de reconversion :

- Premiers parcours de formation « chef de projet » et « Architecte d'entreprise » en 2023,
- Animation de communautés apprenantes
- Création de capsules et de webinaires pédagogiques, de vidéos sur ADN.TV…

Il est également prévu de développer des parcours de formation afin d'intégrer les technologies émergentes. Enfin une action sera lancée pour définir les compétences critiques nécessaires pour former les personnels aux technologies émergentes (Big Data, IA, Cloud…) et proposer des parcours de reconversion aux agents dont la formation initiale et la première partie de carrière ne relèvent pas du domaine numérique.

1 : Conseil Général de l'Economie – Inspection Général des Finances (https ://www.transformation.gouv.fr/files/ressource/Rapport_filiere_numerique_Etat_20230616.pdf)

La Confédération Amicale des Ingénieurs de l'Armement

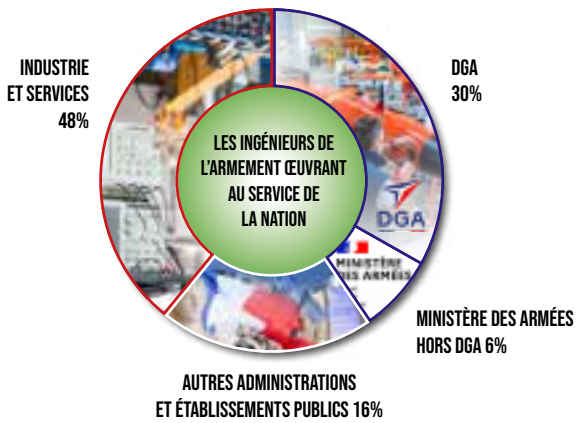
Qui sommes-nous ?

La Confédération Amicale des Ingénieurs de l'Armement, ou CAIA, est une association sans but lucratif, créée en 1969 après la naissance du Corps des ingénieurs de l'armement.

La CAIA regroupe essentiellement des membres ou anciens membres du corps des Ingénieurs de l'Armement ou de ses anciens Corps constitutifs, et des membres associés, personnes physiques ou morales ayant un intérêt pour les buts de l'Association, soit près de 3 000 personnes aujourd'hui.

Le graphique ci-contre donne la répartition par nature d'employeur des près de 1 800 ingénieurs de l'armement aujourd'hui en activité.

Ces derniers sont répartis au sein de la DGA (30%), le ministère des Armées hors DGA (6%), d'autres administrations et établissements publics (16%) et enfin les industries et services 48%).



Les principales missions de la CAIA

La CAIA a pour objet d'œuvrer au profit de ses membres d'une part et de la société française d'autre part en visant à :

- **Resserrer les liens de camaraderie et de solidarité entre les membres et anciens membres du corps des Ingénieurs de l'Armement** et de leur venir en aide, en cas de besoin, ainsi qu'à leurs familles ;
- **Participer pleinement à la cohésion du Corps de l'Armement et au renom des Ingénieurs de l'Armement** auprès des responsables administratifs et de la société civile afin de permettre une meilleure exploitation de leurs compétences au service de l'Etat et dans l'intérêt de la nation ;
- **Proposer, en particulier à l'ensemble de ses membres, un ensemble d'activités permettant d'améliorer la compréhension mutuelle** du fonctionnement des secteurs public et privé de notre nation en vue de renforcer l'efficacité de leur coopération au bénéfice de la nation.
- **Contribuer au renforcement de la connaissance et de la réflexion sur les problématiques de défense, d'armement et de sécurité** au profit de ses membres et, plus généralement de la société civile en France et auprès de partenaires internationaux majeurs.
- **Renforcer les liens entre ses membres et les membres d'associations ayant un champ d'action voisin du sien**, dont les associations d'officiers des Armes, les associations d'ingénieurs de l'Etat, les associations de hauts fonctionnaires et les associations d'anciens élèves d'écoles d'ingénieurs, afin de renforcer l'efficacité de la contribution de ses membres au profit des services de l'Etat.

La gouvernance de la CAIA

Sous l'autorité d'un conseil d'administration de 25 membres, la CAIA est dirigée opérationnellement par un Bureau dont les membres sont les suivants :

Les principales activités de la CAIA

Les activités de la CAIA visent à soutenir l'accomplissement de ses principales missions, et notamment celle d'améliorer, au travers des ingénieurs de l'armement, la compréhension mutuelle du fonctionnement des secteurs public et privé de notre nation en vue de renforcer l'efficacité de leur coopération au bénéfice de notre pays.

Sous la responsabilité d'une équipe d'organisation dédiée, la CAIA organise chaque année à l'automne un grand gala, **le Gala de l'Armement**, qui se tient dans un lieu de prestige à Paris ou dans ses environs (Hôtel Intercontinental Grand Paris, château de Versailles, Automobile-Club de France). Ce gala réunit près de 500 hautes personnalités politiques, administratives, industrielles françaises et européennes du domaine de l'armement.

Sous la responsabilité d'une équipe d'organisation dédiée, la CAIA organise traditionnellement tous les deux ans un **colloque sur un thème d'intérêt majeur** pour notre communauté. Ce colloque est ouvert aux ingénieurs de l'armement ainsi qu'aux responsables administratifs et industriels relevant du domaine traité. Ainsi, la CAIA a organisé un colloque sur le thème « Reconquérir la souveraineté » en 2021 et sur le thème « Le numérique, une arme de souveraineté pour l'Etat » en 2023.

Sous la responsabilité de son comité de rédaction, la CAIA publie chaque années trois numéros du **Magazine des ingénieurs de l'Armement**. Diffusé à tous les IA et à plus d'un millier de personnalités françaises et étrangères, ce magazine fait le point sur un dossier majeur du domaine de l'armement et présente les principales actions de notre association. Les thèmes des derniers numéros parus furent les suivants : **Projets et numérique, Passion armement** et **L'indispensable dualité**.

Depuis quelques années, la CAIA a considérablement renforcé son **Action vers les jeunes IA**. Cette action recouvre *l'accueil des nouveaux IA* en provenance de l'Ecole polytechnique, ou admis sur titre ou en promotion interne. Ces rencontres permettent de leur présenter la CAIA et les principaux enjeux de notre corps. Elle s'est récemment étendue à la mise en place *d'afterworks,* permettant des échanges informels entre jeunes IA (moins de 35 ans).

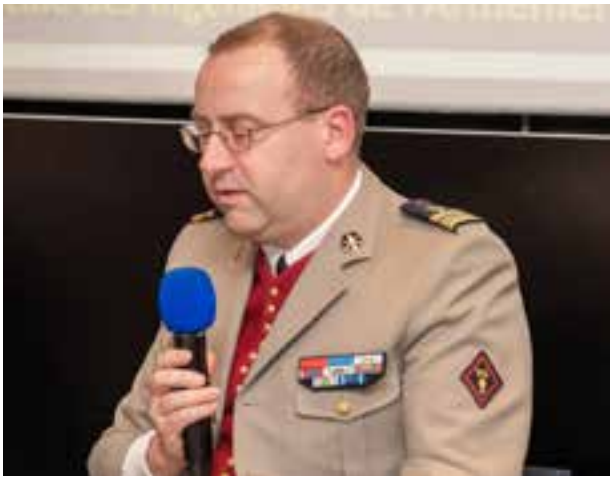
Enfin, la CAIA a lancé depuis début 2023 :

- un cycle de **diners-débats** réunissant les IA et leurs conjoints autour d'une personnalité IA du monde administratif ou industriel. Ces diners-débats permettent une ouverture des ingénieurs de l'armement sur des problématiques majeures portées par les personnalités invitées. Les intervenants 2023 furent successivement Marwan Lahoud, Guillaume Poupard, Nicolas Chamussy, Jean-Brice Dumont et, à titre exceptionnel, Emmanuel Chiva.
- la mise en place de **groupes régionaux** visant à permettre à nos camarades provinciaux de pouvoir participer à des rencontres, visites dans les régions considérées. Les groupes Aquitaine, PACA, Bretagne ont été…??
- une offre de mentoring de **Mentoring** dont la première vague réunit 18 premiers couples de mentors et mentorés.
- Un **pôle réflexion** visant à publier des courtes notes de synthèse et de recommandations de la CAIA sur des problématiques majeures concernant le domaine de l'armement. Les quatre premiers thèmes en cours de réflexion sont les suivants : Politique de déontologie des IA, Politique industrielle dans le domaine de l'armement, la féminisation du corps de l'armement. l'indispensable expertise technique de la DGA : comment l'acquérir, l'entretenir et la pérenniser ?
- Un **Comité Histoire**, qui vise à relancer le travail de mémoire dans le domaine de l'armement, en synergie avec les actions de même nature menées par le Minarm et les industriels de l'Armement.

TABLE RONDE 2 :
L'IA de confiance

Animateur :
Baptiste Chomel de Jarnieu

Intervenants :
Guillaume Avrin (DGE), Marko Erman (Thales), Colonel Jean-Gabriel Herbinet (EMA), Yonathan Teboul (MBDA)



Col. Jean-Gabriel Herbinet, Adjoint du Bureau Numérique, EMAT

Utilisation actuelle d'IA dans les systèmes d'armes

La première phase de la table ronde a été consacrée à une mise en contexte de l'utilisation d'IA dans les systèmes d'armes français. Par manque de temps, l'objectif n'était pas d'être exhaustif mais de donner quelques exemples. Nous avons également abordé le cas particulier de l'IA générative et de ses éventuelles applications au cours des prochaines années.

Le terme d'intelligence artificielle est très employé depuis quelques années avec le développement du Machine Learning, mais il regroupe en réalité un spectre plus large de techniques d'optimisation datant de la fin du 20e siècle. Yonathan Teboul a cité l'exemple du missile de croisière SCALP, développé par MBDA, qui a intégré dès la fin des années 1990 des techniques de « scene matching », permettant d'identifier une cible en comparant des données infrarouges captées par le missile avec des images satellitaires enregistrées. Les véritables avancées sur ces briques de traitement d'image seront de réduire de quelques jours à quelques minutes le temps de préparation de mission avec davantage de précision grâce à des algorithmes plus puissants.

L'Armée de Terre exploite également depuis de nombreuses années les techniques d'optimisation offertes par les premiers algorithmes. **Le colonel Herbinet** a cité en exemple les calculateurs d'artillerie ATLAS (Automatisation des Tirs et Liaisons de l'Artillerie Sol/sol), ainsi que les algorithmes de déclenchement de tir et de mise de feu du char Leclerc. Dans le passé, des algorithmes étaient également utilisés au sein de l'Armée de Terre pour l'optimisation des mouvements au niveau tactique mais la réduction du format des armées a rendu leur usage moins nécessaire.

L'expérience acquise au fil du temps par l'utilisation de ces algorithmes a souligné d'une part l'importance de l'adoption des techniques par les utilisateurs, et d'autre part la nécessité de joindre les connaissances techniques de programmation à l'expertise métier au cours du développement des systèmes.

Parmi les progrès récents en matière d'intelligence artificielle, l'IA générative constitue pour certains une révolution technologique. Les algorithmes de ChatGPT fournissent par exemple des résultats très performants pour la génération de textes ou d'images. Au cours de son intervention, Marko Erman nous a confié que Thalès s'est penché en particulier sur l'IA générative permettant de faire du développement logiciel et les premiers résultats sont très convaincants. Cependant, son utilisation ne peut pas se faire à n'importe quelle condition. Cela dépend notamment

de la criticité des cas d'usages. En effet, les algorithmes de ChatGPT reposent sur des techniques d'apprentissage classique dont les résultats sont obtenus sur la base de corrélation et non de causalité. Ces algorithmes ne donnent pas encore de garantie sur le niveau de confiance de la réponse. Il faudra donc toujours une relecture humaine très importante, représentant dans le cadre de ChatGPT un coût de plusieurs centaines de millions de dollars.

Outre les applications potentielles pour le développement des systèmes de défense, Marko Erman a insisté sur les dangers que font naître ces algorithmes d'IA générative comme la création de *fake* de plus en plus réalistes par des organisations malveillantes et que les réglementations ne pourront pas complètement contrôler. Il faudra donc réfléchir à la manière de faire face à ces dangers en bâtissant des solutions européennes de meilleure confiance, ainsi que des outils capables de déceler l'origine du résultat.

Attentes d'une IA de confiance

A l'échelle internationale, aucune définition de l'IA de confiance ne fait encore consensus. Nous ne nous sommes donc pas attardés à la définir mais nous avons abordé quelques-unes des attentes qui se cachent derrière le concept.

Selon **Guillaume Avrin**, coordinateur national de la Stratégie Nationale d'Intelligence Artificielle (SNIA), il est possible de distinguer **trois types d'exigence associés aux systèmes employant de l'IA**. C'est par la combinaison de ces trois types d'exigence que l'on pourra définir une intelligence artificielle de confiance.

La première exigence concerne le produit. Au sein de l'Union Européenne, la mise sur le marché d'un produit nécessite une certification « CE » (conformité européenne). Cela garantit que le système est conforme à des exigences telles que la résilience ou la robustesse. Dans le cadre de l'IA, cela n'est pas suffisant à cause des performances non linéaires du Machine Learning, un petit changement de paramètre pouvant totalement modifier le fonctionnement du système.

La seconde exigence concerne les processus, qui imposent des conditions sur les différentes phases de vie du système, telles que le développement ou le maintien en condition opérationnelle. La France et l'Europe connaissent des avancées rapides dans ce domaine.

La dernière exigence concerne les compétences, c'est-à-dire les personnes aptes à développer ou utiliser les algorithmes d'intelligence artificielle. Les États Unis sont nettement en avance sur l'Europe en la matière.

Au cours de son intervention, Yonathan Teboul a relevé plusieurs notions à intégrer dès le développement des algorithmes d'IA pour apporter de la confiance dans le système. Tout d'abord, il est important de mettre au point des outils et méthodes développés en France et employés à l'échelle internationale, pour que l'ingénieur puisse développer et maîtriser l'IA en confiance. La responsabilité humaine doit ensuite rester au cœur des décisions et actions effectuées par le système. Cela implique que les humains soient en mesure de comprendre et de contrôler l'IA. Un autre point important et particulièrement sensible dans le cadre de la défense est de développer le système en totale transparence avec les autorités de qualification, afin de rendre les processus décisionnels de l'IA explicables et compréhensibles pour les utilisateurs. Il faut s'assurer enfin de pouvoir disposer d'un socle de données souveraines et en quantité suffisante pour entraîner les algorithmes.

Stratégie du gouvernement

Au cours de la troisième partie de cette table ronde, les intervenants ont présenté la feuille de route nationale concernant l'intelligence artificielle et comportant notamment un volet important consacré à l'IA de confiance.

Le développement d'une IA de confiance en France fait partie intégrante de la Stratégie Nationale d'Intelligence Artificielle lancée par Emmanuel Macron en 2018 à la suite de la remise du rapport de Cédric Villani. Guillaume Avrin en est le coordinateur depuis janvier 2023 et nous a présenté les grandes lignes des deux phases de cette politique depuis son lancement en 2018.

Guillaume Avrin, Coordinateur National pour l'Intelligence Artificielle, DGE.

L'objectif de la première phase, déroulée de 2018 à mi 2022, était de structurer l'écosystème de l'IA pour maximiser l'impact des actions entreprises en évitant les redondances et en positionnant les acteurs sur les enjeux jugés stratégiques. Lors de cette première phase, un volet important a été consacré à l'IA de confiance avec le lancement d'un Grand Défi qui a mené notamment au développement du collectif « Confiance.AI ».

Depuis mi-2022, l'objectif de la seconde phase de la SNIA consiste à diffuser l'IA au sein de l'économie et à l'intégrer sur notre territoire pour gagner en compétitivité et répondre au besoin de nos armées. Guillaume Avrin a présenté trois leviers sur lesquels s'appuie cette seconde phase : la formation, le soutien à l'offre deeptech et le rapprochement entre l'offre et la demande en mobilisant les intermédiaires comme les banquiers, les assureurs et les centres d'essais. Lors de cette seconde phase, de nouveaux dispositifs ont été mis en place pour développer l'IA de confiance. Le 29 mars 2023, Jean-Noël Barrot, Ministre délégué chargé de la transition numérique et des télécommunications, a par exemple lancé un appel à projets « Démonstrateurs d'intelligence artificielle de confiance (DIAC)» pour démontrer qu'il est possible d'intégrer des briques d'IA dans des systèmes critiques.

Marko Erman, Chief Scientific Officer SVP, Thalès.

Marko Erman a ensuite présenté en détail le programme Confiance. AI, qui fait partie intégrante du Grand Défi IA de confiance lancé avec la SNIA en 2018. Thalès est un acteur majeur de ce collectif dont l'objectif est de s'attaquer à l'ingénierie de l'IA, c'est à dire à la méthodologie à l'architecture et aux outils logiciels permettant l'insertion des algorithmes d'IA dans les systèmes complexes. Si les premiers travaux ont permis d'établir un cadre pour le Machine Learning sur des systèmes à criticité « faible », les projets actuels s'attaquent à l'IA symbolique et hybride pour des systèmes à criticité « élevée ». Le programme se concentre en particulier sur quatre industries développant des systèmes critiques : la défense, l'énergie, la mobilité et l'industrie 4.0. Le collectif est composé de grands groupes industriels (pour la défense Naval Group, Airbus, Safran et Thalès), de laboratoires de recherches ainsi que de dizaines de PME et startups. Le consortium est également très présent dans les discussions de standardisation à l'échelle internationale pour établir les normes autour de l'IA de confiance.

Qualification

Une des problématiques importantes de l'IA de confiance est la qualification des systèmes comprenant de l'IA. Avec le développement exponentiel des techniques d'intelligence artificielle, cette qualification doit se penser dès la phase de développement et ne pourra pas se faire avec les méthodes utilisées jusqu'à présent. Selon Guillaume Avrin, les spécificités de l'IA et en particulier du Machine Learning imposent de revoir les méthodologies de qualification des systèmes intégrant des briques d'intelligence artificielle. Tout d'abord, les domaines de fonctionnement de ces systèmes sont très larges et il est donc difficile (notamment dans le cadre de l'apprentissage automatique) de les qualifier formellement. D'autre part, en raison du caractère non linéaire du Machine Learning, il est impossible d'extrapoler le comportement d'un système à partir de quelques points de fonctionnement. Il est donc nécessaire de parcourir un très grand nombre de scénarios, ce qui implique de disposer d'environnements de tests importants. Les développements récents de l'IA générative ont mis en lumière les milliards de paramètres des nouveaux algorithmes d'IA. Ce changement de dimension ne rend plus possible l'évaluation « boite blanche » d'un système, et il est donc obligatoire d'en évaluer le comportement « boite noire » par entrée – sortie. Enfin, les capacités d'apprentissage continu des algorithmes impliquent de devoir ré-évaluer régulièrement les systèmes tout au long de leurs cycles de vie.

En synthèse, le besoin principal pour ces nouveaux systèmes est de caractériser leurs domaines de fonctionnement en parcourant un très grand nombre de scénarios de test grâce au couplage des approches de simulation (non réalistes) et de mise en situation réelle (non exhaustives). Le Colonel Herbinet a ensuite souligné l'importance de la qualification d'un point de vue opérationnel car elle conditionne l'emploi du système au combat. D'une part, il est nécessaire de qualifier l'IA dans le système, mais également le système intégrant l'IA. En plus de la qualification d'un système, ce dernier a abordé une nouvelle notion : sa validation. Au cours de son emploi opérationnel, le paramétrage des algorithmes d'un système devra évoluer pour s'adapter au combat et gagner la bataille. Il est donc nécessaire de mettre au point des procédures de validation de paramétrage pour définir si les algorithmes sont correctement paramétrés et employables dans les conditions du moment.

Enjeu des données

Enfin, dans la dernière partie de cette table ronde, nous nous sommes intéressés au sujet de la donnée, central pour l'IA. Les intervenants ont notamment abordé les questions de sa disponibilité et de son partage, particulièrement sensibles en matière de défense.

Yonatan Teboul, Responsable Groupe du Digital pour les produits et les services, MBDA

Un des enjeux du développement des algorithmes d'IA est d'obtenir en quantité suffisante des données représentatives des conditions opérationnelles. Ces dernières sont souvent uniques et complexes, et il peut être difficile de collecter des données exhaustives et précises. De plus, certaines données opérationnelles sont sensibles ou classifiées, ce qui limite leur disponibilité pour l'entraînement des algorithmes. **Yonathan Teboul nous a confié qu'une solution employée depuis quelques années chez MBDA est l'utilisation de données synthétiques**, notamment pour les campagnes d'essais lors des phases de tests. Les données open source peuvent aussi résoudre le problème de disponibilité, même si cela peut être délicat pour certaines applications sensibles en raison des vulnérabilités que cela peut engendrer sur le système. Des experts du domaine ayant une compréhension approfondie des conditions opérationnelles et des systèmes en place peuvent par ailleurs être nécessaires pour effectuer une labellisation précise et fiable des jeux de données.

D'après le colonel Herbinet, les données détenues en temps de paix par les pays sont déjà suffisamment représentatives de celles que l'on pourrait connaitre lors d'un conflit : le partage des données entre alliés n'est donc pas nécessaire. En revanche, dans l'hypothèse d'un engagement majeur qui se fera certainement dans le cadre d'une coopération, chaque pays aura intérêt à partager et se faire partager les données les plus représentatives du conflit pour que toutes les unités soient préparées au mieux. Il faudra ensuite réentraîner les algorithmes sur ces données délivrées par des forces étrangères. Cela signifie qu'il y a un travail à prévoir entre alliés sur la structuration et la documentation des données, ainsi qu'un cadre de partage pour que la mise à jour soit faite en confiance, sous réserve que cette notion de confiance soit la même pour tous les pays.

TABLE RONDE 3 :
Lever le voile sur la cyber

Animatrice :
IA Pauline Emschwiller

Intervenants :
GDI Aymeric Bonnemaison (COMCYBER), IGA Bruno Marescaux (DGA), Patrick Radja (Naval Group), ICA Frédéric Grelot (GLIMPS)

L'industrie de la défense est aujourd'hui confrontée à une réalité indéniable : l'ère digitale a fait émerger un nouveau front de bataille, celui du cyberespace. Face à ce défi sans précédent, les armées et la DGA se retrouvent en première ligne comme le montre l'exemple du cas Viasat[1]. Le 24 février 2022, une heure avant le début de l'attaque en Ukraine, l'entreprise américaine Viasat a été cyberattaquée. Les forces armées ukrainiennes s'appuyaient sur leur technologie pour le commandement des opérations. La cyberattaque a été un outil simultané à l'attaque russe sur le terrain. La table ronde intitulée «Lever le voile sur la cybersécurité» avait donc pour but de revenir sur ce domaine encore confidentiel des nouveaux conflits hybrides.

Un écosystème étatique intégré et dynamique

GDI Aymeric Bonnemaison, COMCYBER, Ministère des Armées

Dans le domaine de la cybersécurité, l'Etat a mis en place un écosystème particulièrement actif et intégré. Il est structuré autour du C4 qu'on pourrait traduire par le « club des cyberdéfenseurs de l'Etat ». Il est composé de la DGA, du COMCYBER, de la DGSE de la DGSI et de l'ANSSI. Chaque membre possède un certain nombre de moyens et de compétences rares mis au service de différents projets. Par exemple, dans le cas de l'attaque Viasat, il y a eu des dommages collatéraux dans toute l'Europe et la DGA a mené une expertise sur les équipements pour analyser l'attaque.

Focus sur le COMCYBER

Le COMCYBER est le commandement en charge des opérations militaires dans le cyberespace dans lequel il utilise les 3 domaines de lutte (LID, LIO et L2I). Ce nouvel espace de conflictualité est un défi opérationnel de taille afin de préserver les invariants d'une conflictualité militaire et d'assurer la capacité des armées à agir.

Le Comcyber a également un rôle de conseiller ministériel en charge d'assurer la cohérence du modèle ministériel de cyber défense.

La cyberdéfense a été un élément majeur de la loi de programmation militaire (LPM) actuelle et son importance a été à nouveau soulignée pour la prochaine LPM (2024-2030). C'est un choix politique fort. La poursuite du développement de cette capacité s'appuie sur la coopération intense entre les différents acteurs. Elle agit dans tous les champs de la cybersécurité. Il y a à la fois la protection cyber des matériels des armées mais également les trois grands champs de lutte cyber que sont la lutte informatique défensive (LID), la lutte informatique offensive (LIO) et la lutte informatique d'influence (L2I). Ces champs nécessitent de détenir des capacités d'investigation sur les matériels attaqués, des capacités de détection des attaques, des capacités de défense et enfin des capacités de production d'effets cyberoffensifs.

1 : https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

La Cybersécurité à la DGA

La cyber constitue désormais l'une des 5 missions de la DGA. Elle repose sur 4 types d'activité :

- porter à un niveau adapté au niveau de la menace la cybersécurité des systèmes numériques et des systèmes d'armes afin d'être résilient aux agressions cyber ;
- équiper les forces armées de systèmes leur permettant d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace ;
- orienter, maintenir et développer les capacités technologiques et industrielles nécessaires ; contribuer à déployer la stratégie nationale cyber ;
- contribuer à la cyberdéfense de la Nation (C4).

IGA Bruno Marescaux, Chargé de mission Cyber auprès du Délégué Général pour l'Armement, DGA

Cet écosystème est au service des forces armées mais également de l'ensemble de la société française. En effet, les interactions numériques vont croissantes et il est essentiel d'augmenter le niveau de cybersécurité des entreprises françaises, en particulier de celles de la base industrielle et technologique de défense contre les menaces criminelles à but lucratif ou à but de renseignement qui peuvent avoir un impact direct sur la crédibilité des forces armées françaises. La cyber n'est plus un sujet réservé à quelques initiés, il atteint toutes les couches de notre société.

Les entreprises industrielles et l'armée, des partenaires privilégiés

La coopération n'est pas seulement entre les différents acteurs étatiques. En effet, elle s'étend aux entreprises industrielles, mais également aux établissements d'enseignement et de recherche. L'ensemble de l'écosystème doit donc travailler ensemble afin d'être plus résilient à cette nouvelle menace. Le caractère dual, global et versatile de la cyberdéfense oblige à partager sans cesse, à échanger notamment avec le monde de l'industrie. Il est intéressant ici de citer le cercle de confiance qui lie le ministère des armées avec huit maîtres d'œuvre depuis la signature, en 2019, d'une convention[2] de cyberdéfense, première avancée vers une indispensable coopération. Les grandes entreprises industrielles ont ainsi un rôle majeur à jouer dans ce nouveau champ de bataille numérique. Elles sont non seulement les principaux fournisseurs de solutions de défense, mais également des partenaires clés pour l'armée dans le développement de technologies de pointe, mais il est également de leur ressort de fiabiliser et de soutenir leurs sous-traitants face aux nouvelles menaces.

La Cybersécurité chez Naval Group

En tant qu'industriel, Naval Group a adopté une approche à 360°. Ainsi, la cybersécurité est considérée comme un véritable domaine de lutte, et donc comme une performance intrinsèque pour les navires, mais aussi pour leur écosystème, durant tout leur cycle de vie (conception, production, opération et maintenance). Cela concerne notamment les systèmes d'information, les méthodes de développement, les chantiers et bien entendu les fournisseurs, etc.-

En considérant la cyber comme un domaine de lutte, Naval Group se préoccupe de savoir comment pourrait faire un attaquant pour obtenir un effet recherché soit par une attaque directe soit au travers de rebond en exploitant les phases de conception (ex : via l'injection de code malveillant dans un logiciel), ou les phases de maintenance mais aussi en visant la supply chain pour compromettre ou exploiter des vulnérabilités d'équipements que nous utilisons ou des librairies logicielles.

Patrick Radja, VP Cybersecurity Director, Naval Group

Dans ce cadre, l'interaction entre l'armée et les entreprises industrielles a été identifiée comme un élément clé pour construire une défense solide en matière de cybersécurité. Il a été noté que l'adoption de pratiques de défense partagées et la mise en place d'une collaboration approfondie et proactive sont des éléments essentiels pour faire face à la menace grandissante des cyberattaques. Les produits doivent être « cyber by design ». C'est un enjeu important car cela impose de réduire les temps de cycle d'évolution numérique des systèmes de façon importante afin de sans cesse être capable de réagir à une menace qui évolue de façon continue et de corriger d'éventuelles vulnérabilités.

2 : Florence Parly, ministre des Armées, a conclu le 14 novembre 2019 une convention cyberdéfense entre son ministère et les sociétés Airbus, Ariane Group, Dassault Aviation, MBDA, Naval Group, Nexter, Safran et Thales.

L'implication grandissante des startups

Cette menace évolutive nécessite de s'appuyer sur les dernières technologies. Comme dit précédemment, la coopération doit aller jusque dans les laboratoires de recherche et doit encourager l'émergence de nouveaux outils et moyens. Il faut ici souligner différentes initiatives pour soutenir les start-ups du domaine : création de la Cyberdéfense factory en 2019 à Rennes, réalisation de défis cyber depuis 2018 avec l'Agence d'innovation de défense, etc. Cet équilibre entre grandes et plus petites structures est clairement à encourager.

Focus sur Glimps

Startup créée par 4 anciens experts du ministère des Armées en 2019, GLIMPS est un projet pilote de la Cyberdéfense Factory. Cette société propose une technologie unique de Deep Learning, conçue pour lire et comprendre les éléments qui composent un binaire. Cette technologie permet d'automatiser l'analyse de binaires et la détection des menaces en un clin d'œil.

ICA Frédéric Grelot, Co-Founder, Scientist Lead, GLIMPS

Les entreprises et les administrations sont aujourd'hui confrontées à des groupes d'attaquants de plus en plus armés pour contourner leurs solutions de cybersécurité. GLIMPS Malware répond à cette problématique et renforce les lignes de défense existantes grâce à une technologie de pointe capable de détecter les logiciels malveillants et leurs variants.

Les start-ups apportent une capacité d'innovation supplémentaire et une agilité importante. Aujourd'hui, les dispositifs d'amorçage et de soutien du début du développement, en particulier de soutien à la R&D, sont bien présents. Cependant, il est désormais nécessaire d'y ajouter des dispositifs et des financements pour aider à la commercialisation et à l'internationalisation de leurs produits. En effet, cela demande un effort financier important mais nécessaire pour permettre à ces jeunes entreprises de faire leurs preuves et de proposer des produits testés par les utilisateurs et approuvés. Ce n'est qu'ainsi que la France réussira à faire émerger des technologies souveraines et « à la page ».

Le défi de l'attraction des talents

La cybersécurité représente un défi technique de taille et, comme l'a déjà souligné Vincent Tejedor lors de son intervention, la table ronde a clairement souligné que la prochaine bataille sera l'attraction des talents. La pénurie est importante et commune à tous les acteurs. Les participants ont discuté des différentes stratégies pour attirer et retenir les meilleurs talents, notamment l'importance de l'éducation et de la formation. Il faut former davantage tout au long de la carrière les agents. Il faut également développer des filières d'excellence.

En parallèle de la formation, la cyber demandant une expertise forte, la fidélisation aura également un rôle clé, notamment au sein de l'Etat. Il pourrait également être proposé des parcours croisés entre les partenaires étatiques mais aussi privés.

En conclusion, la table ronde «Lever le voile sur la cybersécurité» a fait la lumière sur les défis et les opportunités que présente cette nouvelle réalité. Il est clair que la bataille pour la cybersécurité nécessite un effort concerté de tous les acteurs du monde de la défense. En adoptant une approche intégrée et dynamique, en établissant des liens solides entre l'armée et l'industrie, et en s'appuyant sur l'innovation des startups, le monde de la défense peut préparer efficacement le terrain pour faire face à ce nouveau défi. Le recrutement de talents en cybersécurité restera une priorité, et il ne fait aucun doute que ce domaine continuera d'évoluer et de se développer dans les années à venir.

Patrick Bellouard, Ancien Président d'Eurodéfense France

Conclusion

IGA Thierry Carlier

Je voudrais saisir l'opportunité de cette conclusion pour revenir sur les mots importants choisis pour nous réunir ce jour. « Le numérique, une arme de souveraineté de l'Etat » : rien n'est choisi au hasard. Dans une période où on a tendance à galvauder et amalgamer la signification des mots, il me semble très important de nous y attarder.

Numérique, tout d'abord. On pense immédiatement à ce sujet omniprésent et pourtant « invisible » du cyber, notamment la cyber sécurité, mais cette vision est réductrice. De façon plus générale, le numérique peut se représenter par la connectivité et constitue donc un outil de communication. Ainsi, le numérique est d'abord une opportunité mais également, par nature, une vulnérabilité.

On associe souvent au mot « numérique » trois termes sans trop de distinctions : résilience, sécurité et souveraineté.

La « **résilience numérique** » peut elle-même se décomposer en trois notions distinctes :

- La résilience **au** numérique, c'est-à-dire savoir conserver notre capacité d'action en dépit de l'indisponibilité de nos moyens numériques
- La résilience **par** le numérique, c'est-à-dire utiliser les outils numériques en tant que leviers d'action pour préserver notre liberté d'action
- La résilience **du** numérique, c'est-à-dire la résistance de nos outils numériques aux actions malveillantes.

La « **sécurité numérique** » quant à elle vise la protection et la sécurisation de nos services, de nos infrastructures et de nos données numériques. C'est un enjeu de taille pour le ministère des Armées mais qui concerne l'ensemble de la société. L'actualité nous rappelle malheureusement que cette menace est protéiforme (criminelle ou étatique) et n'épargne personne (emprises militaires, civiles, organisations publiques, privées, médias…).

Enfin, la « **souveraineté numérique** » est un volet particulier de la notion plus large de souveraineté. Chaque citoyen a pu ressentir durant la crise COVID l'impact de la perte de souveraineté (masques, vaccins), permettant ainsi de remettre sur le devant de la scène l'importance de la préservation de notre souveraineté de façon générale. La recherche de souveraineté dans le numérique relève de cette même notion, que l'on connait depuis longtemps dans le domaine de la défense et qui consiste à préserver et exercer notre liberté de choix et d'action sans être soumis à des contraintes ou des influences extérieures. Cette définition s'applique parfaitement au domaine du numérique.

La souveraineté numérique ne signifie pas de rechercher l'autarcie de nos moyens numériques, car chercher à maitriser l'ensemble de nos briques numériques n'est pas réaliste. En revanche, **être souverain, c'est disposer des expertises nécessaires pour être en mesure de faire nos propres choix**, et de déterminer par nous-mêmes où se situe, dans la chaine de valeur, le curseur de la souveraineté. Ainsi, certaines évidences se dégagent : à titre d'illustration, tout comme on ne renoncera jamais à la production souveraine de nos têtes nucléaires, il semble indispensable que nos chiffreurs numériques soient des briques souveraines. Mais pour le reste, nous avons de nombreuses zones grises. Ainsi, où se positionne le curseur de la souveraineté pour la protection de nos données et pour les services qui manipulent ces mêmes données ? C'est un débat essentiel et je suis heureux que ce colloque ait pu contribuer à l'éclairer avec efficacité.

Plus largement, les notions de souveraineté et de sécurité vont-elles nécessairement de pair ? Je pense que tous les experts de la salle seront d'accord avec moi : tout d'abord, si toutes mes données sont hébergées en local, sur le territoire français mais que mes infrastructures sont mal protégées, nous sommes peut-être souverains mais éminemment vulnérables. En parallèle, si nous bénéficions des meilleurs services de cybersécurité mais fournis par un prestataire de service étranger qui traite mes données dans le cloud, ma sécurité est assurée mais pas la maitrise souveraine de mes données. On comprend alors l'enjeu que nous avons à relever : **trouver l'équilibre entre souveraineté et sécurité. Dans ce domaine, n'ayons aucun dogmatisme.**

Il nous faut ainsi savoir placer le curseur au bon endroit entre préservation de nos données et performance de nos services. Il nous faut également accepter que ce curseur n'est pas unique et déterminé une fois pour toutes mais rester souples pour nous adapter aux différents enjeux comme le recours au cloud, les applications de l'IA pour la défense et l'apprivoisement des nouveaux usages tels que Chat GPT.

Cette recherche d'équilibre engage toute la communauté nationale du numérique, et plus particulièrement la communauté du numérique de défense regroupant la DGA, les forces et l'ensemble des industriels, quel que soit leur taille : les « grands » partenaires historiques bien entendu, mais également les nouveaux acteurs tels que les start-ups qui doivent être pleinement intégrées au sein de notre écosystème **comme nous parvenons progressivement à le faire dans le cas du New Space**. La présence des start-ups lors de ce colloque est à ce titre particulièrement importante.

Au cœur de cette communauté, la DGA a un rôle particulier à jouer : elle dispose d'une expertise assez unique au sein de l'Etat et doit assurer la mission importante mais pas toujours simple de faire la synthèse entre l'ensemble de ces enjeux. Ce sujet est au cœur des réflexions du projet de transformation de la DGA.

Enfin, **la notion de numérique comme « arme »,** dernier terme clé du titre de ce colloque, est également essentielle. Ce terme du registre martial nous renvoie paradoxalement à l'omniprésence de la menace sur nos capacités numériques, et pas seulement en temps de guerre. Dès la phase de « compétition » entre les nations, la conflictualité s'exprime dans le domaine numérique par des attaques incessantes. Ainsi, dans cette recherche d'équilibre entre sécurité et souveraineté qui appelle une nouvelle approche des enjeux du numérique au sein du ministère des Armées, notamment vis-à-vis des programmes (tant systèmes d'armes que systèmes numériques), la DGA prendra toute sa place, avec les autres acteurs du MinArm et avec la BITD. Tel est le rôle que la DGA a toujours joué dans tous les domaines de la défense pour répondre aux menaces qui pèsent sur la Nation. Il nous faut jouer ce rôle sur une matière moins palpable qu'à l'habitude, **mais dont le danger majeur serait qu'elle reste un impensé.**

Là encore, le colloque de ce jour est une magnifique opportunité de faire vivre et animer le débat, et surtout de faire progresser l'ensemble de la communauté de défense et sécurité de notre pays. Je tiens donc à adresser toutes mes remerciements et félicitations à la CAIA pour avoir organisé ce colloque et pour le dynamisme de l'ensemble des ingénieurs de l'armement qui œuvrent dans ce domaine essentiel du numérique au sein de l'administration, DGA et autres services de l'Etat concernés, et de l'industrie.

Annexe : Liste des Acronymes

Acronyme	Définition
ADN	Académie du numérique
ANSSI	Agence nationale de la sécurité des systèmes d'information
CAIA	Confédération Amicale des Ingénieurs de l'Armement
COMCYBER	Commandement de la Cyberdéfense
DGA	Direction générale de l'armement
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DIAC	Démonstrateur d'intelligence artificielle de confiance
DINUM	Direction interministérielle du numérique
DMA	Digital Markets Act
DRH-MD	Direction des Ressources Humaines du ministère de la Défense
DSA	Digital Services Act
GAFAM	Acronyme des géants du Web américains Google, Apple, Facebook, Amazon et Microsoft
IA	Intelligence artificielle
IA	Ingénieur de l'armement
L2I	Lutte informatique d'influence
LID	Lutte informatique défensive
LIO	Lutte informatique offensive
MINARM	Ministère des Armées
NIS 2	Network and Information systems Security, version 2
SAER	Système d'aide à l'exploitation du renseignement
SIC	Système d'informations et de commandement
SNIA	Stratégie nationale d'intelligence artificielle