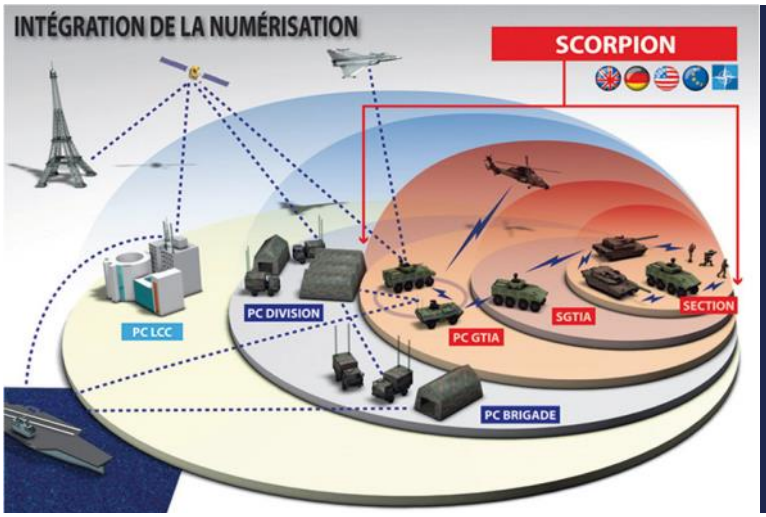
DEFENSE & industries

n°11 - Juin 2018

Fondation pour la recherche stratégique
www.frstrategie.org



Armée de Terre et innovation : des machines et des hommes (surtout)

L'armée de Terre, comme l'ensemble des organismes du ministère des Armées, répond aujourd'hui aux nombreux défis posés par les différents processus d'innovation touchant les institutions et au-delà l'ensemble même de la société civile (voir encadré central). Certes, l'intégration du progrès technologique n'est pas chose nouvelle. Mais à l'inverse du modèle du siècle précédent, caractérisé par une organisation étatique spécialisée dans la programmation militaire, adossée à des industries puissantes investissant massivement dans la R&D et produisant les équipements sur plusieurs décennies, les innovations contemporaines répondent à des stimuli essentiellement civils et sont produites par des acteurs plus nombreux et agiles sur une échelle de temps beaucoup plus courte. Les conséquences sociologiques et organisationnelles n'en sont que plus importantes pour les armées et surtout pour les forces terrestres, dont la dimension humaine reste cardinale.

> *« L'innovation est d'abord une question humaine avant d'être technologique. Si la technologie peut créer les conditions du changement, celui-ci est également déterminé par des facteurs humains et organisationnels.. ».*
>
> Général d'armée Jean-Pierre BOSSER, CEMAT

Le cap fixé pour l'innovation 2035 : supériorité opérationnelle et implication des personnels.

Le constat a été dressé dès 2016 dans *Action terrestre future*[1] d'une double nécessité d'adaptation aux opérations de combat des deux prochaines décennies : maintenir l'homme au cœur de l'action aéroterrestre ; tout en pilotant une approche capacitaire dynamique impliquant le combattant, le système d'arme, le système de forces.

La supériorité opérationnelle contre des adversaires disposant de capacités technologiques avancées et très adaptables est recherchée par la **numérisation totale de la force SCORPION** d'ici 2025-2030. Il s'agit de la colonne vertébrale capacitaire de l'armée de Terre capitalisant sur l'arrivée à maturité des technologies de l'ère numérique (capteurs embarqués et télédéportés, liaisons de données, algorithmes de simulation embarqués, etc.). Mais cette phase annonce déjà la prochaine étape de la **« cybernétisation » de la force au-delà de 2030**, fondée sur l'introduction progressive de la robotique et des algorithmes auto-apprenants dits d'intelligence artificielle, des nanotechnologies dans les domaines de l'énergie et des matériaux. On entre dans les spécifications de SCORPION 2, encore largement à développer.

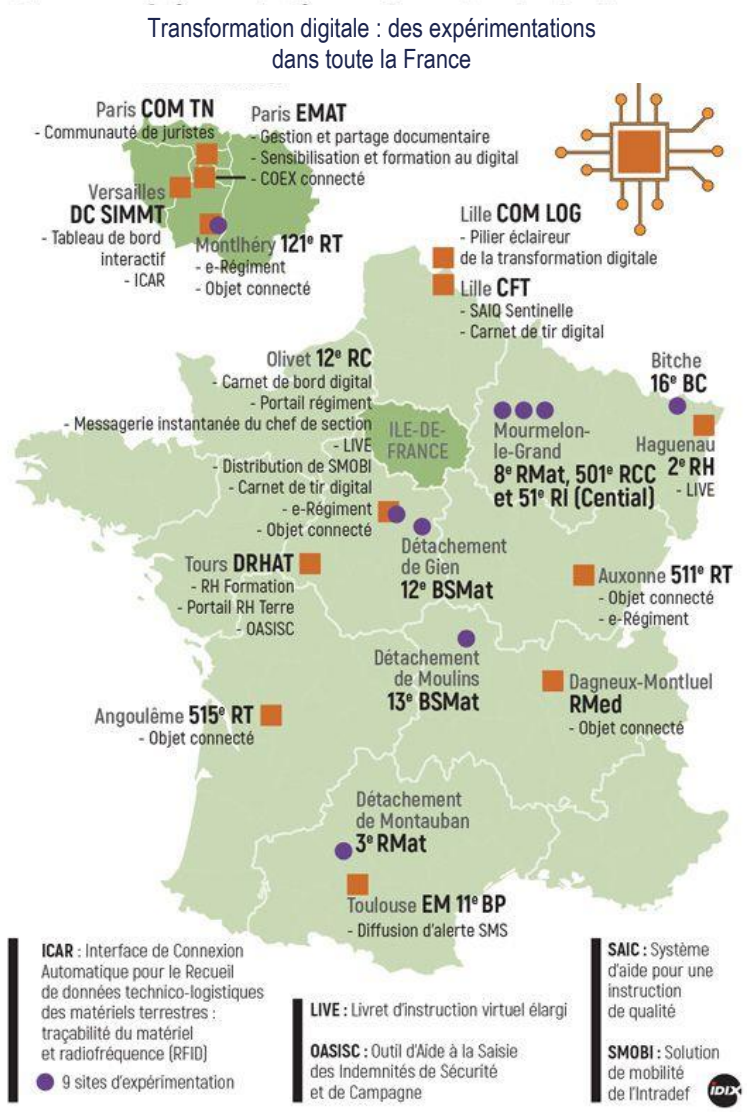
Parallèlement, les technologies numériques : Internet, téléphones portables, tablettes, *smartphones,* objets connectés ont progressivement entraîné un changement des mœurs et des comportements dans la société civile et vont continuer à le faire. Il faut donc, du point de vue institutionnel, capter l'intérêt des futures recrues en offrant au sein des forces terrestres un environnement auquel les engagés sont accoutumés, mais aussi en tirer profit dans l'organisation même des avantages procurés par ces technologies dans la gestion et l'optimisation des tâches de chacun.

Ce dernier point est important, car il relève de l'acceptation de ces changements par les opérateurs eux-mêmes. En effet, dans un environnement où l'adaptation est le maître-mot pour intégrer l'innovation, l'adhésion des personnels constitue la clé de la réussite des changements. Ceci implique de modifier les habitudes et les comportements dans un sens donné, d'agir en profondeur sur les cultures de métiers et les traditions institutionnalisées. Il existe pour cela toute une gamme d'outils expérimentés et disponibles techniquement dans le civil (méthodes *Nudge* et processus d'innovation frugale) qui sont introduits dans les forces.

C'est l'objectif du **plan de transformation digitale de l'armée de Terre**[2]. Il s'agit d'un processus d'enquêtes et d'expérimentations internes lancé en 2016 par le Général Bertrand HOUITTE DE LA CHESNAIS (GMAT à l'époque) avec deux objectifs : accroître la fluidité de la circulation de l'information afin d'augmenter la mobilité du soldat dans ses parcours de formation, d'entraînement et ses missions ; à terme contribuer à la supériorité opérationnelle en maîtrisant un nombre croissant de données de masses numériques générées dans les forces. Le programme a débuté par un tour de France des garnisons pour lancer des consultations parmi les personnels civils et militaires soucieux de proposer des idées novatrices pour améliorer les conditions et performances du service. Une grille de critères a été fixée pour sélectionner les projets expérimentables : un périmètre précis et délimité ; un budget réduit ; un objectif d'usage pratique courant.

Un premier bilan rendu public fin 2017 faisait état de 13 projets dont plusieurs en cours d'expérimentation en corps de troupes, à l'EMAT et certains grands commandements et directions centrales (voir la carte des chantiers en expérimentation ci-après).

Il existe donc plusieurs dimensions à gérer dans les mécanismes d'innovation, chacune avec ses caractéristiques propres[3] et l'homme est bien au cœur des processus de mutation.



Source : ministère des Armées

En termes capacitaires, l'innovation doit permettre d'explorer les voies possibles de ruptures opérationnelles.

Considérant les questions capacitaires à horizon 2035, l'armée de Terre s'apprête à faire face à une gamme probable d'adversaires, étatiques, irréguliers ou hybrides dont on cerne bien aujourd'hui les possibilités techniques[4]. Pour les adversaires étatiques agissant indirectement ou sous couverture et les organisations proto-étatiques fortement paramilitarisées, les capacités classiques à des niveaux de numérisation plus ou moins avancés sont retenues, combinées à un effet de masse, en raison des potentiels de puissance accumulés sur le pourtour du continent européen. La question se pose d'éviter l'engagement de ce type d'adversaire selon ses propres termes. La rupture opérationnelle est alors activement recherchée, l'innovation devant y contribuer sous toutes ses formes et pas seulement technologiques.

En attendant mieux et, en l'absence de toute définition officielle, on peut caractériser le champ d'une rupture par innovation opérationnelle de la manière suivante :

« Une innovation de rupture change les comportements de belligérants (étatiques ou non) dans la confrontation :

- *Par l'imposition d'une forme d'affrontement organisée inédite de niveau stratégique : levée en masse, dissuasion nucléaire dans le passé ; guerre cyber-mondiale aujourd'hui, nanomonde demain et / ou ;*
- *Par l'apparition d'une nouvelle dimension opérationnelle de niveau stratégique et opératif, pour laquelle il faut dédier des moyens auparavant inexistants ou inadaptés : spectre électromagnétique, espace extra-atmosphérique dans le passé, dimension souterraine urbaine dans le futur et / ou ;*
- *Par l'adoption de modes opératoires de niveau opératif ou de modes d'action de niveau tactique surclassant ou déclassant l'efficacité des modes opératoires et d'actions usuellement mis en œuvre et / ou ;*
- *Par un changement du rythme opérationnel en usage ».*

Obtenir une rupture implique de synchroniser en temps réel les cycles courts et longs de l'innovation opérationnelle.

L'innovation recouvre donc quatre cycles distincts liés aux opérations qui se complètent pour produire la rupture recherchée avec leurs propres caractéristiques et chaînes de responsabilité :

- Le **cycle long de l'innovation technologique** : « *recherche, insertion et développement de technologies chargées de réaliser des performances nouvelles ou de constituer des capacités supérieures à celles préexistantes* ». Il est parfaitement maîtrisé par les complexes industriels et militaires des Etats modernes depuis le début du siècle dernier. Il est efficace et produit des effets quand il est chargé de contrer un adversaire que l'on connaît bien ou une menace répertoriée. Il recouvre les activités d'études amont aux retrait / recyclage d'un système d'arme sur quatre à cinq décennies. En France, il s'agit de la trinité, Etat-majors, services techniques, DGA, à laquelle se joint de plus en plus le tissu industriel civil extérieur (sart-ups, PME) ;
- Le **cycle moyen de l'innovation conceptuelle et doctrinale** : *« le pourquoi et le « comment servir » d'une capacité naissante qui accompagne sa mise en œuvre, du déploiement initial à son retrait »*. Il concerne plus les Etats-majors que les industriels et devient d'autant plus important dans l'environnement incertain des deux prochaines décennies, que peuvent se dévoiler soudainement des ennemis ou menaces non pris en compte dans le premier cycle technologique. On est là essentiellement dans la réflexion humaine qui doit trouver des réponses pratiques pour faire face avec les équipements en dotation et ceux programmés à horizon de trois à

Le cadre du pilotage des innovations au sein du ministère des Armées : la feuille de route *ID - Innovation défense*.

- Présenté en mars dernier par Madame Florence PARLY, ministre des Armées, ID - *Innovation défense* concrétise les conclusions des travaux de la *Task force* innovation lancée à la suite de la *Revue stratégique* d'octobre 2017. Il s'agit de développer une approche intégrée au sein du ministère pour introduire les transformations permises par les innovations extérieures. Trois objectifs sont poursuivis pour les forces :
- Tirer profit des boucles courtes technologiques du monde civil au profit des capacités militaires :
- Porter à maturité rapide les nouvelles capacités par prototypage ;
- «Investiguer» les ruptures opérationnelles 2030.

Deux impératifs sont fixés aux grands organismes du ministère :

- S'ouvrir aux opérateurs privés, incluant la dimension européenne et faire travailler ensemble les institutions (états-majors, DGA), les chercheurs universitaires, les grands groupes et surtout les start-ups, PME, TPE, sources d'innovations et dont le soutien financier est indispensable :
- Disposer d'une approche globale du pilotage de l'innovation avec la création d'une direction générale du numérique et des systèmes d'information et de communication (DGNUM) ; d'une nouvelle agence de l'innovation de défense dotée de 100 millions d'Euros de budget ; le développement d'un *Innovation Defense Lab*, pour l'expérimentation et le prototypage rapide de projets à la suite de la première expérience du DGA lab. Ce dispositif a vocation à rationaliser l'ensemble des initiatives mises en place depuis plusieurs années (fond DEFInvest, MIP….).

dix ans. Pour la France, ce sont le CICDE en interarmées et le CDEC pour l'armée de Terre, avec le concours des Ecoles d'armes qui assurent cette gestion ;

- Le **cycle court de l'innovation d'urgence** : *« adaptation immédiate visant à parer une menace mal ou non évaluée et à reprendre une marge de supériorité »*. Il est prioritaire dans les engagements pour contrer les surprises et restaurer une supériorité contestée ou nullifiée et dépend d'une boucle de retour d'expérience rapide et efficace à l'initiative des forces déployées. La lutte anti-IED en offre un exemple illustratif. Ce sont les mêmes acteurs que précédemment auxquels s'ajoutent les services techniques d'armée. Son importance sera d'autant plus grande que les combinaisons possibles de technologies et de modes d'action varient vite dans une campagne face à un adversaire déterminé et inventif ;
- Enfin, le **cycle court de l'innovation d'opportunité** dite **participative** : *« possibilité inopinée de compléter l'un des trois autres cycles à partir de ressources technologiques ou de savoir-faire non initialement prévus à cet effet, disponibles dans ou en dehors des forces »*. Il est d'autant plus nécessaire que s'accroissent les opportunités offertes par la créativité du monde civil, accessibles au plus grand nombre. En France, ce cycle est géré au niveau ministériel par la Mission d'innovation participative, en attendant la mise en place des organismes prévus par la feuille de route *Innovation défense* du ministère[5].

La mutation de la numérisation en cours de la force terrestre en cybernétisation pourrait constituer le fil conducteur des ruptures opérationnelles futures, à condition de la contrôler.

La recherche permanente et la préparation de la rupture opérationnelle pour les deux décennies à venir passent par deux axes d'efforts :

- Avec l'aboutissement de SCORPION 1, conserver la supériorité obtenue par la numérisation totale de la force face à des adversaires qui sont dans une logique d'acquisition progressive des mêmes capacités et continuent à utiliser transitoirement des formes classiques de combat héritées de l'âge industriel ;
- Avec SCORPION 2, rechercher les conditions de rupture par la « cybernétisation » de la force contre des adversaires disposant de capacités modernes numérisées (ISR tactique et / ou opératif couplé à des capacités de frappe de précision dans la profondeur). Cela passera certainement par une « remassification » partielle des forces avec des personnels binomés à des systèmes non-humains, pour les missions ISR, soutien et de combat les plus exposées ; les ressources humaines et financières ne permettant plus de forces à « gros bataillons » dans nos sociétés contemporaines, du moins à horizon prévisible.

A cet égard, et avec toutes les réserves d'usage, on peut considérer une force terrestre numérisée comme un ensemble de capacités animé par une intelligence humaine démultipliée par des architectures de systèmes communiquant en réseaux. Une force cybernétisée pourrait aboutir, à terme, à un ensemble capacitaire animé par une intelligence collective bio-synthétique (coalescence de niveaux d'intelligence non organique et humaine). Ce glissement possible en raison des combinaisons technologiques en cours de développement ne se fera pas en ligne droite et reste à la main du commandement. Il dépendra des combinaisons technologiques évolutives, de la nature et des caractéristiques des adversaires, mais aussi et surtout des changements sociétaux (valeurs, choix éthiques, bouleversements sociaux) et des limites en ressources ; ensemble de facteurs dont on ne peut encore discerner clairement les directions.

On peut simplement deviner que les forces terrestres françaises n'évolueront que très progressivement entre l'une et l'autre sans savoir encore jusqu'à quel point.

C'est donc un long cheminement d'exploration, d'expérimentation, de validation, mais aussi d'acceptation de risque qu'emprunte l'armée de Terre sur au moins trois domaines tendanciels :

- L'impact de la distanciation progressive du combattant de la zone létale comme le permettent déjà les systèmes téléopérés et qui va se confirmer avec le déploiement de systèmes semi-autonomes ;
- L'hyperspécialisation du combattant à capacité humaine renforcée dépendant du nombre et des caractéristiques des équipements déployés ;
- L'agrégation même de cette intelligence bio-synthétique collective dépendant des évolutions des formes de l'intelligence artificielle et des degrés de supervision laissés à l'humain à tous les niveaux stratégique, opératif et tactique et bien entendu, interarmées.

Les chantiers de l'innovation doivent faciliter ce cheminement en retenant ce qui paraît utile du monde extérieur, mais en écartant aussi ce qui ne l'est pas.

« L'adaptabilité » devient un *« enabler »* des facteurs de supériorité opérationnelle maximisant les opportunités de réalisation de ruptures.

L'armée de Terre s'est déjà mise au diapason de ces transformations en précisant comment gagner l'ascendant sur un ennemi par la combinaison de huit facteurs de supériorité opérationnelle (FSO) faisant le lien entre les principes de la guerre et les aptitudes[6] de combat : compréhension, coopération, agilité, masse, endurance, force morale, influence et performance du commandement[7]. Mais c'est dans la manière dont les FSO sont connectés et se soutiennent mutuellement que réside leur pleine efficacité. C'est là qu'intervient une bonne gestion des différentes dimensions de l'innovation précédemment décrites[8]. Laquelle doit encore être caractérisée. L'adaptabilité pourrait être définie comme : *« la fonction de pilotage intégrée de l'ensemble des cycles d'innovation de la Force terrestre. Elle vise à :*

- *Créer et entretenir la synergie entre le cycle d'innovation technologique long et les cycles d'innovation conceptuelle et doctrinale, d'urgence et d'opportunité plus courts ;*
- *Déceler les potentielles innovations de rupture au profit des opérations de la force terrestre, ou dirigées contre elle ;*
- *Favoriser un environnement d'appropriation de l'innovation »*.

L'adaptabilité capitalise sur les enseignements et les bonnes pratiques du monde civil pour mener à bien les projets innovants, que l'Institution militaire s'approprie en tant que de besoin. Sa logique consiste à décloisonner, faciliter le dialogue et offrir un cadre à l'initiative. Un peu comme l'a déjà fait le plan digital de l'armée de Terre en :

- Favorisant une approche collaborative par communauté de métiers, de spécialités ;
- Facilitant les expérimentations de type micro-projet;
- Stimulant la pratique généralisée de la simulation et de la manipulation comme vecteur pour l'appropriation d'une innovation sur laquelle on mise, mais dont on doit convaincre le plus grand nombre de l'utilité.

En conclusion, il n'appartient pas au rédacteur de prendre parti sur la manière dont l'armée de Terre devrait cristalliser l'adaptabilité. Faut-il en faire une fonction opérationnelle à part entière ? L'inclure comme socle des FSO existants ? Créer une entité physique d'aide au pilotage auprès du commandement comme a pu l'être en son temps et à son niveau le *Centre de prospective et d'évaluation* pour les affaires nucléaires au sein du ministère des Armées ? Cela dépendra des arbitrages internes à l'Institution.

Mais on l'aura bien compris dans ce pari organisationnel et culturel tout autant que technologique, la maxime de Jean BODIN se trouve une nouvelle fois confirmée : *« Il n'est de richesse que d'hommes »*.

JEAN-JACQUES PATRY
Chargé de mission, FRS
Directeur du Master 2 géopolitique et sécurité internationale à l'ICP
jjpatry@gmail.com

Notes

1.*Action terrestres futures : demain se gagne aujourd'hui*, EMAT, Paris, septembre 2016, 65 p, pp. 9-10.

2.*La transformation digitale de l'armée de Terre*, dossier TIM, n° 289, octobre 2017.

3.Voir l'article d'Olivier SCHMITT, « Innover dans les armées : les enjeux du changement militaire », *Revue de défense nationale*, mai 2018, pp. 25-30.

4.*Revue stratégique de défense et de sécurité nationale*, Octobre 2017, Partie B, pp. 47-53.

5.« Florence Parly présente son plan en faveur de l'intelligence artificielle, axe d'innovation majeur du ministère des Armées », MinARM, 22 mars 2018.

6.Voir « Eléments de compréhension sur le document action terrestre future », *Argumenterre* n° 11, CDEC, Paris, 2016, 4 p.

7.*Action terrestre future…*, *Op. cit*., pp 22-23.

8.Lieutenant-colonel Thibaut KOSSAHL, EMAT/B.PLANS, « La technologie dans le système des facteurs de supériorité opérationnelle », *Évolutions technologiques et supériorité tactique*, Lettre de la doctrine n° 7, CDEC, Paris, mars 2017, pp. 9-12.

Bundeswehr et innovation : d'une réforme à l'autre ?

Les contraintes financières qui ont émergé suite à la Réunification et à l'évolution des missions de la Bundeswehr, notamment l'ouverture sur les opérations extérieures, ont conduit les pouvoirs publics allemands à conjuguer les logiques de préservation et de modernisation de l'outil de défense. Innovation rimait alors avec rationalisation. C'était tout le sens de la politique initiée sous le mandat de Rudolf Scharping (1998-2002)[1] et poursuivie les quinze années suivantes.

A la faveur d'un contexte budgétaire plus favorable et de la perception d'un environnement stratégique et opérationnel changé, le ministère fédéral de la Défense a entrepris de faire de la Bundeswehr un acteur de l'innovation. Ainsi que l'ont signifié la Chancelière fédérale, Angela Merkel, et la ministre de la Défense, Ursula von der Leyen, dans leurs déclarations au Bundestag le 21 mars 2018[2], ce chantier est appelé à se poursuivre au cours de la législature (2017-2021) qui vient de s'ouvrir. Il se déroule dans le cadre des réflexions sur le profil capacitaire de la Bundeswehr à horizon 2026/2030. Sur un plan plus général, il intervient toutefois plus d'une décennie après le lancement de la modernisation du « site de production Allemagne » (« Standort Deutschland ») sous le Chancelier Gerhard Schröder (1998-2005) et de la parution de la première stratégie high-tech pour l'Allemagne (2006), deux événements qui ont marqué la renaissance de la politique d'innovation fédérale dans un double souci de compétitivité et d'aménagement territorial.

Le discours officiel, qui insiste aujourd'hui principalement sur le défi de la transformation numérique, les équipements pilotés à distance ou autonomes et la révision des procédures d'acquisition, introduit une modification du rapport de la défense aux évolutions technologiques. La maîtrise de ces dernières n'est plus réduite à un élément de prestige et de démonstration d'un savoir-faire « Made in Germany » ; elle est désormais pleinement inscrite dans la stratégie de développement de la Bundeswehr. Mais que recouvre précisément l'innovation pour l'armée allemande d'aujourd'hui ? Quels en sont les objectifs, les instruments et les institutions[3] ? Enfin, quelles sont ses implications en termes d'action publique ? Ce sont donc les modalités du changement entourant le processus d'innovation que nous cherchons à éclairer dans cet article.

L'injonction à l'innovation

Relecture du champ de bataille

Le changement qui semble s'opérer dans le rapport du ministère fédéral de la Défense à l'innovation est encadré par une contrainte liée à une perception nouvelle du champ de bataille. Plusieurs textes guidant les travaux d'élaboration de la prochaine « Conception de la Bundeswehr » (document fixant le niveau d'ambition, d'où découlera le profil capacitaire) laissent entrevoir une telle évolution : *Strategische Vorausschau für die Bundeswehr- Eine langfristige Perspektive bis 2040* (2017, Division Plans du ministère), dont les grandes lignes ont filtré dans la presse nationale, et trois papiers de réflexion de l'état-major de l'armée de Terre (*Thesenpapiere* de la division Plans du Kommando Heer), rendus publics depuis l'automne dernier.

Dans la veine d'autres analyses menées dans la zone euro-atlantique et plus particulièrement aux Etats-Unis, les forces armées allemandes identifient les développements technologiques comme un facteur majeur de vulnérabilité. Elles se représentent un espace de combat où la transparence et la complexité sont appelées à gagner en importance : à la variété d'adversaires potentiels s'ajoutent l'acceptation croissante des nouvelles technologies et la progression de l'accès à celles-ci, l'essor des technologies de l'information et de la communication (TIC) qui renforcent, localement et mondialement, les liens entre les sociétés, ou encore les convergences des nanotechnologies, biotechnologies, technologies de l'information et sciences cognitives ouvrant la voie à des capacités humaines augmentées.

La représentation du champ de bataille du futur est également marquée par les menaces suivantes : la mise en œuvre de capacités plus ou moins sophistiquées de déni d'accès et d'interdiction de zone, l'arrivée de nouveaux vecteurs aériens sous la forme de drones opérant en essaim, des évolutions en matière de tir direct (ex. : développement des armes à énergie cinétique ou emploi accru de missiles anti-chars renforçant la frappe dans la profondeur), et indirect (ex. : charges thermobariques), la généralisation de la dimension cyber et l'accroissement de la dimension spatiale.

L'étude de l'engagement russe en Crimée ou dans l'Est de l'Ukraine renforce cette analyse. De surcroît, elle appelle à mieux prendre en compte les phénomènes d'accélération du temps et de fulgurance. Plus encore, ce travail révélerait le manque de préparation de la Bundeswehr qui ne pourrait plus remplir avec succès ses missions de défense territoriale et collective. Ce sentiment de retard est d'ailleurs conforté par l'acuité de la problématique de la disponibilité des matériels[4].

La maîtrise du rythme de l'innovation technologique, en particulier dans les domaines de la conduite, de la reconnaissance, de l'efficacité et du soutien (« Führung – Aufklärung – Wirkung – Unterstützung ») est, dès lors présentée comme inéluctable et urgente sur les plans stratégique et opérationnel. Elle apparaît comme un moyen de s'afficher en tant qu'allié solide et fiable, de dissuader et de regagner en supériorité opérationnelle[5] dans toutes les dimensions du combat.

Elle se fait ici aussi support de la disponibilité, de l'efficacité, de la robustesse, de l'agilité et de la résilience de la Bundeswehr. Dans ce contexte, la centralité du concept de guerre réseau -centrée (« Vernetzte Operationsführung » abrégé « NetOpFü ») dans la doctrine allemande[6] se trouve consolidée. Par ailleurs, est affirmé le rôle croissant des forces cyber, des systèmes pilotés à distance engagés en couplage avec des systèmes avec pilote (« manned-unmanned-teaming »), d'essaims de drones semi-autonomes ou encore des capacités spatiales.

L'innovation salvatrice ?

Cette relecture du champ de bataille peut être considérée comme un alignement sur les systèmes conceptuels américains, favorisé par la proximité avec les Etats-Unis que nombre d'officiers allemands revendiquent et recherchent. L'importance prise par les technologies et le besoin d'innovation est cependant aussi corrélée à des préoccupations spécifiques de la politique de défense allemande et à un mouvement de contestation interne à la Bundeswehr.

La séquence qui s'est ouverte depuis la parution du Livre blanc sur la politique de défense et l'avenir de la Bundeswehr (2016), et qui doit aboutir à la définition du nouveau profil capacitaire de la Bundeswehr, place au centre du processus les acteurs de la branche capacitaire (divisions Plans du ministère et des composantes d'armée, et l'office subordonné, le *Planungsamt*). Ceux-ci font coïncider ambition technologique et considérations financières. A titre d'exemple, les drones présenteraient « l'avantage de pouvoir être produits plus vite et à moindre coût que les traditionnels systèmes d'armes avec pilote [traduction] »[7]. L'argument est d'autant plus susceptible de porter que les ministères de la Défense et des Finances signalent des interprétations divergentes des termes de l'actuel contrat de coalition relatifs à la trajectoire financière de l'outil de défense[8] et qu'une collision entre les besoins financiers de la Bundeswehr, des systèmes de retraite et de santé n'est pas à exclure.

L'innovation technologique est également décrite comme une partie de la solution au problème des ressources humaines qui touche la Bundeswehr. Il est reconnu que les TIC et les technologies pilotées à distance exigent des personnels qualifiés et capables de s'adapter de manière constante aux mutations technologiques. La nécessité de conduire un débat sur les enjeux éthiques et juridiques n'en est pas moins rappelée. Toutefois, les personnels des branches capacitaires insistent sur l'opportunité qu'offrent l'autonomisation, la robotisation et l'intelligence artificielle pour contourner le besoin de massification des armées et le manque d'attractivité de la Bundeswehr.

Par ailleurs, la perspective d'une relance du processus d'innovation technologique a ouvert un espace de protestation contre l'organisation de l'acquisition d'armement. Cette dernière est régulièrement accusée, par les militaires et politiques (ministre, secrétaires d'Etat et parlementaires), d'être inefficace et inadaptée pour pouvoir faire face aux différents cycles d'innovation, mettant ainsi en péril l'efficacité opérationnelle de la Bundeswehr[9]. A cela s'est greffée une autre critique émanant du secteur civil, en particulier de celui des TIC. En février 2016, dans le cadre de la transformation numérique des armées, le Bitkom, organisation représentant les intérêts des entreprises des TIC, a formulé des recommandations qui pointaient, entre autres, un archaïsme du management de l'innovation et de la gestion de projets[10]. De cette convergence d'une multiplicité de sphères (militaires, politiques et marchés) a émergé une revendication pour initier une nouvelle réforme. Celle-ci viserait la mise en place d'une architecture organisationnelle elle-même innovante pour répondre mieux aux besoins militaires, consolider des technologies-clés et affirmer la souveraineté numérique de l'Allemagne.

Une mise en œuvre pour l'heure avant tout d'ordre organisationnel

Vers la formation d'une nouvelle communauté de l'innovation

Le sentiment grandissant de devoir changer et l'interaction entre différents champs socioprofessionnels ont abouti à la construction d'un nouveau cadre de pensée. Cette situation a contribué à un renouvellement des instruments et des institutions orientant le changement afin de favoriser la créativité ainsi que la diffusion et l'appropriation de l'innovation. Nous pouvons d'ores et déjà identifier un usage accru des méthodes de prospective pour compléter l'identification des innovations de rupture, jusqu'alors principalement déléguée à l'institut Fraunhofer INT[11], anticiper davantage et mieux guider le travail de planification capacitaire.

Mais il convient surtout de relever la création récente de nouvelles entités et l'apparition de profils extérieurs au secteur public dans les organigrammes, qui traduit le parti pris des décideurs politiques de ne placer qu'une confiance limitée dans les acteurs bureaucratiques traditionnels. La transformation numérique a amené, à partir de 2016, à la constitution d'une branche organisationnelle cyber[12] disposant d'un commandement spécifique (le *Kommando Cyber- und Informationsraum*, abrégé KdoCIR)[13] et d'une division dédiée au sein du ministère (*Abteilung Cyber- und Informationstechnik*). Elle est dotée d'un bureau consacré au pilotage de l'innovation dans son domaine. Klaus-Hardy Mülheck, qui a construit sa carrière dans le secteur industriel (ThyssenKrupp, groupe Volkswagen, Daimler ou encore Siemens), en est le directeur.

Pour ce qui concerne les universités de la Bundeswehr où est formée la majorité des futurs officiers allemands, l'institut sur la cyber-défense et le smart data (CODE) de l'établissement de Munich a été transformé en juin 2017 en « cyber-cluster ». Celui-ci se veut être une plateforme d'enseignement, de recherche et de coopération avec l'industrie et les start-ups. Parallèlement, le développement des sciences de l'innovation est notable : cette discipline à la jonction entre les sciences économiques et de l'ingénieur dispose d'un institut spécifique (*Institut für Technologie- und Innovationsmanagement*) à Munich, rattaché à la faculté des techniques aéronautiques et spatiales. Elle est également dispensée à Hambourg dans les enseignements de sciences de gestion.

Une autre structure plus atypique, encore expérimentale et principalement tournée vers les opportunités d'innovation émergeant hors des circuits traditionnels de défense, a vu le jour en janvier 2017 : le *Cyber Innovation Hub* (CIH)[14]. Conçu pour servir de tête de pont entre l'économie numérique internationale, notamment les start-ups et scale-ups, et la Bundeswehr, il bénéficie sur quatre ans (2 de phase pilote, 2 de stabilisation) d'un budget de fonctionnement de 12,6 millions d'euros et d'une enveloppe de 15 millions pour le soutien à l'innovation. Il est dirigé par Marcel Yon, au passé de banquier et d'entrepreneur dans les branches des technologies vertes et de l'information ; le directeur -adjoint, Jan Andresen, et le responsable réseau et marketing, Florian Busch-Janser, ont également évolué

jusqu'alors dans la sphère de la création d'entreprises.

La pérennité du CIH reste certes incertaine au regard, notamment, du départ de Katrin Suder[15], dont la force d'impulsion pour réformer le ministère a été déterminante, et du projet d'agence pour les innovations disruptives en cybersécurité et les technologies-clés[16], qui serait placée sous la tutelle des ministères fédéraux de la Défense et de l'Intérieur. Il n'en demeure pas moins que l'institution, en périphérie de la chaîne de commandement traditionnelle, a le potentiel pour jouer le rôle du « marginal-sécant »[17]. Autant promoteur du changement que point de cristallisation d'un mode d'action alternatif de l'appareil de défense, il est en position de défendre et illustrer la praticabilité d'une gouvernance simplifiée, plus rapide et ouverte sur l'extérieur face à une réalité administrative jugée complexe, voire illisible, et dispendieuse par les acteurs économiques de petite et moyenne tailles. Ses principales ressources ne sont pas financières. Elles résident dans sa maîtrise de l'écosystème des start-ups, et dans son rapport hiérarchique direct avec la haute sphère ministérielle (i.e. bureau du secrétaire d'Etat fonctionnaire en charge de l'armement).

Pour autant, affirmer que cette myriade d'institutions forme système serait, pour l'heure, exagéré. Plusieurs interrogations subsistent. Acteurs nouveaux et plus anciens développent-ils une compréhension commune de l'innovation ? Jusqu'à quel point l'édifice est-il stable, faute d'outil de synthèse et de coordination de l'écosystème ? Au-delà des mots et des rêves de DARPA ou de Silicon Valley de défense à l'allemande ou à l'européenne, la part de l'investissement étatique dans l'innovation sera-t-elle suffisante pour financer les ambitions énoncées ? Sur ce dernier point, le bras de fer engagé entre Ursula von der Leyen et le nouveau vice-Chancelier et ministre fédéral des Finances, Olaf Scholz, sur la planification budgétaire 2019-2022[18] pourrait enjoindre à la circonspection.

Innovation et système d'acquisition

Par ailleurs, comme évoqué précédemment, un lien entre innovation et politiques d'acquisition d'armement a été établi. En conséquence, la révision du système d'acquisition a été placée à l'agenda des décideurs. Une telle entreprise ne constitue pas une nouveauté. Dans le cadre de précédentes restructurations de la Bundeswehr, le sujet avait déjà surgi. Les commissions Weizsäcker (2000) et Weise (2010) avaient alors appelé à la transformation de l'Office fédéral des techniques de l'armement et de l'approvisionnement (BWB) - entité qui a précédé l'*Office fédéral* des équipements, des technologies de l'information et du soutien en service de la Bundeswehr (BAAINBw) – en une agence d'armement et à la gestion de programme en équipes de projet intégrées (*Integrierte Projektteams* - IPT)[19]. Seule la seconde mesure, qui vise à combiner satisfaction des besoins militaires et efficacité économique (respect des coûts et des délais), a été, depuis lors, appliquée. La restructuration du BWB-BAAINBw demeure, quant à elle, non seulement une évidence pour de nombreux acteurs, mais aussi un serpent de mer : les tentatives de changement ont systématiquement été mises en échec par l'organisation interne et les parlementaires, qui redoutent une restriction de leur pouvoir de contrôle et donc leur influence[20].

Même s'ils demeurent, dans la communication officielle, à l'état d'ébauche, les desseins de l'actuel gouvernement ont été dévoilés une première fois par la ministre à la soirée de l'innovation qui s'est tenue en amont de la dernière Conférence de sécurité de Munich (*MSC 2018 Innovation Night*). A cette occasion, Mme von der Leyen a formulé le souhait que la Bundeswehr devienne un « good client »[21]. La formule, quoi que floue, fait écho aux critiques adressées par la Cour fédérale des comptes au ministère de la Défense : celui-ci est, entre autres choses, accusé de ne pas exprimer correctement son besoin[22].

Devant le Bundestag, la ministre est allée plus loin en plaidant pour la poursuite de la modernisation des affaires d'armement : « Cela signifie mettre en œuvre la pluriannualité des finances publiques, améliorer le droit des marchés publics et examiner l'organisation de l'acquisition au sein de l'Office *fédéral* des équipements, des technologies de l'information et du soutien en service de la Bundeswehr. L'Office a atteint ses limites. Il a besoin de plus de moyens financiers et de nouveaux instruments, plus flexibles. [*traduction*] »[23]. Se manifeste ainsi de manière sibylline la volonté de mettre en question les fondements de la directive européenne de 2009 sur les marchés publics de défense et de sécurité. De plus, on comprend que la réforme pourrait, en réalité, n'être que d'ordre institutionnel et se concentrer sur l'organe traditionnel d'acquisition de la Bundeswehr. Dans cette perspective, une task force dirigée par Armin Schmidt-Franke, l'un des deux vice-présidents du BAAINBw, et l'amiral Jean Martens, directeur-adjoint de la division Forces armées (Abteilung Führung Streitkräfte – FüSK) au ministère, a été mandatée. Ses premières recommandations devraient être connues à l'été.

Les prémices d'un ajustement de la gouvernance de la Défense ?

La mise en cohérence de la Défense avec d'autres secteurs d'action publique

En ouvrant la focale, il apparaît que ces transformations esquissées autour d'une plus grande prise en compte de la dimension innovation dans la stratégie de défense peuvent être rapprochées de celles qui traversent d'autres secteurs de l'action publique allemande depuis plusieurs décennies. Elles repoussent les frontières de la politique de défense fédérale. Le ministère de la Défense allemand fait, en effet, désormais converger, par mimétisme, ses lignes d'intervention et méthodes avec celles d'autres ministères, en particulier de l'Economie (BMWi) et de la Recherche (BMBF).

Il s'aligne sur leurs pratiques en soutenant les synergies d'acteurs et les démarches interdisciplinaires et collaboratives afin de créer des écosystèmes favorables à l'innovation, comme l'illustrent la création du CIH et d'un cyber-cluster. Si le premier exemple témoigne de l'aspiration à s'inscrire pleinement dans la stratégie high-tech de 2014 qui s'adressait à l'intégralité de la chaîne de l'innovation, le second s'inspire des *Excellenzcluster* qui visent à établir des institutions de recherche et de formation compétitives et à forte visibilité internationale.

La Bundeswehr manifeste également son intérêt pour des domaines identifiés d'avenir depuis les années 2000 par le gouvernement fédéral, actant une convergence des objectifs du militaire avec le civil. C'est, par exemple, le cas pour l'ingénierie des systèmes, le génie mécanique, les bio- et nanotechnologies, la mobilité ou les TIC qui figurent dans les stratégies high-tech formulées à partir de 2006.

Ce processus ne peut être décorrélé du travail d'identification des filières technologiques à préserver mené par le précédent gouvernement[24].

La Défense reconnaît par ce biais l'enchevêtrement des secteurs militaires et économiques, et inscrit, elle aussi, sa démarche dans une logique industrielle. A cet égard, il convient d'insister sur la relation étroite qu'entretiennent industrie et innovation en Allemagne. La seconde est considérée comme un facteur déterminant du développement de l'industrie manufacturière qui demeure une composante essentielle du modèle économique allemand. Elle est aujourd'hui un enjeu de la modernisation de la structure industrielle dans le cadre du projet *Industrie 4.0*.

Enfin, l'arrivée d'un acteur comme le CIH ou la mise en place en 2016 d'un concept pour consolider les entreprises du Mittelstand évoluant dans le domaine de la défense[25] mettent en lumière la conversion de la Défense à une valeur centrale de l'action publique allemande : le soutien à l'esprit entrepreneurial. Ceci permet de rééquilibrer conceptions techniciennes et économiques de l'innovation de défense. Pour comprendre la place de l'entrepreneur à la fois dans le processus d'innovation et dans la politique d'innovation en Allemagne, il importe de garder à l'esprit la marque que Joseph Schumpeter a imprimée dans l'enseignement allemand des sciences économiques[26] et qui a contribué à héroïser la figure entrepreneuriale auprès de la société. Cet effet se ressent sur la structure économique qui accorde, depuis la crise des années 1970 et plus encore après la Réunification, une large place aux entreprises de petite et moyenne taille, connues sous les appellations KMU ou encore Mittelstand[27] et perçues comme les sources de la puissance économique allemande. Ceci trouve aujourd'hui aussi son prolongement dans les politiques publiques en matière d'emploi, d'industrie et de recherche qui valorisent la création d'entreprises via différents mécanismes (ex. : loi Hartz II, *IKT -innovativ*, *EXIST*, *High-Tech Gründerfonds*) et soutiennent le développement d'entreprises innovantes et les capacités privées de R&D au travers d'initiatives dédiées rassemblées dans le *Zentrales Innovationsprogramm Mittelstand* ou de programmes de subvention à la recherche.

Des relations civils-militaires toujours problématiques

Ce rapprochement du secteur de la Défense avec ceux de l'Economie et de la Recherche augurerait-il d'une meilleure interface entre mondes civil et militaire ? Les différentes transformations organisationnelles, advenues ou envisagées, redistribuent, en effet, les cartes du pouvoir et de l'expertise administrative.

D'une part, le poids conféré à la numérisation dans chacune des armées et la décision de créer le domaine organisationnel cyber modifient les rapports existants et stabilisés depuis 2000 au sein de l'appareil militaire. L'importance de la base interarmées de soutien (*Streitkräftebasis – SKB*) qui gérait jusqu'alors le dossier en est relativisée. De nouveaux jeux de pouvoir entre les différentes armées pourraient également se révéler, avec le risque de complexifier encore davantage les processus décisionnels. Le CIR n'étant pas une composante d'armée à part entière, ses personnels devront gérer au quotidien une double loyauté bureaucratique : permettre l'essor de la dimension cyber tout en satisfaisant les intérêts et besoins de leur armée d'origine. Cette contrainte peut stimuler les dynamiques collaboratives, comme elle peut être instrumentalisée dans le cadre de luttes entre composantes d'armée pour l'obtention de crédits de modernisation et ainsi exacerber un climat de tension entre militaires.

D'autre part, le feu nourri des militaires, appuyés par les décideurs politiques, contre le BAAINBw, organe au statut civil, relance le débat sur la place faite aux militaires dans le processus décisionnel allemand[28]. La mise en cause de la compétence du BAAINBw, couplée à la nomination d'un militaire, le Général Benedikt Zimmer, au poste de secrétaire d'Etat, fonctionnaire en charge des questions d'armement (avril 2018), alimente la méfiance entre personnels civils et militaires. En fonction des résultats de la task force évoquée précédemment, elle pourrait entraîner une modification significative des arrangements acquis entre civils et militaires depuis la création de la Bundeswehr en 1955 via une revalorisation inédite de ces derniers dans le système d'acquisition.

Dans un même temps et, au-delà des enjeux strictement bureaucratiques, le processus d'innovation de la Bundeswehr repose partiellement sur un accroissement des échanges de connaissances entre institution militaire et monde civil. Bien que des organismes tels que le CIH visent à une meilleure interaction entre ceux-ci, des tensions entre les deux univers demeurent perceptibles. Celles-ci s'illustrent dans la persistance de la clause civile (« Zivilklausel ») introduite dans plusieurs universités allemandes depuis 1986 et qui proscrit de concourir à un quelconque effort de recherche militaire ou, plus récemment, dans l'interdiction faite aux militaires allemands de se rendre en uniforme à la conférence re:publica organisée à Berlin sur le numérique avec des financements publics[29]. Cette situation met la Bundeswehr en demeure de poursuivre le travail entamé lors de la rédaction du dernier Livre blanc afin de débattre de ses orientations avec l'ensemble du gouvernement fédéral et de la société allemande. A cet effet, il importera à l'Allemagne de tirer les conséquences de la discussion sur l'achat de drones[30], ainsi que le rappelait récemment Ulrike Franke[31].

Cet éclairage multidimensionnel de la problématique de l'innovation au sein de la Bundeswehr a mis en évidence la complexité du processus à l'œuvre. Berlin s'est engagé dans une voie qui lui impose de concilier des impératifs d'efficience, de rapidité et de souveraineté pour recouvrer le contrôle du rythme de l'innovation et assurer la supériorité opérationnelle des forces, tout en manifestant le souhait de casser des pratiques administratives stabilisées et de renouveler la gouvernance sectorielle. Les faits exposés ont ainsi montré l'ampleur des dimensions organisationnelles et institutionnelles du sujet. Ils invitent aujourd'hui à questionner les éventuels effets de dépendance au sentier et de résistance au changement. Il sera en outre particulièrement intéressant d'analyser le degré d'appropriation de la dynamique par la nouvelle équipe administrative (Benedikt Zimmer, General Zorn, nouveau *Generalinspekteur*, Amiral Stawitzki, nouveau directeur Armement, et Gabriele Korb, nouvelle présidente du BAAINBw) et de se pencher sur le processus d'acceptation de ces transformations par la société civile.

GAËLLE WINTER
Chercheure associée, FRS
g.winter@frstrategie.org

Référence complémentaire

Mölling Christian, « A German Perspective », *in* Quencez Martin (dir.), *The Future of Transatlantic Strategic Superiority. British, German and French Perspectives*, German Marshall Fund, avril 2018, pp. 13-19.

Notes

1.Cf.: Contrat-cadre « Innovation, Investition und Wirtschaftlichkeit in der Bundeswehr » du 15 décembre 1999.

2.Regierungserklärung von Bundeskanzlerin Dr. Angela Merkel vor dem Deutschen Bundestag am 21. März 2018 in Berlin.
Rede der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, bei der Aussprache zur Regierungserklärung zum Thema Verteidigung vor dem Deutschen Bundestag am 21. März 2018 in Berlin.

3.Muller Pierre, « Esquisse d'une théorie du changement dans l'action publique. Structures, acteurs et cadres cognitifs », *Revue française de science politique*, vol. 55, no. 1, 2005, pp. 155-187.

4.Bundesministerium der Verteidigung, « Bericht zur materiellen Einsatzbereitschaft der Hauptwaffensysteme der Bundeswehr 2017 », mis en ligne en février 2018.

5.Voir plus particulièrement la préface du Gal Frank Leidenberger dans Kommando Heer, « Thesenpapier III. Rüstung digitalisierter Landstreitkräfte », mars 2018, p. 5.

6.Déjà présent dans la « Conception de la Bundeswehr » de 2004. Cf. : Bundesministerium der Verteidigung, « Grundzüge der Konzeption der Bundeswehr », août 2004.

7.« Den Vorteil, dass sie im Vergleich zu herkömmlichen bemannten Waffensystemen schneller und günstiger hergestellt werden können », *in* Kommando Heer, « Thesenpapier. Wie kämpfen Landstreitkräfte künftig? », 2017, p. 11.

8.« Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD », 2018, p. 145.

9.Kommando Heer, « Thesenpapier III. Rüstung digitalisierter Landstreitkräfte », mars 2018, p. 5.
Deutscher Bundestag, « Stenographischer Bericht. 26. Sitzung », Plenarprotokolle 19/26, 19 avril 2018, p. 2363 et p. 2365.

10.Bundesverband Informationswissenschaft, Telekommunikation und Neue Medien e.V., « Positionspapier. AK Verteidigung: Neuorganisation des Cyber- und Informationsraums im BMVg und im nachgeordneten Bereich », 22 février 2016.

11.Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalysen, basé à Euskirchen.
A ce sujet : Grüne Matthias, « Technologiefrühaufklärung im Verteidigungsbereich », *in* Zweck Axel, Popp Reinhold, *Zukunftsforschung im Praxistest*, Wiesbaden, Springer, 2013, pp. 195-230.

12.La Bundeswehr est composée de trois composantes d'armées (Heer, Marine, Luftwaffe) et de trois domaines organisationnels (soutien, santé, cyber).

13.Pour une présentation exhaustive, se reporter à : Mittler Report, *Europäische Sicherheit & Technik*, *Sonderausgabe Cyber- und Informationsraum*, Bonn : Mittler Report, 2018, n°1/2018.

14.Werner Kathrin, « Warum die Bundeswehr junge Gründer umgarnt », *Süddeutsche Zeitung*, 16 mars 2018.

15.Secrétaire d'Etat fonctionnaire de 2014 à 2018.

16.Mentionnée sous l'acronyme ADIC (« Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien ») dans l'actuel contrat de coalition.

17.« un acteur qui est partie prenante dans plusieurs systèmes d'action en relation les uns avec les autres et qui peut, de ce fait, jouer le rôle indispensable d'intermédiaire et d'interprète entre des logiques d'action différentes, voire contradictoires. » : Crozier Michel, Friedberg Erhard, *L'Acteur et le système*, Paris, Le Seuil, 1981, p. 86.

18.Sprenger Sebastian, « German defense budget angers critics – including the defense minister », *DefenseNews*, mis en ligne le 2 mai 2018.

19.Kommission „Gemeinsame Sicherheit und Zukunft der Bundeswehr", *Bericht der Kommission an die Bundesregierung*, mai 2000, p. 111.
Strukturkommission der Bundeswehr, *Vom Einsatz her denken. Konzentration, Flexibilität, Effizienz*, octobre 2010, p. 73.

20.Nassauer Otfried, Linnenkamp Hilmar, « Rüstungsbeschaffung: Zeit für eine grundlegende Reform », Berliner Informationszentrum für Transatlantische Sicherheit (BITS), juin 2014, 9 p.

21.Munich Security Conference, *MSC 2018 Innovation Night*, vidéo du 15 février 2018 : https://www.securityconference.de/mediathek/munich-security-conference-2018/video/msc-2018-innovation-night/

22.Bundesrechnungshof, *Schlechtes Projektmanagement verzögert und verteuert Modernisierung von Fregatten gravierend*, 2017 Bemerkungen, Ergänzungsband Nr. 7, avril 2018.
Bundesrechnungshof, *Kapazitäten in Eurofighter-Simulatoren bestmöglich für fliegerische Ausbildung nutzen*, 2017 Bemerkungen, Ergänzungsband Nr. 8, avril 2018.

23.« Das bedeutet die Umsetzung der Überjährigkeit im Finanzwesen, die Verbesserung des Vergaberechts und die Untersuchung der Beschaffungsorganisation im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Dieses Bundesamt leistet hervorragende Arbeit, aber es ist an seiner Grenze angekommen. Es braucht mehr Ressourcen und neue, flexiblere Instrumente. » Rede der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, bei der Aussprache zur Regierungserklärung zum Thema Verteidigung vor dem Deutschen Bundestag am 21. März 2018 in Berlin.

24.« Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland » du 8 juillet 2015.

25.Bundesministerium der Verteidigung. *Konzept des Bundesministeriums der Verteidigung zur Stärkung des wehrtechnischen Mittelstands*, 20 avril 2016.

26.Hilger Susanne, « Innovation und Wachstum aus wirtschaftshistorischer Perspektive », *in* Mai Manfred (dir.), *Handbuch Innovationen*, Wiesbaden, Springer, 2014, pp. 38-46.

27.Ce terme est à double sens : il désigne les petites et moyennes entreprises, les entreprises familiales de taille plus importante et les champions cachés ; il renvoie aussi à une catégorie socioprofessionnelle intermédiaire. Cf. : Bleuel Petra, *Suffit-il de s'inspirer du « modèle allemand » pour augmenter la performance des PME françaises ? Une analyse comparative entre la France et l'Allemagne*, thèse de doctorat Economies et finances, Université Côte d'Azur, CNRS, I3S, France, 2017.

28.Hoeffler Catherine, « Les réformes des systèmes d'acquisition d'armement en France et en Allemagne : un retour paradoxal des militaires ? », *Revue internationale de politique comparée*, vol. 15, no. 1, 2008, pp. 133-150.

29.Schillat Florian, Thissen Swen, « Bundeswehr lehnt sich gegen re:publica auf: Guerilla-Aktion bei Netzkonferenz », *Stern*, 2 mai 2018.
Lubberding Frank, « Heuchelei und ‚Angriffskrieg' », *Frankfurter Allgemeine Zeitung*, mis en ligne le 4 mai 2018.

30.Faute de consensus sur l'armement des drones, les partenaires de la coalition viennent de s'accorder sur l'acquisition de drones armables, mais non armés. Thiels Christian., « Kampfdrohne ohne Waffen – vorerst », ARD, 29 mai 2018. Accessible sur tagesschau.de.

31.Franke Ulrike, « Killer roboter ? Es geht auch anders. », *Zeit Online*, mis en ligne le 14 avril 2018.

DEFENSE INNOVATION UNIT EXPERIMENTAL

Capturer l'innovation de défense : à la découverte de DIUx

Quatre lettres, comme un nom mystérieux de programme de recherche secret : DIUx. L'acronyme est formé des lettres de « *Defense Innovation Unit eXperimental* », et désigne un laboratoire d'innovation créé par la défense américaine afin de capturer l'innovation du monde civil. Il s'agit d'une véritable innovation en soi, qui témoigne de la volonté du gouvernement américain de garantir sa souveraineté technologique, en pratiquant l'innovation ouverte, une initiative qu'il est intéressant d'analyser.

La menace du dépassement

C'est le général Robert Cone, ancien directeur du TRADOC (Training and Doctrine Center) américain, qui déclarait en 2013 « *ce qui me tient éveillé la nuit, c'est que l'on puisse rater la dernière innovation technologique – et que nos ennemis puissent l'obtenir* »[1]. Force est en effet de constater le pouvoir nivelant des technologies grand public. La mise à disposition de technologies de rupture à l'échelle mondiale via des groupes internationaux privés (on parle des GAFA – Google, Amazon, Facebook, Apple – américains ou des BATX– Baidu, Alibaba, Tencent, Xiaomi – chinois) entraîne une démocratisation de l'accès à l'innovation.

Le domaine le plus évident est celui du numérique : sans nécessiter d'outil industriel de production, ce secteur devient accessible au plus grand nombre. L'intelligence artificielle comme le « big data » sont en libre-service, et permettent à tout développeur de réaliser des programmes jusqu'alors réservés aux acteurs traditionnels de la défense. La reconnaissance d'images, la fouille massive de données ne sont dès lors plus réservées aux industriels de défense…

D'autres domaines, comme la fabrication traditionnelle, connaissent également une révolution, du fait de l'apparition de techniques comme le prototypage rapide, l'impression 3D ou fabrication additive. Enfin, les domaines les plus technologiquement avancés, jusqu'ici considérés comme régaliens et réservés, s'ouvrent aux innovateurs les plus audacieux. C'est par exemple le cas de la biotechnologie, avec le développement et la démocratisation de nouvelles technologies de « ciseaux à ADN », en l'occurrence l'endonucléase CRISPR-Cas9, un « couteau suisse génétique » permettant aux biohackers de manipuler les gènes à l'envi. Ce que les auteurs de science-fiction avaient imaginé, nous le vivons donc aujourd'hui, avec une course à l'armement et à la créativité qu'il est impératif de garder sous contrôle.

Si vis pacem, para bellum

Les Etats-Unis ont vite pris la mesure de cette compétition, et ont compris la nécessité de se doter de structures et de mécanismes permettant de ne pas être dépassés voire déclassés. C'est d'ailleurs ce qu'affirme la « *Third Offset Strategy* » - troisième stratégie de compensation, qui préconise une rupture stratégique et une affirmation de la supériorité américaine par l'acquisition de moyens technologiques pour lesquels les États-Unis disposent d'un avantage asymétrique. Cette stratégie comporte deux précédents : la première Offset Strategy américaine est intervenue dans les années 1950, avec la mise en service d'armes nucléaires tactiques. La deuxième, dans les années 1970, reposait sur le développement d'armes conventionnelles de précision. La troisième stratégie, en 2014, affirme la nécessité de développer les technologies d'intelligence artificielle, de robotique, de traitement des données ; autant de domaines aujourd'hui très largement développés par des entreprises privées.

Dès l'an 2000, un chercheur en physique théorique au MIT, Ashton Carter, écrivait un article intitulé « *Keeping the Technological Edge* » (conserver l'avance technologique) qui prédisait le dépassement de la recherche gouvernementale dans le monde de la défense, par le monde civil. Dans cet article prémonitoire, celui qui allait bientôt devenir secrétaire américain à la Défense avait compris l'impérieuse nécessité de constituer de nouvelles relations et des partenariats novateurs avec le secteur privé. Il ne l'oubliera pas.

Lorsque Ashton Carter prend ses fonctions en 2015, l'un de ses premiers déplacements est un voyage dans la Silicon Valley – à l'époque un événement pour un secrétaire d'état américain à la défense, puisqu'aucun de ses prédécesseurs n'avait daigné visiter ce haut lieu de la technologie américaine depuis plus de vingt ans. Dans la foulée, il annonce lors d'un discours fondateur à l'université de Stanford la création d'une nouvelle entité au sein du Ministère de la Défense (DoD) américain qu'il baptise DIUx, et qu'il localise à Mountain View, au cœur de la Silicon Valley.

Ce fait est, en soi, une révolution, car une telle entité gouvernementale devrait traditionnellement être logée à Washington, au sein du pouvoir et de l'écosystème de défense américain. Le choix de placer une telle structure au cœur du berceau des startups et de la high-tech américaine n'est pas anecdotique : l'ambition est de capturer l'innovation au stade de la recherche et du développement, en amont. DIUx dépend d'ailleurs hiérarchiquement du sous-secrétaire à la recherche et à l'ingénierie du DoD[2] (auparavant, elle reportait directement au ministre).

Il convient de noter que DIUx n'est pas la seule passerelle entre le monde de l'innovation civile et la défense : en 1999, la CIA créait le fond d'investissement en capital-risque In-Q-Tel, chargé de financer les start-ups les plus aptes à développer des technologies utiles à la communauté du renseignement. Parmi ses investissements les plus emblématiques, on trouve Palantir ou Google Earth (initialement baptisée Keyhole EarthViewer).

Mais le mode d'action de DIUx est, quant à lui, radicalement différent d'un capital-risqueur traditionnel.

Investissement non dilutif

Il ne s'agit pas en effet de prendre des participations dans des sociétés. DIUx a été dotée dès sa création en 2015 d'un budget lui permettant de financer des projets pilotes, de manière à fournir du capital non dilutif[3] (à la différence de prises de participation traditionnelles). Le processus est le suivant : DIUx identifie en collaboration avec les différentes entités du ministère de la Défense les sujets d'intérêt et lance un appel à participations. En l'espèce, il s'agit, pour la startup, de fournir une description de sa solution (quel que soit son niveau de maturité), et, pour DIUx, de juger de l'adéquation de cette dernière aux besoins opérationnels. En cas d'intérêt, DIUx demande à la startup de lui fournir une proposition commerciale lui permettant de réaliser, avec l'entité concernée, un projet pilote. Notons toutefois que DIUx s'intéresse à l'innovation, mais non uniquement aux startups. L'agence peut en effet décider au cas par cas de travailler avec des PME, voire des grands groupes, à condition que l'innovation commerciale corresponde à un besoin opérationnel avéré.
L'idée est de partager les coûts : la société candidate a déjà investi dans sa R&D, celle-ci n'est donc plus à la charge de l'Etat. DIUx finance un projet pilote, mais si celui s'avère positif, les coûts d'acquisition ne sont pas à sa charge, mais à celle de l'entité du ministère de la Défense qui souhaite déployer la technologie (pour un dollar dépensé par DIUx, l'entité concernée débourse, en moyenne, trois dollars).

Afin de financer ces projets pilotes, DIUx dispose, en 2018, d'un budget de 29,6 millions de dollars, montant auquel il convient d'ajouter des financements privés (notamment par des firmes d'investissement en capital-risque).

Cependant, le développement de cette agence n'a pas été un long fleuve tranquille, en particulier en raison des différences culturelles entre les différents acteurs impliqués.

Concilier deux communautés

Le monde de la défense et le monde des startups, jusqu'à ce jour, partagent peu de caractéristiques, à commencer par la longueur et la complexité des procédures. Une startup, comme toute communauté technologique émergente, travaille sur le temps court, contrainte par sa trésorerie, ses investisseurs, son paysage concurrentiel – ce qui peut d'ailleurs l'amener assez rapidement à « pivoter », c'est-à-dire changer radicalement d'orientation stratégique. Elle n'a donc pas les moyens de s'insérer dans les processus classiques d'acquisition.

De plus, les startups acceptent de prendre des risques, de procéder à des tests afin de raffiner leur modèle, et de se tromper, à condition de le faire rapidement (« *fail fast* ») pour pouvoir rebondir. Une culture évidemment très différente des structures étatiques ou privées traditionnelles, qui ont une aversion à la fois à la prise de risque (potentiellement néfaste à la création de valeur pour l'actionnaire) et à l'ouverture vers l'extérieur (syndrome bien connu du « *not invented here* »).

Très tôt, dès les premiers dossiers examinés, cette différence de culture est apparue comme un frein au développement concret de DIUx. Ainsi, en Silicon Valley, toute réunion s'achève soit sur une décision (positive ou négative), soit sur un contrat, alors que dans la culture du ministère de la défense, une réunion débouche généralement…sur une autre réunion. Cela peut paraître anecdotique, néanmoins il s'agit là d'une différence culturelle majeure ; les cycles de développement technologiques de la Silicon Valley sont tout simplement incompatibles avec le mode de pensée traditionnel du Pentagone.

DIUx 2.0

Pour y remédier, DIUx a, à son tour, « pivoté ». L'entité est devenue en 2016 – selon l'expression d'Ashton Carter, « DIUx 2.0 ». Elle a surtout modifié son mode de fonctionnement, avec deux innovations majeures. En premier lieu, un engagement à pouvoir démarrer un projet en moins de 60 jours afin de rester compatible avec le mode de fonctionnement de la Silicon Valley. Ensuite, une restructuration de DIUx (qui compte aujourd'hui une cinquantaine de collaborateurs) en trois équipes : l'une (Engagement team) jouant le rôle d'intermédiaire entre les startups civiles, les entrepreneurs et les opérationnels, la seconde (Foundry team) réfléchissant à l'adaptation nécessaire des technologies aux problématiques militaires, et la dernière (Venture team) jouant le rôle de veilleur, afin d'identifier les technologies possédant des applications militaires.

DIUx aujourd'hui, et demain

En avril 2018, DIUx a annoncé avoir financé 67 contrats depuis sa création, essentiellement vis-à-vis de sociétés qui n'étaient pas en relation avec le monde de la défense. DIUx a défini cinq domaines d'intérêt prioritaires : les technologies de l'information (en particulier tout ce qui est applicable aux systèmes d'information opérationnels), l'espace (services à la demande pour l'accès à l'espace, satellites, transfert de données large bande), l'intelligence artificielle, la robotique et systèmes autonomes (avec en particulier les technologies de collaboration homme-machine) et l'humain, qui regroupe des thématiques comme les biotechnologies, l'homme augmenté ou le biomédical. Parmi les projets pilotes les plus emblématiques, on peut citer Shield AI, une technologie permettant à un nano ou microdrone de réaliser en intérieur une cartographie en temps réel, ou Halo, une société qui fournit des bandeaux permettant une stimulation transcrânienne du cerveau afin de doper les performances physiques.

Afin de court-circuiter les processus traditionnels d'acquisition, une innovation majeure a été de permettre à DIUx de passer des contrats en utilisant un mécanisme nommé « *Other Transaction Agreements Commercial Solutions Openings* », qui permet à l'agence de respecter son engagement à financer un projet pilote en moins de 60 jours. Ce mécanisme permet également de négocier des conditions particulières en termes de jalons de paiement et de propriété intellectuelle (deux sujets particulièrement prégnants pour une startup).

Des interrogations subsistaient sur le maintien de DIUx, créée sous la présidence de Barack Obama, dans la nouvelle administration Trump (et en particulier sur la volonté du Congrès américain de poursuivre son financement). C'est en réalité l'inverse qui se produit : pour 2019, l'administration américaine a demandé une augmentation de 41 millions de dollars supplémentaires (par rapport à 2018) pour DIUx, ce qui devrait amener son budget annuel à 71 millions de dollars – de quoi financer de nombreux projets.

Une source d'inspiration ?

On le voit par cet exemple emblématique, si l'innovation de défense est à la mode, ce n'est pas une mode. Capturer l'innovation dans le civil, la transférer au monde de la défense

nécessite de penser de nouvelles structures, des modes de fonctionnement novateurs. C'est une véritable transformation en profondeur.

Cette tendance, on pourrait l'appeler, selon les mots de Michael Docherty[4], la « disruption collective » : le ministère de la défense jouant le rôle d'incitateur à la performance, les PME et startups étant les innovateurs, et l'agence agissant en qualité d'intermédiaire entre communautés.

L'exemple de DIUx permet de souligner les changements de mode de pensée nécessaires au succès d'une telle politique : accélération des rythmes, acceptation du risque, de l'échec et de l'erreur, agilité et capacité à s'adapter rapidement. Il convient également de penser les mécanismes contractuels permettant l'achat rapide d'une innovation au profit des opérationnels.

En France, la création de l'Agence de l'Innovation de Défense est un signal fort, une volonté politique de maintenir une souveraineté technologique nationale et européenne. A cet égard, l'exemple de DIUx peut constituer une source d'inspiration. Il démontre qu'avec des moyens somme toute raisonnables, et une organisation novatrice, il est possible de constituer une telle dynamique de disruption collective au sein de la communauté de défense.

EMMANUEL CHIVA
Directeur de la stratégie d'Agueris,
président de la commission RT&I
du GICAT

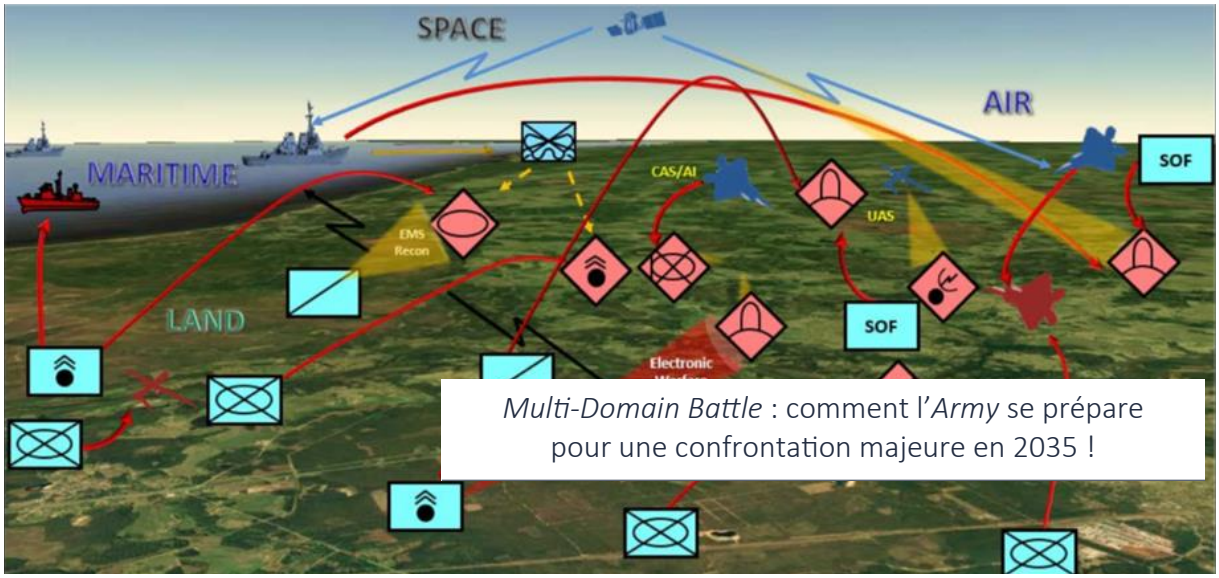
Notes

1.Morones Mike, « Interview with GEN Robert Cone », *DefenseNews*, 16 December 2013.

2.« Report to Congress Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization » - In Response to Section 901 of the National Defense Authorization Act for Fiscal Year 2017.

3.L'investissement non dilutif est défini comme n'entraînant pas de réduction du contrôle des actionnaires actuels, du bénéfice par action, ou de la rentabilité de l'entreprise – c'est donc un mode d'action particulièrement attractif pour une startup qui peut ainsi recevoir des subventions ou du financement sans dilution des fondateurs.

4.Docherty Michael, *Collective Disruption: How Corporations and Startups Can Co-Create Transformative New Businesses*, Boca Ratan, FL: Polarity Press, 2015.



Multi-Domain Battle : comment l'*Army* se prépare pour une confrontation majeure en 2035 !

[Version refondue et actualisée de l'article paru dans la Revue D&I n°10 de décembre 2017.]

Le 17 octobre 2017, *Multi-Domain Battle* (MDB), le concept commun à l'*US Army* et l'*US Marine Corps* a été rendu public, après deux années de préparation.

MDB se présente sous la forme d'un document devant guider la stratégie capacitaire des deux *services* pour les années 2025-2040[1]. La notion de multi-domaine est par ailleurs incluse dans la nouvelle version du manuel de doctrine de base de l'Army pour les opérations, le FM 3-0 *Operations*[2]. Du côté des *Marines*, le document prolonge *The Marine Corps Operating Concept . How an Expeditionary Force Operates in the 21st Century*[3] publié en 2016. Si les Marines sont créditées de l'élaboration de la notion de MDB, c'est sans conteste l'Army qui en assure le marketing le plus actif et a pris les mesures les plus radicales pour réorienter sa stratégie capacitaire.

MDB constitue **la réponse des forces terrestres aux défis générés par l'émergence militaire chinoise puis la réémergence russe** et auxquels l'instrument américain tente de trouver des réponses depuis une décennie. MDB entérine ainsi le **retour au primat du haut du spectre des opérations**. L'Army achève ainsi de tourner le dos à la guerre irrégulière et à la contre-insurrection, sa priorité absolue entre 2004 et l'orée de la décennie 2010.

MDB au croisement du contre-déni d'accès et de la compétition stratégique permanente

Comme la plupart des concepts américains, *Multi-Domain Battle* représente une évolution, non une transformation radicale.

La première racine généalogique de MDB est évidemment la réponse aux fameuses menaces de A2/AD (*Anti-Access, Area Denial*).

MDB se nourrit ainsi du concept interarmées publié en 2012, le *Joint Operational Access Concept*, construit autour de la notion de **« *Cross-Domain Synergy* »,** la nécessaire synergie entre les opérations dans les milieux terrestre, aérien, maritime, spatial et cyber. A cette époque, les Américains étaient surtout préoccupés par l'A2/AD chinois et le rééquilibrage en région Asie-Pacifique, un environnement accordant la primauté aux réponses aériennes et navales. A cet égard et à l'aune du défi posé de nouveau par les Russes depuis 2014, **MDB constitue l'aboutissement du rétablissement des forces terrestres dans le jeu institutionnel pour développer la stratégie de contre-déni d'accès**. Il s'inscrit dans le prolongement du *Joint Concept for Access and Maneuver in the Global Commons* (JAM-GC), réécriture interarmées du concept *Air-Sea Battle* qui devait initialement sceller une coopération limitée à l'Air Force et la Navy.

> Le développement de MDB découle directement de la « troisième stratégie de compensation » (Third Offset Strategy) destinée, sous la précédente administration, à accélérer la transformation des forces américaines pour faire face aux défis capacitaires russes et chinois. Son plus ardent promoteur, le *Deputy Secretary of Defense* Bob Work appelait ainsi en 2015 au développement d'une doctrine « Air Land Battle 2.0 » par analogie à la doctrine Army-Air Force qui structurait la seconde stratégie de compensation face aux soviétiques au début des années 80.

L'ensemble de ces documents admettent que les forces américaines ne disposeront plus d'une suprématie dans l'ensemble des milieux. Elles doivent donc désarticuler le dispositif A2/AD adverse en créant des brèches, en **opérant à partir de « fenêtres d'avantage » temporelles ou géographiques, dans un ou plusieurs milieux**. Compte tenu des systèmes adverses de défense anti-aérienne multicouches longue portée, de guerre électronique et de frappes de précision dans la profondeur, la séquence classique de l'acquisition initiale de la suprématie aérienne et navale préalable à la projection des forces terrestres ne serait plus opérante[4]. L'Army et l'USMC estiment donc, d'une part, devoir opérer sans soutien, d'autre part, pouvoir contribuer à ce contre-déni d'accès avec leurs propres moyens de projection des feux.

Pour le *Marine Corps*, qui rappelons-le est une force intégrée interarmées par destination, le problème se présente de la manière suivante : *« **The Marine Corps is currently not organized**, trained, and equipped to meet the demands of a future operating environment characterized by complex terrain, technology proliferation, information warfare, the need to shield and exploit signatures, and an increasingly non-permissive maritime domain »*[5]. En d'autres termes, la mission principale des *Marines* qui consiste à entrer en premier devient problématique, d'autant plus que la zone littorale d'engagement s'urbanise tendanciellement et très rapidement.

Résumons nous : pour l'*Army*, une fois entrée sur le théâtre, il faut survivre et prendre la lutte à bras le corps, y compris en intervenant dans les autres milieux aérien, maritime, spatial et cybernétique ; pour les *Marines*, il faut tout simplement pouvoir entrer !

La seconde racine généalogique, plus récente, réside dans l'émergence de la « compétition stratégique ». Les menées de Pékin en mer de Chine, l'interprétation de la stratégie menée par Moscou en Ukraine ont redonné comme on sait une forte impulsion aux notions de stratégies « hybrides », « ambigues », de « zones grises ». De fait, à partir de la *National Military Strategy* de 2016, les Américains estiment être engagés dans une compétition stratégique permanente avec les grandes puissances « révisionnistes ». Ces dernières usent du renseignement, de la guerre non-conventionnelle, de la guerre de l'information et des démonstrations de forces conventionnelles pour consolider leur diplomatie, interdire des espaces et s'organiser pour une éventuelle escalade. Une telle situation remet ainsi en cause la distinction classique binaire paix/guerre. MDB entend donc préparer les forces terrestres non seulement au conflit armé mais aussi aux activités relevant de cette période de compétition permanente.

Les auteurs de MDB construisent leur réponse sur une nouvelle **représentation de l'espace opérationnel (« *battlespace operatonal framework* »)**, dictée par l'adversaire et qui présente trois attributs :

- **« expanded » (étendu).** Cette extension se manifeste dans le temps avec des cycles de compétitions / conflits armés ; dans les milieux avec l'extension de la confrontation au cyber et à l'espace, dans la dimension géographique avec l'extension des zones de contact par les effets cyber de la guerre électronique et l'extension de la portée des armes ; dans le champ des acteurs avec un recours aux proxies. Par conséquent, toutes les forces, même celles qui ne sont pas présentes sur le théâtre des opérations sont menacées comme les forces au contact aussi bien par des munitions de précision à longue portée que par des tentatives de décrédibilisation par fausses nouvelles ou attaques systémiques cyber.
- **« Congerved » (convergent).** L'adversaire est en mesure de faire converger ses capacités sur les points faibles des Américains et de leurs partenaires.
- « **Compressed » (comprimé).** L'extension de l'espace opérationnel et la convergence des capacités aboutissent à une compression des niveaux classiques de la guerre, stratégique, opératif et tactique.

Cette configuration de la menace et de l'espace opérationnel amène l'Army et l'USMC à identifier cinq grands problèmes :

1. Comment dissuader l'escalade, défaire les menaces de déstabilisation et transformer les espaces déniés en espaces contestés en cas d'escalade ?

2. Comment manœuvrer de cette profondeur stratégique et opérationnelle contestée avec suffisamment de puissance de combat pour défaire l'ennemi ?

3. Comment conduire une manœuvre dans la profondeur terrestre, aérienne, navale pour supprimer et détruire les feux indirects, systèmes de défense antiaérienne et réserves ennemis ?

4. Comment les forces américaines permettent aux capacités terrestres de défaire l'ennemi dans la zone de contact ?

5. Comment consolider les gains, réaliser des effets soutenables, mettre en place les conditions de dissuasion de long terme et s'adapter au nouvel environnement de sécurité ?

La réponse de MDB s'articule en trois axes :

- **Une « posture calibrée »** combinant des forces de présence avancée, des forces expéditionnaires en mesure de se projeter en quelques jours et les forces des partenaires ;
- **Des « forces résilientes »** en mesure d'éviter la détection, de survivre au contact, d'opérer sans ravitaillement continu ni flancs sécurisés, de manœuvrer en environnement dégradé selon les principes du « *mission command* », du commandement par intention ;
- **Enfin, la « convergence » des capacités** permettant de mener des manœuvres « semi-indépendantes »,
  « *crossdomain* » dans la profondeur de l'espace opérationnel depuis n'importe quelle localisation.

La réarticulation de la stratégie capacitaire de l'Army

Pour réaliser MDB, l'Army a redefini les priorités de sa stratégie capacitaire, autour de **six grands domaines, les « Big six ».** Dans la programmation 2019-2023 qui accompagne la requête budgétaire 2019, elle entend réaligner sur ces priorités plus d'un milliard de $ (les crédits de R&D étant d'environ 10 Mds$ par an)[6]**.** Leur développement est confié à plusieurs ***« Cross-Functional Teams »*** [7].

> La modernisation de l'Army implique une rationalisation des procédures d'acquisition et d'innovation. C'est à quoi va s'employer le *Futures & Modernization Command* (FMC) installé à l'été 2018. En attendant, ces composantes sont déjà au travail sous la forme de huit Cross-Functional Teams (CFT) dans six domaines prioritaires : *Long Range Precision Fires, Next Generation Combat Vehicule, Future Vertical Lift, Networks* (deux CFT : une sur l'architecture informationnelle sécurisée et l'autre sur le remplacement de la technologie GPS), Air *and Missile Defense, Soldier* (soldat numérisé et augmenté). La dernière équipe approfondira les systèmes d'apprentissage et d'entrainement par simulation.
>
> Chaque CFT est confié à un général de brigade ou de division disposant d'une expérience récente de commandement. Sont rassemblés sous ses ordres des équipes du TRADOC, du matériel, du soutien, des spécialistes des armes, des techniciens extérieurs ou des universitaires. Leur mission consiste à qualifier précisément les futurs besoins opérationnels dans leur domaine de compétence, en accompagnement des programmes lourds, de proposer et d'expérimenter des solutions innovantes rapides.

***Cross-Domain Fires* : les feux de précision de longue portée et les moyens cyber-électroniques** afférant pour combiner des effets matériels et immatériels dans les domaines de lutte. L'objectif est tout d'abord de disposer dans les cinq ans de systèmes opérationnels doublant les portées des feux d'artillerie. Ainsi, le programme *Extended Range Cannon Artillery* (ERCA) prend en compte l'allongement des portées des tubes de 155 mm (extension de 40 km recherchée en sus des 24 / 30 km acquis). Il inclut l'obusier XM907, le projectile à propulsion additionnelle XM1113, un système de chargement automatisé XM654 « supercharge » et un tout nouveau système de contrôle de tir[8]. La *Guided Multiple Launch Rocket – Extended Range* permettra aux lance-roquettes multiples de passer de 70 à 150 km de portée. Enfin, les missiles ATACMS seront remplacés par des *Precision Strike Missile* de 500 km de portée *(Long-Range Precision Fires requirement)*. Illustration type du multi-domaines, une version anti-navire de

ces PRSM doit être développée à plus long terme pour dissuader et soutenir la *Navy* dans l'approche littorale[9].

Ces systèmes doivent pouvoir opérer dans l'environnement électromagnétique dégradé qui caractériserait toute confrontation avec les puissants moyens de guerre électronique russes et chinois (Voir ci-après).

Les effets recherchés sont également immatériels. A cet égard, la doctrine de l'Army a acté la convergence de la guerre cyber et de la guerre électronique. Ce sont les *Cyber-Electromagnetic Activities* (CEMA). L'intégration de ces deux fonctions et le développement de nouveaux moyens, comme les outils de *situational understanding* sont en cours de développement[10]. Surtout, l'Army entend remettre sur pied des capacités d'attaque électroniques négligées pendant une décennie (hormis la lutte anti-IED). Le système de *Multi-Function Electronic Warfare* incluant une capacité sur drone MALE et l'intégration de ces moyens au sein de compagnie renseignement / GE doivent être opérationnels pour 2023[11]. Enfin, il s'agit de démultiplier les capacités de ciblage nécessaires à l'emploi de ces moyens : réseaux de capteurs disséminés, liaison directe des niveaux tactiques avec les capteurs satellitaires, etc .

Next Generation Combat Vehicle **(NGCV)** constitue le second chantier. Il s'agit d'accélérer le développement des engins devant remplacer les chars M-1 et VBCI M2/3, une démarche un temps mise en sommeil après les deux fiascos que furent les programmes *Future Combat Systems* puis *Ground Combat Vehicle*. Le NGCV doit constituer la famille d'engins blindés pour la manœuvre semi-autonome ou autonome en environnement hautement agressif. Il doit être de petite dimension (engagement en zone urbaine), surprotégé par des dispositifs passifs et actifs, raisonnablement gourmand en carburant et surdoté en munitions à effets différenciés à longue portée. Pour l'heure, le concept mise sur un transport de troupe 2+6 équipé d'un 50mm. Mais il ne s'agit que d'un démonstrateur[12]. Bien entendu, l'ensemble est numérisé et conçu pour travailler en collaboratif avec des unités semi-robotisées. L'Army compte procéder en trois phases d'expérimentation : une série de test des premiers prototypes en 2020, une seconde en 2022, la troisième en 2023-24[13]. La R&D porte pour l'heure deux engins de combat : le NGCV proprement dit, un blindé habité, optionnellement télépiloté et un *Robotic Combat Vehicle* optionellement habité. Le général Milley, *Chief of Staff* de l'Army, a en effet expliqué que « *Every vehicle needs to have the capability to be robotic* »[14].

Future Vertical Lift **(FVL)** accompagne NGCV dans la troisième dimension. L'aérocombat figure en bonne place comme outil de renseignement, de force de frappe et de transport de troupes et de soutien pour les opérations « distribuées » dans la grande profondeur ennemie ; de même que pour l'évacuation sanitaire de combattants. Le premier projet du FVL, le *Joint Multi-Role-Technology Demonstrator* (JMR-TD), lancé en 2012, est de remplacer les 3.000 hélicoptères d'attaque AH-64 et UH-60 de manœuvre arrivant en fin de vie opérationnelle[15]. Pour l'heure, les hélicoptères lourds CH-47 ne sont pas concernés et, une fois modernisés, doivent rester en service jusqu'en 2060. Dans le cadre de MDB, l'*Army* a besoin de plate-formes durcies (blindage et systèmes redondants pour pilotage et navigation, autopilotées et téléopérées), capables de déplacements rapides, discrets, avec emport d'équipements lourds sur de grandes distances et en mesure de s'affranchir d'infrastructures sol devenues trop vulnérables. BOEING-SIKORSKY avec le projet SB-1 *Defiant* et BELL HELICOPTER et son convertible V-280 *Valor* sont positionnés sur JMR-TD. Le second projet est le *Next-Generation Tactical UAS*. Cette nouvelle génération de drones tactiques doit être multi-rôles (reconnaissance, attaque, guerre électronique, relais de communication, lutte contre les autres drones) et pouvoir, là encore, opérer en environnement dégradé[16].

Les réseaux et le C3I ont constitué pendant des années la priorité programmatique de l'Army. Cette dernière vient cependant de remettre à plat sa stratégie en matière de SIC[17]. L'architecture Internet de combat WIN-T, dont la version « *On The Move* » achève sa mise en service, donne satisfaction en opérations de contre-insurrection. Elle pourrait cependant se révéler vulnérable aux attaques électroniques et cybernétiques. L'Army mise ainsi sur le développement de la modularité des communications et des moyens de transmission à basse probabilité d'interception et de détection (*Low Probability of Interception and Detection*, LPI/LPD). S'y ajoute l'extrême vulnérabilité du GPS (déni d'accès spatial, brouillage ou corruption des signaux) qui constitue la base de la capacité de positionnement, de navigation et de timing de tous les systèmes, capteurs et effecteurs numérisés. De multiples axes de réponse doivent permettre l'« *Assured PNT* » : le renforcement du signal GPS avec le code M, le développement de sources de PNT terrestres (les « pseudolites »), la miniaturisation des horloges permettant la synchronisation des réseaux de communication et des radars[18].

Enfin le volet réseau/C3I inclut également la recherche difficile de l'interopérabilité des systèmes d'information, le renforcement des capacités de renseignement d'origine électromagnétique et le développement des capacités cyber. L'ensemble de ces transformations s'opère au moment où toutes les infrastructures informationnelles du *Department of Defense* et des armées passent en *Cloud* confiés à des opérateurs privés.

Air & Missile Defense redevient une préoccupation de survie pour des unités terrestres manœuvrants sous couverture aérienne temporaire et confrontées aux munitions de précision (missiles ou couples hélicoptères-missiles) et aux drones (manœuvres de saturation en essaim). L'architecture antimissile est interarmées, mais il faut la compléter par une densification des systèmes de défense de courte portée *(Maneuver Short-Range Air Defense – SHORAD)*. Afin de reconstituer sa défense antiaérienne, l'Army compte, entre autres, sur le *Low-cost Extended Range Air Defense* qui doit remplacer le Patriot, et pour la plus courte portée, le développement incrémental de l'*Indirect Fire Protection Capability* reposant sur une variante des missiles Sidewinder, puis potentiellement des lasers de combat de 100 KW vers 2023[19]. Toutefois, la grande affaire réside dans l'*Army's* ***Integrated Air and Missile Defense Battle Command System (IBCS)***. Il s'agit d'une architecture C2 spécialement destinée à la lutte antiaérienne et antimissile intégrée. Le programme, dont l'*Army* est l'intégrateur, en est encore en phase de tests pour les anti-missiles[20].

L'équipement du soldat (numérisé et augmenté) fait partie du dernier chantier. Concernant l'homme lui-même, deux capacités nouvelles sont explorées : les munitions à détonation programmable et autoguidées (combat urbain et en zones compartimentées) et les aides à l'effort (exo-squelettes). L'*Army* se concentre sur des expérimentations de niveau groupe et

section de combat pour acquérir de l'expérience sur la généralisation de binomes humains / machines. Il s'agit surtout de tester des mini-machines de reconnaissance, des fardiers téléopérés et d'introduire les premiers véhicules automatisés dans des convois logistiques[21]. Ceci constitue la première étape d'un plan de long terme exposé dans l'*US Army Robotics and Autonomous Systems*. Ce plan de robotisation a été présenté en mars 2017[22]. Pour les *Marines*, il n'existe pas de document officiel comparable (ils dépendent de la *Navy* pour les programmes), mais une initiative robotique multi-milieux avec expérimentations est en cours[23]. MDB va donc nécessairement évoluer, voir se transformer, au fur et à mesure de ces avancées.

Une première réorganisation structurelle : l'alourdissement des unités légères et la création de brigades MDB.

En attendant que ces chantiers produisent des résultats, il a été décidé d'augmenter la **protection et la mobilité des brigades d'infanterie légère *(Infantry Brigade Combat Team – IBCT)***. Celles-ci deviennent en effet trop lentes et trop vulnétrables. Notamment les brigades aéroportées et aéromobiles qui, une fois à terre, se déplacent à la vitesse du piéton[24]. Trois programmes sont donc lancés simultanément :

- Un transporteur léger de reconnaissance et de mobilité ; le ***Ground Mobility Vehicle*** **(GMV)**. Un 4X4 aérotransportable et aérolargable embarquant 9 hommes ;
- Un blindé léger de découverte et d'appui, aérotransportable ***(Light Reconnaissance Vehicle*** **– LRV)**, avec 6 hommes à bord et un 30 mm capable d'engager blindés légers et points d'appuis adverses ;
- Un blindé chenillé léger aérotransportable ***(Mobile Protected Firepower - MPF)***, d'appui contre les blindés lourds et les casemates. Il est doté d'une capacité de tir indirect pour les zones urbaines.

L'ensemble illustre la nouvelle « philosophie » de l'acquisition de l'*Army*. Ces plate-formes sont déjà disponibles chez les constructeurs et ne demandent que des modifications mineures pour répondre aux besoins des unités légères. Il est donc possible de les intégrer en phase C du processus d'acquisition (production-déploiement) en éliminant les phases A et B d'études amonts et de réalisation technique. Cette pratique de recours aux ressources extérieures tend à devenir une nouvelle norme, pour réduire les coûts et les délais d'acquisition.

Enfin, un nouveau type d'unité, la *Multi-Domain Task Force* (MDTF), est mis sur pied. Il s'agit d'une brigade de 1.500 personnels toutes armes, disposant de moyens de guerre électronique, cyber et d'appui spatial et de moyens d'aérocombat permettant de créer les fameuses « fenêtres d'avantage » contre les capacités A2/AD adverses. Le plan est de mettre sur pied 5 MNTF. La *17th Field Artillery Brigade* de l'*Army Pacific Command* (USARPAC) sert d'unité pilote jusqu'en 2020[25]. L'objectif est d'étudier toutes les contraintes et les possibilités tactiques d'une unité de petite taille capable de mener des opérations en semi-autonomie ou autonomie complète, lors d'attaque contre les systèmes AD/A2 adverses ou en mission de reconnaissance offensive dans la profondeur ennemie. Ces expérimentations prennent pour cadre le théâtre Asie-Pacifique, là ou l'*Army* est susceptible d'intervenir au profit de la *Navy* et des *Marines*, voire d'ouvrir des couloirs de pénétration à l'USAF.

Apports et défis de la Multi-Domain Battle

Il serait tentant chez l'observateur blasé de ne voir dans MDB qu'un nouvelle avatar de communication. De fait, MDB est un vecteur de réaffirmation de l'Army dans la compétition institutionnelle avec les autres services. De fait, il reformule et synthétise des éléments de concepts opérationnels développés depuis les années 90, comme par exemple la manœuvre opérationnelle depuis des distances stratégiques. Il n'en reste pas moins que MDB constitue un effort véritable de reconceptualisation guidant de façon cohérente la stratégie capacitaire de l'Army. Il s'agit du premier vrai concept visant l'adaptation d'un *service* à la compétition stratégique actuelle. MDB oblige donc la plus puissante force terrestre au monde à s'interroger :

- Sur la manière de conserver sa liberté de manœuvre dans un environnement hautement létal ;
- Sur la manière de piloter les processus d'innovation de plus en plus complexes ;
- Sur la manière de réexpliquer ce qu'est la nature de la puissance terrestre à des personnels militaires qui n'utilisent même plus ce terme et à des civils qui n'en ont qu'une vision parcellaire, déformée ou inexistante.

Le concept pose cependant de multiples questions et défis. Sur le plan stratégique tout d'abord, il s'ancre dans la vision américaine d'une hyper-rationalisation de la stratégie russe dont beaucoup de spécialistes pointent en fait les échecs, le caractère réactif ou opportuniste. MDB propose une vision cyclique « compétition / conflits armés » qui ne vaut que par le caractère régional limité du dit-conflit. A cet égard, on est frappé par l'absence de la dimension nucléaire dans la « période compétition ».

Ensuite, sur le plan institutionnel, MDB propose une véritable stratégie, non une « bataille ». Détail révélateur, le document cite 200 fois le terme « Joint » contre quelques dizaines de mentions des termes « Land » ou « Ground ». Le niveau pertinent de mise en œuvre de MDB est clairement interarmées / interagences. Un Rapprochement avec USAF est certes en cours mais MDB ne semble pas entièrement compatible avec le nouveau concept interarmes *Joint Concept for Integrating Campaigning* (JCIC).

Sur le plan capacitaire, MDB n'apporte pas de réponse à plusieurs grands défis déjà bien identifiés : la cohérence entre opérations « semi-indépendantes » selon le principe du *Mission Command* et convergence des effets nécessitant une excellente synchronisation ; les seuils techniques limitant la projection de forces lourdes significatives ; le développement de la flexibilité doctrinale et organisationnelle nécessaire pour réaliser des opérations multi-domaines.

Sur le plan financier enfin, la mise en œuvre de MDB suppose la pérennisation de cette nouvelle priorité accordée à la modernisation et surtout le maintien du haut niveau de crédits actuels, obtenus par le volontarisme des « *Defense Hawks* » du Congrès. Dans le contexte politique « tendu » que connaît Washington, la perspective des élections de mi-mandat, ce maintien n'est pas forcément garanti.

PHILIPPE GROS
Maître de recherche, FRS
p.gros@frstrategie.org

JEAN-JACQUES PATRY
Chargé de mission, FRS
Directeur du Master 2 géopolitique et sécurité internationale à l'ICP.
jjpatry@gmail.com

Notes

1.*Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040*, Draft Paper, Version 1.0, October 2017, 79 p.

2.FM 3.0, *Operations*, Headquarters Department of the Army, October 2017, 364 p.

3.*The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, Department of the Navy, Headquarters United States Marine Corps, September 2016, 27 p.

4.Conference delivered by the Deputy Secretary of Defense Bob Work, U.S. Army War College, Carlisle, PA, April 8, 2015.

5.*The Marine Corps Operating Concept*… Op.Cit, p. 8

6.Sydney J. FREEDBERG Jr., « Army Shifts $1B In S&T, Plans Modernization Command: UnderSec McCarthy », *Breaking Defense*, December 07, 2017.

7.General David PERKINS, « Multi-Domain Battle : The Advent of Twenty-First Century War », *Military Review*, November-December 2017, pp. 8-13.

8.Daniel WASSERBLY, « Picatinny Arsenal advances M777 extended range howitzer », Jane's Defence Weekly, 01 March 2017.

9.Sydney J. FREEDBERG Jr., « Army Will Field 100 Km Cannon, 500 Km Missiles : LRPF CFT », *Breaking Defense,* March 23, 2018.

10.Kashia SIMMONS, « Cyber Quest 2016: Exploring tactics, tools for CEMA situational understanding », TRADOC, August 5, 2016.

11.SYDNEY J. FREEDBERG JR., « Army Reorganizes, Accelerates EW: Synergy Or Hostile Takeover? », *Breaking Defense,* December 13, 2017.

12.Ben JUDSON, « Next-Gen Combat Vehicle prototyping kicks off», *Defense News*, October 10, 2016. et Ben JUDSON, « What is the Next-Gen Combat Vehicle? », *Defense News*, November 3, 2016.

13.Jen JUDSON, « First Next-Gen Combat Vehicle and robotic wingman prototypes to emerge in 2020 », *Defense News*, March 16 2018.

14.Matthew COX, « Army Chief Wants Robotic Vehicles, AI for Future Battles », *Military.com*, 17 Jan 2018.

15.Dr. Bill LEWIS, « Future Army Aviation Research », *Army Technology*, March/April 2015, Volume 3, Issue 2, pp. 6-7.

16.Layne B. MERRITT, *Army Aviation S&T Overview*, Presented to Huntsville Aerospace Marketing Association, June 2017.

17.Courtney MCBRIDE, « In new report, Army details network modernization plans », *Inside Defense*, February 02, 2018

18.Mark POMERLEAU, « What is the Army doing to assure GPS and navigation? » *C4ISRNet*, May 3, 2017, et voir Amanda ROMINIECKI, « PM PNT tests pseudolite characterization and performance », *APG News*,November 15, 2017.

19.Sydney J. FREEDBERG Jr., «Army Races To Rebuild Short-Range Air Defense: New Lasers, Vehicles, Units », *Breaking Defense*, February 21, 2017.

20.Françis MAHON, « Support IBCS, Best Missile Defense C2 We've Got: Former MDA Tester », *Breaking Defense*, June 12, 2017.

21.Sydney J. FREEDBERG Jr., « Armed Robots: US Lags Rhetoric, Russia », *Breaking Defense*, October 18, 2017.

22.*The US Army Robotic and Autonomous Systems Strategy*, TRADOC, March 2017, 26 p.

23.Sydney J. FREEDBERG Jr., « Semper Robotic: Marines Try Out New Tech, Tactics », *Breaking Defense*, October 20, 2016. Sydney J. FREEDBERG Jr., « Marines Seek To Outnumber Enemies With Robots », *Breaking Defense*, October 25, 2016.

24.Andrew FEICKERT, *Infantry Brigade Combat Team (IBCT) Mobility, Reconnaissance, and Firepower Programs*, CRS, September 26, 2017, 14 p.

25.J. Scott NORWOOD, SES Strategic Effects Director, U.S. Army Pacific, *The Future of Multi-Domain Battle*, présentation au workshop *Multi-Domain Battle in Megacities*, 21 March 2018. et voir Sydney J. FREEDBERG Jr. « New Army Unit To Test Tactics: Meet The Multi-Domain Task Force », *Breaking Defense*, March 21, 2017.

Base industrielle de cybersécurité : quels acteurs et enjeux pour la Défense ?

Face aux opportunités et vulnérabilités engendrées par la numérisation croissante de la Défense - et de l'économie plus généralement - les autorités publiques soulignent l'importance de disposer d'une souveraineté numérique. Ainsi, la Revue stratégique de cyberdéfense, publiée en février 2018, rappelle les objectifs suivants : « *La souveraineté numérique peut être entendue comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant part de la numérisation croissante de la société* »[1]. A cet égard, la revue souligne que cette souveraineté passe notamment par la maîtrise de la cybersécurité et le renforcement de « *la base industrielle française et la fondation d'une base industrielle de cybersécurité européenne* »[2].

Cet article se propose de définir les acteurs qui composent cette base industrielle de cybersécurité et ce, dans le contexte des besoins liés à la Défense.

Marché(s) de la cybersécurité : quelques segmentations

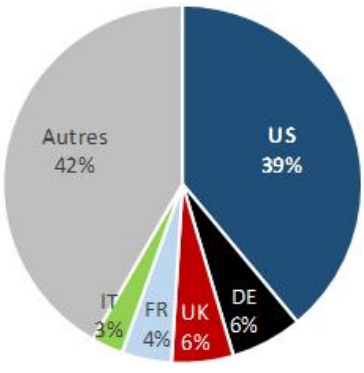
En l'absence de définition unanimement partagée et en raison d'un marché très évolutif, de nombreuses estimations du marché de la cybersécurité sont disponibles, variant considérablement en fonction du périmètre qui lui est appliqué. Par exemple, pour 2017, le cabinet Gartner évalue ce marché à 89 Mds$[3] quand il atteint les 138 Mds$ pour Markets&Markets[4].

La multitude des enjeux et des dynamiques liés au marché de la cybersécurité peut être mis avant à travers différentes segmentations. Une première est réalisée par type de solutions :

- grande famille : solutions matérielles, logicielles ou prestations de services de conseils de formation, de gestion de risques, d'audit, de test de pénétration, etc ;
- type de systèmes à sécuriser: infrastructures fixes, équipements de mobilités, bases de données, systèmes industriels, systèmes d'armes, etc. ;
- fonction de sécurité assurée : pare-feu, antivirus, chiffrement, authentification, etc. ;
- ou encore par niveau de sécurité recherché (de la technologie du paiement sans contact aux solutions de cryptographie Secret Défense).

La segmentation peut être aussi géographique : la demande en matière de cybersécurité est très hétérogène en fonction des zones et des pays. Le niveau de maturité d'un marché est étudié à l'aune de plusieurs critères, qu'ils soient liés à la situation économique, à son environnement géopolitique et cyber, la réponse à la menace cyber notamment. A titre d'exemple, selon les données communiquées par l'*European Cyber Security Organisation* (ESCO), les États-Unis représenteraient près de 40% du marché mondial en matière de cybersécurité. Les principaux marchés européens, pris individuellement, ne dépasseraient pas les 6%[5].

Marchés nationaux de la cybersécurité, en %



Source : ECSO

Une demande portée par les marchés civils

Au niveau national, une approche par type de clients « Défense » et « civils » semble nécessaire. Elle permet d'ajuster l'analyse aux enjeux propres de chaque client, que ce soit notamment en matière de :

- volume du marché ;
- maturité du marché ;
- besoins et contraintes spécifiques.

Toutefois, la distinction Défense/civil n'est pas figée et des caractéristiques communes peuvent apparaître.

La Défense renvoie à un marché très mature nécessitant les technologies les plus complexes. Liées à des domaines de souveraineté, les contraintes sont également plus fortes en termes de sécurité et les contrats portent souvent sur de petites séries (principe de différenciation des solutions). L'accès à ce type de marché est donc limité et nécessite souvent des regroupements d'acteurs industriels de tailles diverses pour répondre à des besoins techniques complexes. Pour ces raisons, la Défense reste un marché de niche pour les acteurs industriels, et ce, malgré des taux de croissance affichés substantiels.

Les marché civils offrent quant à eux les taux de rentabilité les plus élevés. Ils tirent donc le marché de la cybersécurité. En revanche, des spécificités se font jour entre trois catégories[6] :

- administrations publiques et gestionnaires d'infrastructures vitales : il s'agit ici de marchés faisant essentiellement l'objet de règlementation. L'accès y est donc limité et contraignant ;
- grands groupes et ETI : les exigences de sécurité sont fixées individuellement. Marchés les plus rentables mais les problématiques d'internationalisation des sites des groupes et ETI poussent ces derniers à recourir à des prestataires

en matière de cybersécurité reconnus sur le marché et disposant de solutions innovantes ;

- PME & consommateurs : les budgets mobilisables sont relativement faibles, les clients ont recours à des solutions référencées comme leader du marché.

Par ailleurs, les marchés civils peuvent être appréhendés à travers une approche métier. L'objectif est alors de prendre en compte le contexte, les règles juridiques et normes techniques spécifiques s'imposant à celui-ci (secteur bancaire, santé, e-administration, etc.).

Enfin, les intégrateurs, en plus d'être des acteurs industriels, se présentent également comme une catégorie de clients importants. Dans ce cas, ils peuvent se positionner comme intermédiaires sur de nombreux marchés.

La cybersécurité recouvre donc des solutions très variées. La demande est disparate et la Défense apparaît comme un marché de niche. Ce constat explique pourquoi, au-delà des groupes de défense, des profils variés d'acteurs industriels disposent ou développent une offre en matière de cybersécurité, notamment à destination du marché Défense ou pouvant satisfaire aux exigences des clients Défense.

Les spécificités propres à chaque acteur industriel semblent de moins en moins marquées (logique d'intégration verticale des activités), néanmoins la création d'une typologie d'acteurs offre une vision d'ensemble des écosystèmes impliqués dans la cybersécurité ainsi que des différents modèles économiques. Or, la compréhension de ces modèles par les pouvoirs publics semble déterminante pour mener des actions de soutien et de renforcement d'une base industrielle de cybersécurité.

Le positionnement des industries de défense sur le marché de la cybersécurité

Les industriels historiques de la défense figurent en tant que leaders du marché auprès du client Défense. Ils bénéficient de la relation privilégiée nouée avec ce dernier, de capacités d'intégration et de maîtrise d'œuvre de programmes complexes ainsi que d'une empreinte internationale. Les groupes de défense privilégient un mode de vente directe auprès du client Défense. Par ailleurs, en assurant une présence locale via l'adoption d'une stratégie multidomestique, ils nouent également des relations directes avec les clients étrangers. Dans ce cadre, la stratégie de pénétration de marché peut passer par la création *ex-nihilo* d'une filiale (société de droit local) ou par l'acquisition d'un acteur local, qu'il soit consultant ou éditeur. Ainsi, quand la R&D est réalisée localement, les groupes se positionnent en tant que « fournisseur domestique » des clients Défense (solutions de souveraineté).

En outre, dans un contexte de contraction des commandes d'équipements de défense au milieu des années 2000, ces acteurs avec notamment aux États-Unis, Raytheon, Lockheed Martin et Northrop Grumman (pour ne citer que les principaux), en Europe, BAE Systems, Airbus Defence & Space, Thales, Leonardo et Rohde & Shchwarz ont affiché progressivement des ambitions de positionnement sur les marchés civils (administrations publiques & OIV et grands groupes principalement), et ceci, malgré une très forte intensité concurrentielle.

Le développement d'une offre en matière de cybersécurité peut alors dériver pour ces derniers de :

- « *spin-in* » de technologies défense ;
- stratégie de croissance externe. Les groupes de défense ont été à l'origine de nombreuses opérations de rachats d'entreprises au cours de ces dix dernières années, avec pour cœur de cible les acteurs de la cybersécurité (PME, ETI et filiales de grands groupes)[7] ;
- Établissement de partenariats stratégiques avec des acteurs spécialisés.

Cette extension de leur gamme de solutions permet aux groupes de défense d'atteindre de nouveaux marchés, en diversifiant leur portefeuille clients vers des administrations civiles, voire des acteurs privés (grands groupes). La consolidation de leur offre de cybersécurité passe ensuite par les axes stratégiques suivants :

- Création d'une ligne d'activités (Business Unit, BU) dédiée à la cybersécurité. Par cette stratégie, les groupes visent en priorité le marché domestique de la Défense, les administrations civiles (nationales et internationales) et les opérateurs d'importance vitale (OIV). L'intégration de solutions sur étagère, via le développement de partenariats avec les leaders mondiaux de la cybersécurité, permet de renforcer cette ligne d'activités.
- Mise en place d'une filiale cybersécurité dédiée, laquelle consolide les activités des acteurs spécialisés rachetés par le groupe de défense. Il peut ainsi bénéficier de leurs canaux de ventes, mais, si ces entités nouvellement acquises disposent d'une « marque » forte (très bonne visibilité auprès des clients finaux), celle-ci peut être préservée. Les acquisitions d'entreprises spécialisées ciblent généralement des acteurs positionnés sur les marchés civils, permettant au groupe de défense de diversifier son portefeuille client et se positionner sur les marchés les plus attractifs (grands groupes).

A l'inverse, les groupes de défense sont de plus en plus confrontés à la concurrence des entreprises issues du secteur du numérique et des télécommunications. Dans ce contexte, ils doivent notamment être en mesure de résoudre les problématiques liées à l'absence de synergie avec leur cœur d'activités. Plus particulièrement, ils doivent adapter leur stratégie en prenant en compte les caractéristiques propres à la cybersécurité tel que le cycle court de l'innovation.

Ainsi, plusieurs acteurs défense ont opéré un retrait des marchés civils[8]. Par exemple, avec la vente de sa filiale Morpho à Oberthur, le groupe Safran a opté pour une stratégie de recentrage autour de ses activités dans l'aéronautique et la défense[9]. Aux États-Unis, Lockheed Martin a notamment fait le choix de sortir des marchés administrations publiques et IT après la cession en 2016 des activités IT & Technical Services à Leidos.

Marchés de la cybersécurité et de l'armement : approche comparée

	Cybersécurité	Armement
Demande (principaux clients)	Disparate	Limitée aux clients gouvernementaux
État de la concurrence	Forte intensité concurrentielle	Variable selon les segments
Barrières à l'entrée	Faibles	Fortes
Cycle d'innovation	Court	Long
Ruptures technologiques (fréquences)	Élevée	Modérée

Le groupe américain a néanmoins conservé ses activités cyber les plus critiques[10].

La montée en puissance des entreprises issues du numérique

Depuis quelques années, les entreprises issues du secteur du numérique (au sens large, électronique inclue) affirment leurs ambitions sur le marché de la cybersécurité, dont client Défense. Celles-ci disposent de plusieurs avantages concurrentiels :

- base clients très importante sur le marché civil (grands groupes et administrations publiques) ;
- positionnement sur des activités à forte rentabilité (intégration, conseils et services associés) ;
- capacités d'investissement élevées (politique de fusion-acquisition) ;
- politique de partenariat dédiée avec les start-ups et PME spécialisées ainsi que les incubateurs, laboratoires collaboratifs, etc. Les structures des grands groupes sont trop lourdes pour répondre à l'exigence du cycle court de l'innovation qu'impose la cybersécurité, amenant ces derniers à coopérer avec des structures innovantes et agiles (start-ups et PME). Or, les entreprises du numérique disposent ici d'un avantage par rapport aux groupes de défense dans la coopération avec ces start-ups et PME car elles sont pleinement intégrées dans leur écosystème.

Même si leur catalogue d'offres tend à se « lisser » en raison notamment du développement des activités d'infogérance et de services de *cloud computing*, des disparités subsistent entre les différents acteurs du numérique. Ces disparités, liées au positionnement d'origine sur le marché, permettent de comprendre les stratégies actuellement mises en œuvre.

Fabrication de matériels et d'équipements : les acteurs *pure-players*, c'est-à-dire les entreprises spécialisées dans la production de matériels et d'équipements, offrent des solutions sécurisées *by design*. Dans ce cadre, ils privilégient le développement en interne de technologies de sécurité (brevets) tout en établissant des partenariats stratégiques avec des acteurs spécialisés de la cybersécurité. Toutefois, la sécurité est aujourd'hui encore majoritairement perçue par les clients finaux comme un coût supplémentaire, et non comme un avantage compétitif. A terme, ce constat devrait évoluer, les produits sécurisés *by design* constitueront un élément déterminant de différenciation de l'offre (intégration de clauses de sécurité). En effet, le développement des réglementations nationales et internationales sur plusieurs marchés spécialisés semble inéluctable (systèmes industriels connectés et objets connectés notamment).

Aujourd'hui, l'accès aux marchés pour les fabricants de matériels et d'équipements est principalement réalisé en B2B (*Business to Business*) et se traduit par des accords négociés entre les systémiers-intégrateurs mondiaux ainsi que par la vente indirecte (solutions intégrées dans le catalogue d'intermédiaires spécialisés). Néanmoins, la volonté des fabricants de matériels et d'équipements de diversifier leurs activités au profit d'une offre de services a tendance à faire évoluer la relation avec les systémiers-intégrateurs : d'un canal de vente historique, celle-ci tend dorénavant vers un partenariat (avec pour certains cas des ambitions de croissance externe).

Les systémiers-intégrateurs, presque exclusivement américains, cherchent quant à eux à diversifier leurs activités. Dans ce cadre, une stratégie d'intégration verticale est largement privilégiée, avec pour cible les éditeurs de logiciels et les prestataires de services informatiques. Ils profitent ainsi d'une situation dominante grâce à leurs activités IT à partir desquelles ils proposent des solutions de cybersécurité dédiées mais aussi des services associés.

Édition logicielle : les grands groupes mondiaux *pure-player* historiquement positionnés sur le marché de la cybersécurité, hormis SAP et Sophos, sont non-européens et cotés en bourse.

En phase de croissance externe, ils profitent d'importantes réserves de *cash*. Leur objectif est d'intégrer en permanence des mécanismes et des solutions de sécurité dans leur offre et de disposer d'une main d'œuvre qualifiée en nombre suffisant.

À leur côté, les PME disposant de technologie(s) de niche représentent dans ce contexte des cibles privilégiées des éditeurs de logiciels, mais aussi des fabricants de matériels et d'équipements ainsi que des groupes de défense. Pour ces acteurs, la confiance client représente une problématique majeure. Malgré un coût élevé, ces derniers ont ainsi largement recours aux processus nationaux de certification et de qualification, afin de garantir un niveau de sécurité auprès des clients.

De plus, à leur stade (start-up ou PME), l'objectif primordial des éditeurs spécialisés est de disposer de capacités de financement élevées (capital-risque, fonds publics, entrée en bourse, etc.) en vue d'assurer une croissance interne importante et disposer le plus rapidement possible d'une visibilité critique sur le marché. En effet, la vente indirecte en B2B constitue le canal de vente privilégié. Dans ce cadre, l'entreprise doit tisser un réseau composé de systémiers-intégrateurs, de revendeurs et de grossistes. Or, pour intégrer des solutions dans leur catalogue, ces derniers s'appuient essentiellement sur :

- la réputation commerciale de la solution (référencement, qualification, certification, etc.);
- la capacité de l'entreprise à déployer la solution à grande échelle.

Dans une moindre mesure, les éditeurs disposent également du canal de vente *online* dont la qualité dépend principalement du référencement web.

Prestation de services : les prestataires de services sont principalement les entreprises de services du numérique (ESN). Parmi les ESN, les groupes de taille mondiale tirent profit de leurs références clients type « grands comptes » pour déployer des solutions de sécurité des SI. Ces entreprises développent notamment des offres de services de sécurité managés autour de SOC/CERT. À leur côté, subsistent les ESN à rayonnement local, principalement positionnées sur les marchés des ETI/PME et administrations (collectivités territoriales par exemple).

Un des enjeux majeurs des ESN réside dans leur capacité à créer une relation de confiance et de proximité avec les clients finaux. Elles doivent ainsi assurer un maillage du territoire, en partie réalisé grâce à la création de sites de services locaux rattachés au groupe. À l'international, les problématiques restent similaires. Les ESN privilégient une stratégie multidomestique, condition d'une proximité suffisante avec le client final. Elles sont alors en mesure d'intervenir en tant qu'intégrateur, aux côtés des systémiers-intégrateurs historiques (catégorie fabricants de matériels et d'équipements informatiques).

Enfin, la sélection par les clients finaux dépend également des solutions intégrées. Dans ce cadre, les ESN multiplient les partenariats et accords de distribution avec les acteurs mondiaux dans leur domaine, essentiellement américains, car mieux reconnus par les clients finaux, en partie grâce à leur

présence au sein de *benchmarks* réalisés par des cabinets anglo-saxons tels que ceux du cabinet Gartner[11].

La catégorie des prestataires de services recouvre aussi les acteurs industriels spécialisés dans les travaux de R&D. Leur modèle économique repose sur la licence de brevets (royalties). Ces acteurs sont pleinement insérés dans l'écosystème de recherche local en prenant part à de nombreux projets de recherche (et menés bien souvent en partenariat). Ce modèle économique impose de détenir de nombreux brevets (problématiques liées aux dépôts) qu'il convient ensuite de revendre, principalement aux acteurs relevant de la catégorie fabrication de matériels et d'équipements. L'entreprise peut aussi développer son modèle économique sur la vente de services associés au développement d'un produit. Dans ce cas, celle-ci a aussi recours au réseau de vente indirect.

Les opérateurs de télécommunication

Grâce à leurs moyens techniques et financiers, les opérateurs de télécommunication ont pénétré progressivement le marché de la cybersécurité par le biais d'offres de solutions de sécurisation des données et de services de cloud. Maîtrisant les « tuyaux » d'information, l'axe de développement privilégié consiste à sécuriser l'information qui y circule.

L'acquisition d'entreprises prestataires de services et l'établissement de liens de partenariats avec les fournisseurs spécialisés (systémiers-intégrateurs, éditeurs de logiciels et fabricants de matériels et d'équipement) forment le socle de développement de leurs activités de cybersécurité.

Le rachat d'activités industrielles de cybersécurité permet aux opérateurs de télécommunication de créer ou renforcer une nouvelle BU cyber. Celle -ci peut alors étoffer les offres historiques de communication des opérateurs par l'intégration de solutions et de services de cybersécurité, ou opérer directement sur le marché de la cybersécurité (solutions dédiées). La multiplication des partenariats avec les entreprises spécialisées du secteur a pour objectif d'intégrer des solutions de cybersécurité reconnues par les clients au sein des offres historiques et/ou intégrer une brique technologique dans le développement d'une offre 100% de cybersécurité (*via* la BU cyber).

Une filière de cybersécurité européenne ?

Le secteur industriel français de la cybersécurité a connu d'importantes mutations au cours des dernières années. Les pouvoirs publics français ont notamment multiplié les initiatives visant à renforcer ce secteur[12]. En parallèle, le paysage industriel français de la cybersécurité a vu l'entrée de nouveaux acteurs (issus de la Défense, sécurité numérique, etc.). Enfin, de nombreuses opérations de fusion-acquisition[13] ont participé à la consolidation des activités de cybersécurité des entreprises tête de pont de la filière (Thales-Gemalto, Atos-Bull, Airbus Cybersecurity, Sopra-Steria, Idemia, etc.).

Malgré ces évolutions, le secteur industriel de cybersécurité français semble toujours atomisé[14]. Or, l'environnement déjà hautement concurrentiel voit l'émergence de filières nationales en Chine, en Israël, au Royaume-Uni, ou encore en Allemagne. Rappelons par ailleurs que les États-Unis disposent du tissu industriel le plus dense dans le domaine de la cybersécurité. Bénéficiant notamment de la taille du marché domestique, la base industrielle de cybersécurité américaine comprend les principaux acteurs mondiaux : systémiers-intégrateurs (Cisco, FireEye, IBM, Microsoft, HP Dell), éditeurs de logiciels *pure-player* (Symantec, etc.), ou encore groupes de défense disposant d'une offre cyber (Raytheon, Lockheed Martin, General Dynamics, etc.).

Dans ce contexte, la Commission européenne s'est emparée des sujets numériques et *in fine* de la cybersécurité. Les initiatives prises par cette dernière s'inscrivent dans le cadre de la Stratégie de cybersécurité de l'Union européenne[15], laquelle affiche notamment les objectifs de développement de capacités industrielles et technologiques en matière de cybersécurité. Ainsi, la communication relative à la création d'un « marché numérique unique » (*Digital Single Market*)[16] rappelle ces enjeux et illustre la volonté de la Commission européenne d'influencer la structuration du marché européen de la cybersécurité à travers une évolution du cadre réglementaire et des initiatives public-privé.

Des avancés concrètes ont eu lieu *via* notamment l'adoption de règles européennes, avec l'objectif de construire un véritable marché européen de la cybersécurité. Par exemple, l'adoption du règlement EIDAS, abrogeant la directive 1999/93/CE relatif à la signature électronique en Europe[17], permet d'harmoniser les normes européennes sur le segment de l'identification électronique. De plus, l'adoption, le 6 juillet 2016, de la directive *Network and Information Security* (NIS)[18], devrait permettre de renforcer la sécurité des réseaux et des systèmes d'information européens. Cette dernière est également susceptible d'avoir des effets sur la structuration du marché.

Les avancées vers un marché unique européen de la cybersécurité semblent tangibles. Néanmoins, plusieurs problématiques demeurent en raison de divergences entre États membres. Premièrement, la mise en place de schémas de certification de solutions de cybersécurité à l'échelle européenne s'annonce délicat[19]. Deuxièmement, l'absence de définition partagée entre États membres en matière d' « industrie de cybersécurité européenne » représente un point dur majeur [20].

Quelle politique industrielle de défense en matière de cybersécurité ?

La compréhension des enjeux industriels propre aux différents acteurs offre un premier aperçu des dynamiques actuellement à l'œuvre. Il ressort de ce constat la difficulté d'adopter des mesures de soutien à grande échelle tant les problématiques et modèles économiques des acteurs industriels de cybersécurité divergent. De plus, le développement d'une capacité nationale de cybersécurité, et plus spécifiquement cyberdéfense, est inhérent à la présence au préalable d'une industrie de défense et du numérique ainsi qu'à l'adoption d'une stratégie nationale spécifique, intégrant un volet industriel. Quelques pays, dont la France, ont pour l'heure mis en œuvre une politique industrielle dédiée à la constitution d'une base industrielle et technologique de cybersécurité (BITC). Ainsi une première lecture de ces orientations de politiques publiques fait ressortir les points suivants :

- développement de formations universitaires adaptées permettant de disposer de ressources humaines en qualité et nombre suffisant (à même d'accompagner la croissance du secteur) ;

- politique de R&D dédiée (plan d'investissements, feuilles de route industrielles) ;
- Adoption de nouvelles règlementations contraignantes en matière de cybersécurité avec pour objectif de stimuler la demande et conséquence de structurer de nouveaux marchés ;
- multiplication de mesures incitatives en vue d'attirer les investissements en capital-risque ;
- mise en place de clusters régionaux réunissant notamment les acteurs industriels et leurs centres de R&D, les pôles de formation, les laboratoires de recherche, les clients finaux et les capitaux-risqueurs.

En outre, l'orientation civile des acteurs industriels de la cybersécurité impose au ministère des Armées de repenser le dialogue Etat-Industries dans ce domaine. Ce constat pose d'ailleurs plus généralement la question de la capacité des Armées à intégrer les innovations venues du civil, en particulier dans les domaines liés à la cybersécurité et à l'intelligence artificielle. C'est notamment l'objectif affiché par la LPM 2019-2025 : « *capter en cycle court l'innovation issue du marché civil, en tirant partie de la révolution numérique (…). Cette démarche s'appuiera largement sur la construction d'un écosystème d'innovation, interne au ministère des armées et connecté avec les écosystèmes d'innovation civils* »[21]. La création d'une agence de l'innovation placée au sein de la DGA est censée apporter une première réponse à cette problématique, comme le rappelle, Florence Parly, ministre des Armées : « *La nouvelle agence de l'innovation aura donc pour mission d'organiser les échanges avec cet écosystème de l'innovation, qui est plutôt civil* »[22].

Dans ce contexte, le renforcement de la base industrielle de cybersécurité française et européenne, nécessaire pour garantir un niveau de souveraineté numérique, dépasse le seul cadre d'une politique industrielle de défense. Celle-ci semble devoir s'inscrire dans une action plus transversale afin de bénéficier d'effets de levier pour la structuration du secteur. La prise en compte, dans cette approche transversale, des besoins spécifiques liés à la Défense apparaît essentielle pour atteindre les objectifs affichés.

KÉVIN MARTIN
Chargé de recherche
Pôle Défense & Industries, FRS
k.martin@frstrategie.org

Notes

1.Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, 12 février 2018.

2. *Ibid*.

3. « Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017 », *Gartner,* 7 décembre 2017.

4. « Cybersecurity Market worth 231.94 Billion USD by 2022 », *Markets&Markets*, juillet 2017.

5. ECSO, *European cybersecurity industry proposal for a contractual public-private partnership*, juin 2016.

6. Cette segmentation s'appuie sur celles adoptées par diverses études : TechUK, *Assessing Cyber Security Exports Risks,* November 2014 ; Pierre Audoin Consultants, *Competitive analysis of the UK cybersecurity sector*, juillet 2013 ; AFDEL, *Livre Blanc cybersécurité : hisser les acteurs français au niveau de la compétition mondiale*, juin 2014.

7. En Europe on peut, par exemple, évoquer les acquisitions d'Airbus (Arkoon, Netasq), de Thales (activités cyber d'Alacatel Lucent, Vormetric, Guavus, Gemalto), BAE Systems (Detica, Stratesc, ETI A/S, Norkom, SilverSky) ou Rohde & Schwarz (GateProtect, Adytom Systems, Sirrix AG, DenyAll).

8. « Top five U.S. defense contractors bungle commercial cybersecurity market opportunity », *CSO*, 28 janvier 2016.

9. Cession de Morpho par le groupe Safran, réponse du Ministère de la défense à la question écrite n°23397, *JO Sénat* , 23 février 2017, p. 737.

10. « Lockheed Martin Successfully Closes Transaction to Separate and Combine IT and Technical Services Businesses with Leidos» *Communiqué de presse Lockheed Martin,* 16 août 2016.

11. Cf. Gartner Magic Quadrant.

12. D'Elia Danilo, « La cybersécurité, entre bien public et marketing de la peur », *in Quelles stratégies face aux mutations de l'économie mondiale ?* , Etude de l'IRSEM, n°38, avril 2015.

13. Depuis 2011, l'auteur dénombre près de 100 opérations de fusions-acquisition dans le domaine de la cybersécurité impliquant des acteurs industriels français.

14. Alliance pour la confiance numérique, *L'observatoire de la filière de la confiance numérique en France*, 2017.

15. Communication de la Commission européenne, *Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé*, 7 février 2013.

16. Communication de la Commission européenne, *Stratégie pour un marché unique numérique en Europe*, 6 mai 2015.

17. Parlement européen et Conseil de l'Union européenne, *Règlement N° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, 23 juillet 2014.

18. Parlement européen et Conseil de l'Union européenne, *Directive 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, 6 juillet 2016.

19.Mazucchi Nicolas, *2018, une année charnière pour l'Europe dans le cyber ?*, Note de la FRS, 22 janvier 2018.

20. Cf. Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, 12 février 2018 : « *La construction d'une base industrielle de cybersécurité et cyberdéfense [européenne] se heurte aujourd'hui à deux difficultés (…) La seconde difficulté est une certaine différence de conception entre États membres de l'Union européenne sur la nature d'une entreprise européenne »,* p.120.

On notera que cette problématique n'est pas spécifique à la cybersécurité, la question renvoyant à celle de la BITD européenne. Voir à ce sujet Hélène Masson (ed.), Christian Mölling, Keith Hartley, Martin Lundmark, Krzysztof Soloch, *Defining the « European Defence Technological and Industrial Base »: Debates & Dilemmas (I)*, Note de la FRS, 26 juillet 2013.

21. Ministère des Armées, *Projet de loi de programmation militaire 2019/2025—Rapport annexé*, 2018, p. 54.

22. « Entretien de la ministre des Armées », *Usine nouvelle*, 31 mai 2018.

Le LCA60T de Flying Whales
source FW


Le NATAC (Navette de Transport Automatique de Containers) de la société française Voliris. *source : Voliris*

Regain d'intérêt pour les aérostats : les dirigeables transporteurs de charges lourdes

L'usage militaire d'aérostats remonte à plus de deux siècles, lors des guerres de la révolution française, et a connu son paroxysme durant la première guerre mondiale, que ce soit par le recours à des ballons captifs pour l'observation et les sondages d'artillerie, ou par le bombardement aérien de villes belges, anglaises ou françaises par les premiers dirigeables Zeppelin.

Malgré le déclin des dirigeables commerciaux avant la seconde guerre mondiale, les aérostats sont utilisés de manière continue jusqu'à aujourd'hui par des forces armées, notamment américaines. Outre des dirigeables porte-avions au milieu des années 1930 (USS Arkon et USS Macon), des dirigeables et des ballons ont servi pour la lutte anti-sous-marine pendant une partie de la guerre froide. Des ballons captifs contribuent toujours à la protection de périmètres, qu'ils s'agissent de frontières ou de bases militaires.

Appartenant à la famille des aéronefs, les aérostats désignent les « plus-léger -que l'air », par opposition aux aérodynes (les « plus-lourd-que-l'air »). Parmi les aérostats, le dirigeable se distingue du ballon par sa motorisation et sa capacité à être manœuvré. Les ballons peuvent être captifs ou libres.
Vecteurs aériens économiques et endurants, les aérostats bénéficient d'un regain d'intérêt pour l'ISR (Intelligence, Surveillance, Renseignement, missions qui feront l'objet d'un prochain article), mais aussi pour leur potentiel en matière logistique. En effet, le poids croissant de la logistique sur les capacités d'action d'une force militaire lors des opérations extérieures incite à explorer de nouvelles solutions de transport.

Pour des forces militaires ou de sécurité civile, l'intérêt porté aux dirigeables transporteurs de charges lourdes (LCA, pour *Large Capacity Aircraft*) provient de la conjonction de deux éléments : les retours d'expérience militaires récents en matière logistique, et la maturité à court terme de plusieurs projets de LCA ayant une capacité d'emport jusqu'à 60 tonnes.

Les limites des dirigeables comme vecteurs logistiques stratégiques (entre la métropole et un théâtre d'opération extérieur)

Les besoins massifs en vecteurs logistiques stratégiques ces dernières années, que ce soit pour le retrait d'Afghanistan ou pour le déploiement des dispositifs en Afrique subsaharienne, ont souligné la faiblesse des moyens patrimoniaux français dans ce domaine, et une très forte dépendance à des opérateurs étrangers, en particulier russes et ukrainiens[1] (notamment des AN-124 et un AN-225).

Cependant, les projets au-delà de 100 tonnes demeurent théoriques, et tous les projets dans cette catégorie sont aujourd'hui suspendus ou abandonnés (RosAeroSystems, Aeros…)[2]. De plus, l'emploi de ces dirigeables géants comme vecteur stratégique ne va pas de soi dans une perspective militaire. Le poids logistique nécessaire à un déploiement ne sera pas compatible avec les limites d'un aérostat : incertitudes de la réalisation des vols liées aux conditions météorologiques, vitesse moindre des dirigeables, insertion dans le trafic aérien international d'un tel « pont aérien », interdiction de vol au-dessus de certains États, impact d'un détour sur la durée totale du vol, etc. Pour la phase de soutien au stationnement dans la durée, le recours au transport maritime conservera un avantage par son coût moindre, et le respect des délais (transport *just in time*).

Le succès, à court et moyen termes, de LCA moins ambitieux (autour de 2 tonnes, et entre 12 et 60 tonnes, matériels en cours de développement) sera très probablement la condition pour ré-explorer la faisabilité et l'intérêt des LCA « hyper lourds ».

L'intérêt des LCA comme vecteur logistique intra-théâtre (au sein même d'un théâtre d'opération)

En zone où la menace est sensible (zone non permissive), les retours d'expérience démontrent que tout convoi de ravitaillement circulant entre une FOB (base opérationnelle avancée ou *forward operating base*) et la BSIA (Base de soutien interarmées) devient une opération militaire mobilisant de gros moyens interarmées, et entravant pendant cette période la capacité de la force à exécuter sa mission principale.

Dans le cadre de la force Barkhane, les opérations « Charente » permettent le ravitaillement de l'ensemble des positions implantées dans la bande saharo-sahélienne (BSS)[3]. D'une fréquence de 1 à 2 par mois, les convois « Charente » mobilisent entre 60 et 150 véhicules et jusqu'à 400 hommes, parfois entre 10 et 14 jours pour faire l'aller-retour entre les points les plus éloignés. Ces convois nécessitent également la mise en alerte d'une chaine sanitaire, incluant des moyens héliportés, ainsi que le recours à des hélicoptères de reconnaissance et à des drones (et dans certains cas des avions de chasse et des éléments terrestres en alerte). Hommes et matériels sont

alors exposés à des attaques ennemies, à l'image du convoi « Charente 09 » entre Gao et Tessalit en avril 2016 au cours duquel trois personnels ont trouvé la mort lors de la destruction d'un véhicule blindé par un IED.

Le transport automatisé de charges lourdes par des aérostats permettrait de s'affranchir du risque relatif aux IED et des contraintes du milieu naturel, dans le but à la fois de préserver les hommes et d'économiser l'emploi des moyens patrimoniaux des armées.

Dans une logique de standardisation menée depuis 2011, le container de 20 pieds (KC 20) constitue le principal conditionnement (50 à 80% des Unités à Transporter – UAT) de matériel utilisé par les Armées, qui en détiennent 6500 en propre aujourd'hui. Outre une manutention plus aisée (y compris le chargement dans les avions) et le fait que les camions tous terrains de l'armée de Terre ne peuvent pas transporter des containers de taille supérieure (y compris les porteurs polyvalents logistiques ou PPLOG), une logistique standardisée permet d'éviter les ruptures de charge entre le point de départ et la destination finale, où le container servira également à stocker et protéger le matériel. Le transport par container de 20 pieds, avec une capacité de chargement et déchargement autonome, apparaît donc comme un préalable pour tout nouveau vecteur logistique intra-théâtre.

Les avantages d'un dirigeable sont nombreux : coût d'utilisation inférieur aux autres vecteurs aériens, capacité d'emport entre 12 tonnes et 60 tonnes pour les projets les plus avancés (soit de 1 à 4 KC 20), possibilité à moyen terme de droniser les aérostats, faible empreinte au sol pour l'atterrissage et le décollage (vertical ou sur une piste courte et sommairement aménagée). La vitesse des principaux dirigeables oscillera entre 100 et 150 km/h, ce qui, conjuguée à une endurance d'au moins 1000 km, permettra d'effectuer un aller-retour Gao-Tessalit en une nuit.

L'utilisation des LCA n'aurait pas été possible sur tous les théâtres d'opérations où ont été engagées les armées françaises ces deux dernières décennies. Pour autant, son intérêt opérationnel pour le soutien logistique de nos forces armées déployées sur un théâtre d'opération apparait manifeste malgré des contraintes : le recours à les LCA doit être limité à des zones d'opérations où le niveau de menace est faible à modéré[4], dans des périodes temporelles où la météorologie permet à ces machines d'évoluer en toute sécurité. Un affrètement de LCA auprès d'un opérateur civil, en fonction des besoins en OPEX, apparaît davantage pertinent qu'un achat sur étagère et la création d'une unité dédiée.

Les dirigeables automatiques ou pilotés pourraient également contribuer à diverses missions comportant une dimension militaire ou sécuritaire : désenclavement de zones difficiles d'accès (par exemple après une catastrophe naturelle de grande ampleur), opérations dans des aires où le climat est particulièrement hostile au matériel et aux hommes (désert), ou encore de milieux pour lesquels les forces ne disposent pas de vecteurs logistiques adaptés (Arctique).

Une filière française particulièrement dynamique

Des dirigeables automatiques ou pilotés capables de transporter des containers sont actuellement en phase d'étude technique ou de démonstrateur en France, au Royaume-Uni, en Allemagne ou encore aux États-Unis. Une offre crédible de LCA se construit et devrait déboucher sur des modèles commerciaux à un horizon de cinq ans. La filière française se caractérise par son dynamisme. Dix des 19 démonstrateurs habités développés dans le monde depuis le milieu des années 1990 sont français[5]. La filière s'est notamment structurée dans le sud-est, initialement autour du pôle de compétitivité Pégase depuis 2007. En décembre 2013, l'initiative « Nouvelle France Industrielle » portée par le gouvernement de Jean-Marc Ayrault consacre l'un de ses « 34 Plans » au secteur « Dirigeables et drones civils », affichant l'ambition d'un chiffre d'affaires d'un milliard d'euros en 2025 par la filière dirigeable[6]. L'initiative « Nouvelle France Industrielle » est refondue en 10 solutions industrielles à l'arrivée d'Emmanuel Macron au ministère des Finances. Les projets de dirigeables sont intégrés dans la solution « Transports de demain »[7].

Trois projets seront labellisés en 2014 par le nouveau pôle de compétitivité SAFE Cluster, né de la fusion des pôles Pégase et Risques :

- Le LCA60T (dirigeable de 140 m ayant une capacité d'emport de 60 tonnes à la vitesse de 100 km/h) de Flying Whales ;
- L'Aerolifter d'Airstar (dirigeable filoguidé d'une capacité de 2 tonnes) ;
- Le Stratobus de Thales Alenia Space (dirigeable dédié à l'ISR, emportant 250 kg).

Les constructeurs anglo-saxons HAV et Lockheed Martin ont bâti leurs projets à partir de démonstrateurs destinés à un usage militaire. Outre une conception initiale qui a déjà au minimum 10 ans, l'Airlander 10 (HAV) et le LMH-1 (Lockheed Martin) doivent encore faire l'objet de modifications pour s'ajuster à des demandes commerciales civiles. Le LMH-1 devrait achever d'ici 2020 le processus de certification de vol, ce qui lui permettrait d'être le premier LCA disponible sur le marché à cet horizon. 24 appareils ont fait l'objet d'intention d'achat, mais aucune commande ferme n'a été passée.

Par opposition, l'approche des deux constructeurs français Voliris (concepteur du NATAC - Navette de Transport Automatique de Containers) et Flying Whales (LCA-60t) repose pour chacun d'eux sur un usage précis : le transport de fret par container dans des zones difficiles d'accès pour le premier, et l'exploitation forestière pour le second. Flying Whales a la particularité de conduire à cet effet une démarche industrielle (faisabilité économique, faisabilité technique, définition et dimensionnement des sous-systèmes, création d'un consortium d'ingénierie avec une trentaine de partenaires, etc.) avec une équipe d'une quarantaine de salariés. Et l'actionnariat de Flying Whales s'est engagé sur un investissement de 90 millions d'euros, et se compose notamment de ses deux principaux clients (dont l'ONF), ce qui constitue un gage de pérennité du projet.

Conclusion

Les cinq prochaines années feront sans doute figure de test pour l'avenir du dirigeable charge lourde. L'intérêt pour cette filière est périodique, et n'a débouché au final que sur une trentaine de dirigeables légers (hors Intelligence, Surveillance et Renseignement) en service dans le monde, principalement pour la communication, la publicité ou le tourisme. La convergence constatée aujourd'hui entre quatre facteurs (une demande identifiée pour des dirigeables charges lourdes, un financement entre autres par des

clients potentiels, un fort soutien politique à la filière aérostatique, et une commercialisation à un horizon court) donne une crédibilité inédite à cette gamme d'aérostats, et à des usages militaires potentiels

Alexandre TAITHE
Chargé de recherche, FRS
a.taithe@frstrategie.org

GBA (2s) Philippe BOUSSARD
Chercheur associé, FRS

Notes

1.CORNUT-GENTILLE François, *Rapport d'information relatif au transport stratégique*, Assemblée nationale, n°4595, 28 mars 2017, 59 p.

2.Les projets de l'américain Aeros allaient jusqu'à 250 voire 500 tonnes (pour les projets ML 868 et ML 86X), avec en théorie des coûts d'acquisition, d'exploitation et de maintenance nettement inférieurs à celui des avions très gros porteurs, tout en disposant d'une autonomie de plusieurs milliers de km.

3.Voir : « Opex : la force Barkhane et l'opération Charente 19 », *L'histoire en rafale,* 29 septembre 2017,

4.Pouvant facilement évoluer à 10 000 pieds, les dirigeables sont peu vulnérables aux tirs d'armes légères. Les phases de décollage et d'atterrissage (ou de déchargement) exigeront la protection d'un périmètre autour de l'aérostat. Le stationnement ne devra être envisagé que dans une zone permissive. Au regard de leur volume et de la très faible surpression à l'intérieur de l'enveloppe, les dirigeables résistent très bien à des perforations multiples. Un impact conduit à une perte d'hélium inférieure à 20 m3 par heure, à comparer aux dizaines de milliers de m3 contenus dans un LCA.

5.MOLGA Paul, « Les Français repris par la folie du dirigeable », *Les Echos*, 21 janvier 2016.

6.http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/17780.pdf

7.https://www.economie.gouv.fr/nouvelle-france-industrielle/transports-demain

Les mutations de l'industrie finlandaise de la défense et les participations capitalistiques croisées entre pays nordiques : une approche d'économie historique

Cet article s'intéresse aux mutations de longue durée de l'industrie finlandaise de la défense et à ses évolutions récentes qui conduisent à la mise en œuvre de participations industrielles et capitalistiques croisées entre certains pays nordiques. Ces relations concernent plus spécifiquement deux Etats : la Norvège et la Finlande, via les firmes Kongsberg, Patria et Nammo. La Suède et le Danemark, bien que participant à la coopération nordique de défense (NORDEFCO), ont en effet mis en œuvre d'autres formes de restructuration. Issues d'un long processus de consolidation et scellées par la montée de la firme norvégienne Kongsberg au sein du capital du groupe finlandais Patria en 2016, ces participations croisées peuvent être résumées comme suit :

- Le gouvernement norvégien détient 50,001% de la firme de défense et d'ingénierie Kongsberg Gruppen, le reste des parts étant coté à la bourse d'Oslo.
- Le gouvernement finlandais détient 50,1% de la firme d'aéronautique et de défense finlandaise Patria, le reste des parts étant détenu par Kongsberg Gruppen.
- Le gouvernement norvégien détient 50% des parts de la firme transnationale de munitions Nammo, à parité avec le groupe finlandais Patria.

Cet article repose sur une perspective d'économie historique visant à mettre en évidence les mutations de la firme comme organisation par rapport à celles de son environnement[1]. Il cherche donc à comprendre le processus par lequel l'industrie finlandaise de la défense a été amenée à s'orienter vers ce qui s'apparente à une coopération régionale renforcée dans le domaine industriel. Pour ce faire, nous nous intéresserons d'abord à l'évolution de l'industrie de la défense de la Finlande de son développement dans les années 1920 jusqu'à la fin de la guerre froide (I), puis aux mutations consécutives à la fin de la guerre froide et à la recherche de partenariats internationaux (II).

Historique des activités industrielles militaires finlandaises aujourd'hui consolidées dans Patria des années 1920 à la fin de la guerre froide

La Finlande est un pays qui obtient l'indépendance de la Russie soviétique en 1917. Pratiquement dépourvu d'industrie de la défense à cette date, le pays développe des capacités industrielles militaires modestes, qui prennent une nouvelle ampleur lorsque survient la guerre d'hiver face à l'Union soviétique en 1939, suivie de la Seconde Guerre mondiale puis de la guerre froide. Sont ici étudiées les activités relatives à l'aéronautique militaire (A), aux véhicules militaires (B) puis aux armes lourdes (C) afin d'analyser le processus de consolidation du secteur sur le long terme : toutes ces activités sont en effet consolidées en une entité unique, Patria, à la fin des années 1990.

Le secteur aéronautique militaire

Le président directeur général de Patria déclarait en 2011 « notre histoire industrielle remonte à 1921, lorsque l'usine d'avions de l'armée de l'air a débuté ses activités à Suomenlinna »[2]. Initialement simple atelier de maintenance de l'armée finlandaise, ce dernier devient une entreprise à la fin des années 1920 sous le nom de Valtion Lentokonetehdas (entreprise d'Etat de construction d'avions). Alors que le site de Suomenlinna (une forteresse du XVIII^{ème} siècle sur une petite île dans la baie d'Helsinki) est peu adapté au développement de cette activité, l'usine est transférée à côté de la ville de Tampere en 1936, à quelques 180 kilomètres au Nord d'Helsinki.

L'entreprise produit quelques avions de conception finlandaise pendant le second conflit mondial, mais ces derniers ne donnent pas entière satisfaction à l'armée de l'Air et son activité consiste surtout dans l'assemblage d'avions militaires allemands mais aussi britanniques sous licence. Après la fin des hostilités, le gouvernement finlandais cherche à réorganiser la production industrielle du pays. Ainsi, « en 1946, plusieurs ateliers du domaine de la métallurgie sont regroupés afin de former Valtion Metallitehtaat (Ateliers métallurgiques d'Etat). Au début de l'année 1951, le groupe Valtion Metallitehtaat fut renommé Valmet Oy, et sa production s'est développée au fil des ans jusqu'à inclure la fabrication de navires, d'avions, d'armements, de locomotives, de tracteurs, de moteurs maritimes, d'élévateurs et, bien sûr, de machines à papier »[3].

La fin du second conflit mondial marque cependant un coup d'arrêt pour le développement de l'industrie aéronautique militaire finlandaise, en raison des restrictions imposées par le traité finno-soviétique de 1948. Alors que cette période est caractérisée par un saut technologique du fait du développement de l'aviation à réaction, l'industrie aéronautique finlandaise qui intervient uniquement dans le domaine des petits avions à turbopropulseur se focalise sur deux domaines d'activité : assemblage local sous licence puis maintenance des avions de l'armée de l'air finlandaise acquis auprès de constructeurs étrangers, et fabrication d'avions d'entraînement pour forces armées. Le premier avion de conception finlandaise, le Vihuri, est ainsi produit dès 1951. Dans les années 1960, l'entreprise assemble localement les avions d'entraînement Fouga Magister acquis auprès de la France. Par la suite, elle assemble les avions de chasse suédois Draken, les

Les derniers programmes aéronautiques militaires finlandais

Les avions d'entraînement à turbopropulseur Vinka (à gauche) puis Redigo (à droite) constituent les derniers avions militaires de conception finlandaise. Succédant à plusieurs générations d'appareils, le Vinka est le premier avion de conception entièrement finlandaise. Construit à 30 unités au début des années 1980, il n'a pas été exporté mais il est toujours en service dans l'armée de l'Air de la Finlande. La cellule du Vinka a par la suite été modernisée afin de produire une nouvelle génération d'avions d'entraînement, le Redigo, jusqu'à ce que les droits pour la conception de l'appareil soient cédés au groupe italien Aermacchi en 1996, année de l'intégration de Valmet dans Patria.
Sources : airforce-technology.com et lentoposti.fi

avions d'entraînement britanniques Hawk dans les années 1980 et les avions de chasse américains Hornet dans les années 1990[4]. Elle poursuit également ses activités de construction d'avions d'entraînement, en particulier le Vinka puis le Redigo dans les années 1990. Les années 1980 sont cependant caractérisées par de fortes difficultés pour le conglomérat, qui se sépare de plusieurs de ses activités : chantiers navals, véhicules et engins agricoles… Les activités relatives à l'aéronautique restent cependant au sein du groupe Valmet, avant d'être séparées et intégrées dans Patria en 1996. L'entreprise abandonne alors ses capacités dans la construction d'avions d'entraînement et se focalise désormais sur la maintenance d'avions et d'hélicoptères ainsi que sur la fabrication de composants et sous-systèmes pour les grands constructeurs mondiaux. Il s'avère que « depuis 1922, l'entreprise a construit elle-même trente modèles d'avions, dont 19 de conception finlandaise »[5].

Les activités relatives aux véhicules militaires

Si la Finlande possède une petite industrie automobile focalisée sur la construction de camions et d'engins spécialisés qui se développe progressivement au début du XX^{ème} siècle, la décision de se doter d'une industrie dans le domaine des véhicules militaires remonte à la guerre de continuation face à l'Union soviétique à partir de l'été 1941. Du fait du besoin de véhicules de transport de troupes et des difficultés d'approvisionnement, « *la solution fut d'établir une entreprise dont les actionnaires seraient l'Etat de Finlande, le propriétaire du seul fabricant de véhicules [de l'époque] (Oy Suomen Autoteollisuus Ab), ainsi que diverses entreprises dominantes dans le secteur des métaux, et le seul fabricant de pneus du pays* »[6]. Baptisée Yhteisisu (Sisu, la marque sous laquelle sont commercialisés les véhicules, signifiant courage ou détermination en finnois), la nouvelle entreprise est localisée à Hämeenlinna, ville peu industrialisée mais bien desservie par les infrastructures de transport et située à cent kilomètres au Nord de la capitale. La naissance d'Yhteisisu en 1941 s'explique donc par la volonté de mettre en place une firme spécialement dédiée à la fabrication de véhicules militaires. Un contrat est passé avec l'armée finlandaise pour la livraison de camions et de bus, bien que la guerre se termine avant que la production n'ait réellement débuté.

Après une période d'interrogations sur la pertinence du maintien de l'activité, Yhteisisu ne reprend réellement sa production qu'en 1946. L'entreprise prend le nom de VAT (Vanajan Autotehdas Oy) en 1948 et ses véhicules sont alors commercialisés sous la marque Vanaja. Dépendant essentiellement des commandes publiques de l'Etat finlandais, VAT s'affirme peu à peu. Elle abandonne la seule production de véhicules militaires et institutionnels et diversifie ses activités vers le secteur privé finlandais puis, avec un succès limité, vers les marchés internationaux. Se faisant, elle entre en concurrence directe avec l'autre acteur finlandais du secteur, Suomen Autoteollisuus, en produisant des camions robustes, mais aussi des bus et tramways. Vanaja se tourne à nouveau vers la production de véhicules spécifiquement militaires dans les années 1960 avec la construction du camion Proto (abréviation de son surnom de 'prototype' durant la phase d'essais) baptisé KB-45 dans l'armée finlandaise. Construit en partenariat avec les forces armées, le premier prototype de ce camion à quatre roues motrices est réalisé en 1962.

Vanaja et Suomen Autoteollisuus fusionnent finalement en 1968, ce qui donne naissance à un acteur unique de l'industrie du poids lourd en Finlande. La nouvelle entité conserve le nom de l'entreprise principale, Suomen Autoteollisuus. Suite au décès de son fondateur en 1974, elle devient une entreprise publique.

En 1981, l'entreprise adopte le nom d'Oy Sisu-Auto Ab. C'est cette même année qu'est réalisé le premier prototype d'un véhicule blindé à six roues motrices, suite à un appel d'offres de l'armée finlandaise auquel participent deux entreprises : le constructeur d'engins agricoles « *Valmet avec son produit basé sur un tracteur et Sisu avec un véhicule basé sur la technologie du poids-lourd* »[7]. Sisu l'emporte avec un véhicule baptisé Pasi, abréviation de Panssari-Sisu ou Sisu blindé en finnois. Véhicule blindé de transport de troupes à six roues motrices, le Pasi ou XA-180 dans l'armée finlandaise est destiné à transporter dix fantassins avec leur équipement. Il s'avère rapidement approprié aux opérations de gestion de crise en-dehors du territoire national et connaît un grand succès à l'exportation : « *les premiers véhicules furent délivrés aux Nations Unies en août 1984, et vers la fin de cette même année, les livraisons ont débuté pour les Forces de Défense Finlandaises* »[8]. Dans les années 1980, Sisu produit également une nouvelle génération de

Programmes emblématiques de véhicules militaires finlandais

Le camion Proto ou KB-45 (à gauche) constitue l'une des premières réalisations modernes de l'industrie militaire finlandaise dans le secteur terrestre. Les camions sont utilisés pour transporter des troupes et des munitions, mais également pour remorquer des systèmes d'artillerie. Le véhicule Pasi ou XA-180 (à droite, en configuration maintien de la paix photographié en 1998) fait partie des rares véhicules, avec son successeur l'AMV, à avoir fait l'objet de ventes significatives à l'export. Initialement conçu pour les besoins de l'armée finlandaise, il s'est rapidement avéré adapté au besoin de transport de troupes sous blindage léger de nombreuses forces armées, en particulier dans le cadre d'opérations de maintien de la paix.
Source : Patria.

camion militaire, le Masi (abréviation de 'Maasto Sisu' signifiant Sisu tout terrain) baptisé SA-150. L'entreprise se tourne brièvement dans la production de véhicules à chenilles avec le Nasu. Il s'agit d'un véhicule léger destiné au transport de troupes et qui peut également servir comme plateforme d'arme lourde (de mortier de 120 mm notamment). Dans les années 1990, l'entreprise produit également un véhicule de déminage pour l'armée finlandaise, le RA-140 DS, exporté en petite quantité. A l'exception de quelques projets à l'exportation, la grande majorité des véhicules construits par Vanaja puis Sisu Auto ont été uniquement produits pour les forces armées nationales. Seuls le XA-180 et ses versions ultérieures ont fait l'objet de livraisons internationales à plus grande échelle[9].

En 1994, Sisu est dans un premier temps intégrée au sein du conglomérat public Valmet, avant que sa branche véhicules blindés ne soit finalement consolidée dans une nouvelle entité, Patria, à la fin de l'année 1996. Les activités de fabrication de camions restent cependant indépendantes, dans le cadre de l'entreprise Sisu Auto Oy, qui reste impliquée dans la construction de camions militaires à 4, 6, 8 et 10 roues motrices via sa filiale Sisu défense. Forte du succès du XA-180, Patria conçoit à la fin des années 1990 un véhicule plus avancé, l'*Armoured Modular Vehicle* (AMV) à six et huit roues motrices, ce qui lui permet d'être doté d'un armement plus lourd et d'un blindage plus important. Alors que le premier prototype est dévoilé en juin 2000, le véhicule remporte également des succès importants à l'exportation avec près de 1 600 véhicules aujourd'hui commandés par huit pays.

Les activités relatives aux armes lourdes

Deux entreprises finlandaises sont historiquement présentes dans le domaine des armes lourdes, Tampella Oy, spécialisée dans les mortiers, et Vammaskosken Tehdas Oy qui intervient dans le domaine de l'artillerie et des munitions. Créée dans les années 1930 à Tampere, Tampella est une entreprise industrielle qui intervient dans la construction de machines outils, de locomotives, mais également dans le secteur forestier. Elle devient surtout active dans le secteur militaire en construisant des mortiers dans les années 1940 : « *lors de la Seconde Guerre mondiale, l'armée de terre finlandaise avait grandement besoin de mortiers lourds de 120 mm afin de compenser son manque d'artillerie. Comparés à l'artillerie, les mortiers étaient également mieux adaptés aux combats finlandais en terrains forestiers* »[10]. Le prototype d'un mortier lourd de 120 mm (le 120 Krh/40) est ainsi testé juste avant la guerre d'hiver et produit en série durant la guerre de continuation face à l'Union soviétique.
Pour ce qui est de la seconde entreprise, son histoire « *remonte à la Seconde Guerre mondiale, lorsque les premières armes étaient réparées à Vammala. A cette époque, le dépôt de l'armée finlandaise effectuait ce travail mais peu de temps après la guerre, l'entreprise Vammaskosken Tehdas fut établie* »[11]. Elle se spécialise alors dans la fabrication de canons d'artillerie et de munitions de gros calibre.

Les deux entreprises poursuivent leurs activités séparément jusqu'à ce qu'en 1991, les branches défense de Tampella Oy et Vammaskosken Tehdas Oy fusionnent pour former une nouvelle

Programmes emblématiques de l'industrie finlandaise dans le domaine des armes lourdes

Système d'artillerie de 155 millimètres (155 GH APU) et système de mortier à double canon AMOS (monté sur le châssis d'un véhicule AMV). Exporté en Egypte dans le cadre d'une production locale sous licence, le 155 GH APU constitue le dernier système d'artillerie conçu par Patria faute de commandes nationales par la suite. Issu d'un projet de partenariat entre le Danemark, la Finlande, la Norvège et la Suède, le mortier à double canon AMOS (*Advanced MOrtar System*) est quant à lui conçu dans le cadre de la coentreprise finno-suédoise Patria-Hägglunds suite au retrait du Danemark et de la Norvège du programme.
Source : Army Guide/Patria

entité, Vammas Oy. Dans les années 1990, Vammas développe en particulier un canon d'artillerie de 155 mm, le 155 GH 52 APU remorqué par un véhicule. Alors que l'entreprise est intégrée dans Patria à la fin de l'année 1996, elle obtient en 1998 un contrat pour la livraison de 27 canons d'artillerie 155 GH 52 APU pour l'armée finlandaise. Le système est par la suite exporté en Egypte en 1999 dans le cadre d'un accord de production locale sous licence[12]. En 2000 cependant, l'armée finlandaise annule un programme de système d'artillerie automoteur auprès de Patria. Faute de financement, cette décision condamne les activités de l'entreprise dans le domaine de l'artillerie. Patria se recentre alors sur les seuls systèmes de mortiers à tourelles de 120 mm pour véhicules militaires.

Ces éléments permettent de constater que l'industrie finlandaise de défense, pratiquement inexistante à l'indépendance du pays en 1917, se développe dans l'urgence de la guerre d'hiver face à l'Union soviétique en mêlant conjointement volonté étatique et initiative privée. La base industrielle est alors fortement fragmentée, y compris dans certains secteurs : l'industrie des armées lourdes, mortiers et artillerie, compte ainsi deux producteurs jusqu'en 1991. Elle est, tout au long de la guerre froide, essentiellement tournée vers le client national. Les exportations sont en effet peu nombreuses et, à l'exception de quelques succès comme les véhicules militaires Pasi, la production vise uniquement à satisfaire les besoins de l'armée nationale.

Une première tentative de consolidation a lieu avec le regroupement progressif d'activités militaires au sein du conglomérat industriel civil et militaire Valmet, jusqu'à ce que la plupart des industries de l'aéronautique et de la défense soient finalement consolidées au sein d'une nouvelle entité, Patria, au sortir de la guerre froide. Cette évolution a lieu dans un contexte de fortes restructurations capacitaires puisque plusieurs activités sont définitivement abandonnées, en particulier la construction d'avions d'entraînement et de systèmes d'artillerie. Elle implique cependant une mutation profonde de l'industrie, par la recherche désormais constante de partenariats internationaux.

La consolidation en deux entités, Patria et Nammo, et la recherche constante de partenariats internationaux

Après avoir étudié l'évolution historique des industries militaires finlandaises, cette seconde partie s'intéresse plus spécifiquement aux mutations post-guerre froide. Elle porte donc sur les principales entreprises actuelles, sur leur évolution récente et sur les liens capitalistiques entrecroisés qu'elles entretiennent. L'étude s'y focalise sur la création et l'évolution de la principale entreprise de défense du pays, Patria (A), sur le munitionnaire Nammo, issu d'une consolidation capitalistique entre la Norvège, la Suède et la Finlande (B), puis sur l'alliance stratégique récente formée entre Patria et la firme norvégienne Kongsberg (C).

Patria : une entreprise majoritairement publique en quête de partenaires internationaux

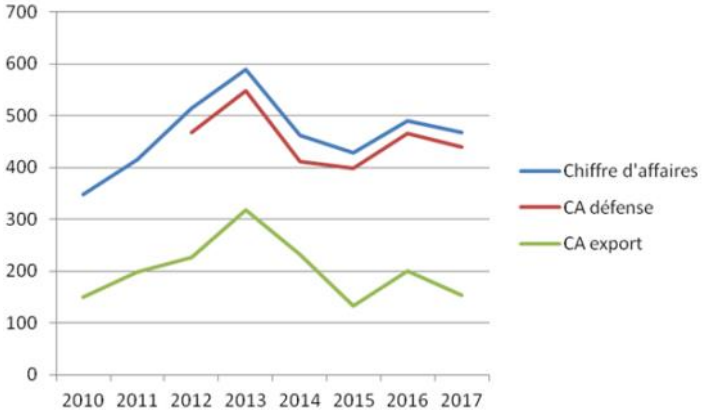
Patria est aujourd'hui la principale entreprise de défense de Finlande et malgré plusieurs évolutions de la structure de son capital, elle reste détenue à une faible majorité par le gouvernement finlandais (50,1%). Dans ce cadre, « *le Ministère de la défense est chargé de la détermination des objectifs stratégiques pour l'actionnaire principal. L'entreprise joue un rôle important dans la sécurité des approvisionnements de la Finlande, et plusieurs de ses divisions sont essentielles pour la défense nationale en temps de crise* »[13]. Son chiffre d'affaires est essentiellement militaire. En légère diminution du fait de la tendance à la contraction des débouchés export, il se situe autour de 500 millions d'euros.

L'origine de l'entreprise remonte à la fin des années 1990. Dans le contexte de la consolidation du secteur de la défense observé au même moment dans d'autres pays européens, cinq entreprises finlandaises de défense et de l'aérospatial sont regroupées au 1er octobre 1996 au sein d'une nouvelle entité, Suomen Puolustusväline (ou « Equipements finlandais de défense »). Il s'agit de :

- Vammas (artillerie, mortiers et munitions de gros calibre)
- Lapua (munitions de petit calibre)
- Sisu Defence (véhicules blindés)
- Vihtavuori (explosifs)
- Finavitec (aérospatial)

La nouvelle entreprise regroupe donc la grande majorité des activités aéronautiques et militaires de Finlande. Elle débute ses opérations en janvier 1997 avant d'être rebaptisée Patria. Initialement détenue à 100% par l'Etat finlandais, son organisation est celle d'une holding, chapeautant les cinq entreprises qui conservent une autonomie. La maison-mère, Patria Industries Oyj, détient les entreprises du groupe à 100% ainsi qu'un certain nombre de filiales et coentreprises. Quelques années après la création de la nouvelle entité, le Ministère du commerce et de l'industrie annonce ouvrir un processus pour trouver un ou plusieurs partenaires et propriétaires stratégiques pour Patria. Alors qu'Airbus (à l'époque EADS) et BAE Systems (alors actionnaire de la firme suédoise de la défense et de l'aérospatial Saab à hauteur de 35%) font part de leur intérêt, c'est EADS qui l'emporte avec la signature d'un accord en janvier 2001 portant acquisition de 26,8% du capital, le gouvernement finlandais conservant les 73,2% restants[14]. Les motivations semblent alors principalement liées aux activités aérospatiales de Patria : pour l'avionneur européen EADS nouvellement créé, il s'agit en effet de

Evolution du chiffre d'affaires de Patria, 2010-2017, millions d'€ courants



Source : rapports annuels (données antérieures non disponibles)

faire entrer un Etat supplémentaire dans l'organisation du groupe, en particulier dans le contexte de la compétition pour un programme d'hélicoptères commun aux pays nordiques, le NSHP (*Nordic Standard Helicopter Program*), par la suite remportée par l'hélicoptère NH90 proposé par EADS. Ainsi, « *pour les pays scandinaves, le geste politique de l'opération NSHP […] a une dimension industrielle. La Finlande, qui entend conserver une industrie de défense indépendante, a choisi d'adosser Patria à EADS, qui propose, dans le cadre de la compétition NSHP, le nouvel hélicoptère de transport NH90 d'Eurocopter. Sans être directement impliquées dans une offre concurrente, BAE Systems et Saab étaient, selon certains, sensiblement plus proches des hélicoptéristes Westland ou Sikorsky […]. Par ailleurs, la perspective de glaner de la charge sur l'A380 d'Airbus aurait constitué un argument de poids en faveur d'EADS* »[15].

Le début des années 2000 est une période florissante pour Patria. L'année 2003 constitue à ce titre un tournant important avec la vente de 690 véhicules blindés de type AMV à la Pologne, qui marque la première exportation de la nouvelle génération de véhicules militaires construits par Patria, mais surtout la première exportation majeure de l'entreprise depuis sa création en 1996. L'année 2005 marque ensuite la montée de Patria au sein du groupe Nammo (cf. *infra*), de 27,5 à 50% du capital, à parité avec le gouvernement norvégien. Les bons résultats de l'entreprise nordique de munitions ont un impact immédiat sur les résultats de Patria. Alors que l'entreprise obtient d'autres succès internationaux pour son véhicule AMV, elle se trouve cependant impactée par les difficultés que traverse EADS à partir de 2007. A partir de 2008, Patria est confrontée à de forts soupçons de corruption. En juin 2008, quatre employés du groupe ayant joué un rôle dans le cadre de la vente de canons d'artillerie à l'Egypte entre 1997 et 2004 sont arrêtés par la police finlandaise. Les allégations portent également sur la vente de 136 véhicules AMV à la Slovénie en 2006, ce qui engendre des tensions diplomatiques entre la Slovénie et la Finlande et conduit finalement à l'annulation du contrat à l'exception des 30 véhicules déjà livrés[16]. Dans le même temps, Patria fait face à des accusations de corruption dans sa tentative de commercialiser le mortier Nemo auprès de la République tchèque[17]. Toutes ces allégations, ainsi que les longues procédures judiciaires qui s'ensuivent, affaiblissent l'image de l'entreprise.

Comme un grand nombre de firmes du secteur de la défense, Patria est également confrontée à des difficultés consécutives à la chute des budgets militaires européens suite à la crise de 2008. Dès 2009, son nouveau président directeur général relève que « *les ministères de la défense qui sont nos clients les plus importants avaient établi leurs budgets avant la crise financière, d'où un marché assez bon. Dans un grand nombre des pays importants que nous avions ciblés cependant, l'évolution économique a rapidement conduit à freiner brutalement. Tout compte fait, la récession a eu pour conséquence des changements significatifs dans les calendriers de livraison mais a aussi retardé la date d'entrée en vigueur de nouveaux projets, qui sont toujours dans la phase de soumission, dans tous les domaines* »[18].

Après avoir échoué dans sa tentative de fusion avec BAE Systems à l'automne 2012, EADS réévalue en profondeur sa stratégie dans le secteur de la défense. Rebaptisée Airbus, elle vend à la fin de l'année 2014 sa participation dans Patria à l'Etat finlandais qui détient de nouveau la totalité du capital de l'entreprise. Cette situation est cependant présentée comme temporaire, l'objectif affiché par le gouvernement étant de trouver un partenaire stratégique sous la forme d'une firme étrangère présente de façon minoritaire et durable au sein du capital de Patria.

Nammo, entreprise transnationale intégrée entre la Norvège, la Suède et la Finlande

Nammo AS est une entreprise créée en 1998 dans le cadre d'une consolidation transnationale des activités relatives aux explosifs et aux munitions entre les firmes norvégienne Raufoss, suédoise Celsius et finlandaise Patria. Détenue à 50% par le gouvernement norvégien et à 50% par Patria depuis le retrait de la Suède du capital de l'entreprise en 2006, son siège social se situe dans la ville de Raufoss en Norvège. Elle constitue donc la seule entreprise transnationale de défense des pays nordiques et figure, aux côtés de groupes beaucoup plus importants comme Airbus et MBDA, parmi les rares entreprises de défense européennes aux activités intégrées entre plusieurs Etats.

La création d'une entreprise de fabrication de munitions en Finlande remonte à 1923 dans la ville de Lapua. Il s'agit d'une entreprise publique, qui le reste jusqu'en 1991. A cette date, elle est privatisée et prend la forme d'une société à responsabilité limitée. Depuis les années 1980, elle diversifie par ailleurs ses activités dans le secteur civil en produisant des munitions pour la chasse et le tir sportif[19].

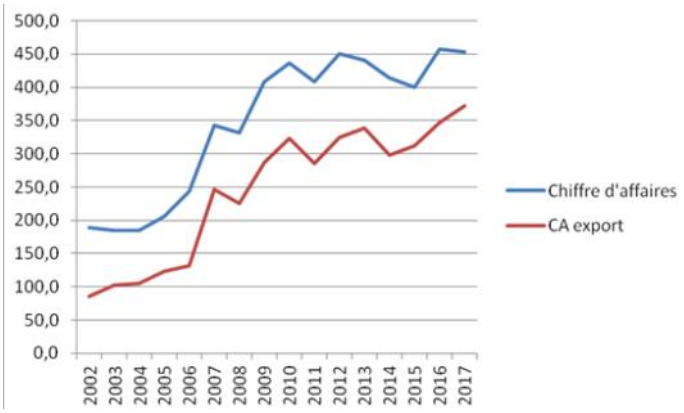
Lapua fait partie des cinq entreprises finlandaises rassemblées à la fin de l'année 1996 en une nouvelle entité, Patria. Elle ne reste cependant qu'une année et demie au sein de Patria. Le groupe Nammo est en effet créé en septembre 1998 sous la forme d'une holding rassemblant les activités relatives aux munitions de trois entreprises préexistantes dans les pays scandinaves qui deviennent des filiales à 100% : Nammo Raufoss (Norvège), Nammo Liab (Suède) et Nammo Lapua (Finlande). L'actionnariat de la nouvelle entité est alors réparti entre Raufoss (Norvège, 45%), Celsius (Suède, 27,5%) et Patria (Finlande, 27,5%).

Alors que Raufoss cherche au début des années 2000 à se recentrer sur ses activités civiles, l'Etat norvégien fait l'acquisition des 45% que détient l'entreprise au sein de Nammo[20]. Le groupe suédois Celsius est racheté cette même année par son compatriote Saab, sans que cela change l'actionnariat de Nammo. Un protocole d'accord (*memorandum of understanding*) est signé en 2001 entre les gouvernements norvégien, suédois et finlandais pour renforcer leur coopération dans le domaine des munitions[21]. Par la suite, le groupe allemand Rheinmetall fait part en 2005 de son intérêt pour une prise de participation significative au sein du capital de Nammo, qui reste cependant sans suite. L'entreprise entreprend progressivement une stratégie d'expansion internationale, ouvrant des sites de production ou en procédant à des acquisitions en Allemagne et aux Etats-Unis.

A la fin de l'année 2005, le groupe suédois Saab qui fait face à des difficultés et à une diminution des dépenses militaires suédoises annonce son intention de se retirer de l'actionnariat de Nammo de façon à rationnaliser son organisation et à se focaliser sur ses propres opérations. Ses parts sont alors vendues au gouvernement norvégien (5%) et à Patria (22,5%). Nammo est dès lors une coentreprise détenue à parité par le gouvernement norvégien et par Patria[22].

Au niveau de ses domaines d'intervention, Nammo « *conçoit, produit et vend des munitions à usage militaire et* civil,

Evolution du chiffre d'affaires de Nammo, 2002-2017, millions d'€ courants



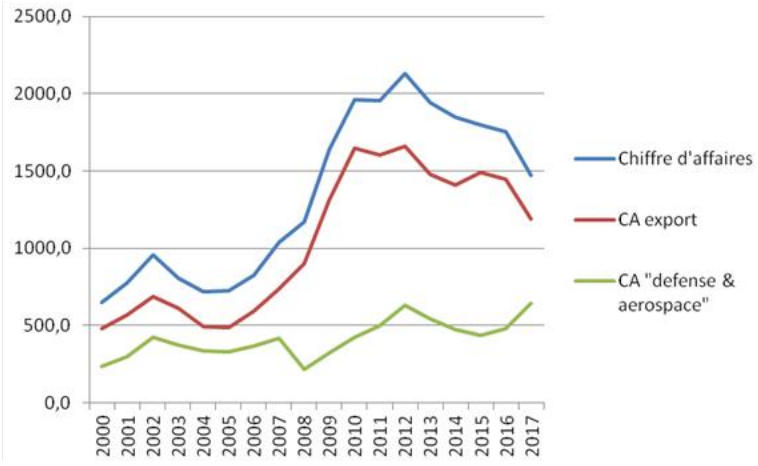
Source : rapports annuels

des systèmes d'armes à épaules, des moteurs de fusées pour applications spatiales et militaires, et constitue l'un des principaux fournisseurs de services de démilitarisation conformes aux règles environnementales »[23]. Son chiffre d'affaires oscille entre 400 et 450 millions d'euros en fin de période dans le graphique ci-après, ce qui en fait une entreprise de taille comparable à Patria. Bien que Nammo ne communique pas le montant de son chiffre d'affaires défense, ses activités civiles sont cependant très restreintes lorsque rapportées à l'ensemble. On constate par ailleurs que l'entreprise est fortement exportatrice (sont considérés comme marchés export les zones géographiques autres que les trois Etats fondateurs : Norvège, Suède et Finlande).

Le rapprochement Patria - Kongsberg

En mars 2016, la division militaire de l'entreprise norvégienne de défense et d'ingénierie Kongsberg annonce son intention de faire l'acquisition de 49,9% du capital de Patria, le gouvernement finlandais restant l'actionnaire majoritaire à hauteur de 50,1%. Créée au début du XIX^{ème} siècle, Kongsberg est détenue à 50% par le gouvernement norvégien, les autres 50% étant cotés à la bourse d'Oslo. Ce mouvement constitue donc une alliance stratégique, et non une fusion puisque les deux entreprises poursuivent leur existence comme deux entités distinctes. La coopération industrielle existante entre la Norvège et la Finlande s'en trouve renforcée, d'autant que le fabriquant de munitions, de poudres propulsives, et d'explosifs Nammo est lui-même détenu depuis 2005 à 50% par le gouvernement norvégien et 50% par Patria.

Evolution du chiffre d'affaires de Kongsberg, 2000-2017, millions d'€ courants



Source : rapports annuels

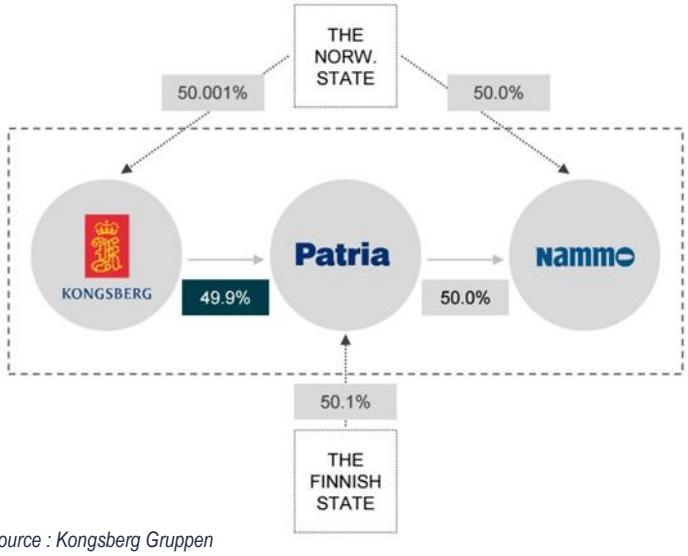
Kongsberg est une entreprise majoritairement civile dont le chiffre d'affaires est largement supérieur à celui de Patria, de l'ordre d'1,5 milliard d'euros en 2017. Sa diminution très marquée entre 2012 et 2017 dans le graphique ci-après doit être relativisée car elle est fortement amplifiée par les fluctuations du taux de change entre l'euro et la couronne norvégienne. Malgré cette différence de taille, le chiffre d'affaires défense de Kongsberg est relativement proche de celui de Patria, autour de 500 millions d'euros. On constate également que le groupe Kongsberg est fortement dépendant des ventes à l'exportation.

Ce rapprochement contribue donc à renforcer la coopération entre pays nordiques dans le domaine de l'industrie de la défense. Ensemble, les deux entreprises représentent ainsi le deuxième groupe nordique dans le domaine de la défense en chiffre d'affaires, derrière la firme suédoise Saab. La nouvelle entité dispose ainsi de compétences très larges, à la fois civiles et militaires : véhicules blindés, systèmes d'armes pour véhicules, aérostructures, maintenance de moteurs d'avions et d'hélicoptères, assemblage d'avions et d'hélicoptères, systèmes navals… Dans ce contexte, « *l'objectif principal de l'activité en cours de fusion et d'acquisition est de renforcer l'avantage concurrentiel afin de remporter de grands contrats nationaux et régionaux face à une présence et des offres accrues en provenance de rivaux 'étrangers'* »[24]. Alors que le groupe Kongsberg affiche ouvertement qu'un des éléments clés de la stratégie de marché de sa division aéronautique et défense est la formation d'alliances avec des entreprises de défense internationales, le rapprochement avec le Finlandais Patria « *a pour ambition de créer un ensemble complémentaire dont chaque élément pourra mieux rivaliser en Europe du Nord et au-delà* »[25].

Ces éléments permettent de constater que la consolidation des industries finlandaises de la défense suite à la fin de la guerre froide s'est effectuée en trois temps.

Tout d'abord (1996-1997), la majorité des entreprises de la défense et de l'aéronautique du pays sont consolidées en une entité unique détenue par l'Etat, Patria. Une telle évolution revient à assembler des activités industrielles certes disparates, mais elle permet d'obtenir une certaine taille

Représentation des participations croisées



Source : Kongsberg Gruppen

critique dans le cadre d'activités toutes fortement liées à l'Etat.

Dans un second temps (1998-2001), le gouvernement finlandais cherche activement des partenaires internationaux sous la forme de partenaires stratégiques, de façon à pérenniser une industrie stratégique confrontée à la fois la chute du budget de la défense d'un Etat de quelques cinq millions d'habitants ainsi qu'à une internationalisation croissante du secteur. Ces partenariats se manifestent par des liens capitalistiques et industriels : Nammo est issue de la consolidation des activités de fabrication de munitions de la Norvège, de la Suède et de la Finlande, et l'actionnariat est au départ réparti entre les trois Etats. Quant à Patria, la présence d'EADS à hauteur de 26,8% de son capital lui donne accès à une visibilité européenne et mondiale.

Plus que le retrait de la Suède du capital de Nammo en 2006, c'est surtout la décision d'EADS (devenu Airbus) de se retirer du capital de Patria dans le cadre d'une vaste réorganisation interne en 2014 qui marque la troisième phase : après une période d'incertitude marquée par une reprise de l'intégralité du capital par le gouvernement finlandais, un partenariat stratégique est trouvé avec le groupe norvégien Kongsberg en 2016, ce qui renforce une coopération industrielle militaire existante entre les deux Etats.

Conclusion

Cet article a étudié la mise en place de partenariats capitalistiques et industriels croisés entre la Norvège et la Finlande en les replaçant dans le temps long, à travers l'étude des mutations de l'industrie finlandaise de la défense depuis les années 1920. Il a mis en évidence la succession de deux grandes périodes qui correspondent à deux modes de régulation différents du secteur.

Des années 1920 jusqu'à la fin de la guerre froide, la Finlande se dote progressivement d'une industrie militaire dans le cadre d'initiatives publiques comme privées, via un vaste soutien gouvernemental. La guerre d'hiver, la guerre de continuation (Seconde Guerre mondiale) et la guerre froide voient alors se développer un système national de production d'armement. Ce système est avant tout tourné vers le client national, avec plusieurs productions au niveau de plateformes (avions d'entraînement, véhicules, systèmes d'artillerie…) et des exportations restreintes. Une première consolidation a lieu durant cette période avec le regroupement d'une partie des industries aéronautiques et de défense au sein d'un vaste conglomérat industriel civilo-militaire : Valmet.

La fin de la guerre froide ouvre cependant la voie à un processus d'internationalisation, de recherche accrue de débouchés export et de redimensionnement capacitaire. Alors que la totalité des entreprises de l'aéronautique et de la défense sont consolidées en une entreprise unique détenue par l'Etat, Patria, certains programmes ambitieux (avions d'entraînement, systèmes d'artillerie) sont remis en cause. Toujours avec un soutien gouvernemental actif, la recherche de partenariats internationaux passe alors par deux éléments : l'intégration transnationale des activités relatives à la fabrication de munitions entre la Norvège, la Suède et la Finlande (Nammo) et l'entrée de l'avionneur européen EADS au sein du capital de Patria à hauteur de 26,8%. La décision d'EADS, devenu Airbus, de se retirer du capital de Patria en 2014 implique alors une reprise temporaire de la totalité du capital de l'entreprise par la puissance publique, qui cherche activement un nouveau partenaire international. En 2016, le groupe norvégien Kongsberg fait l'acquisition de 49,9% du capital de Patria : cette alliance stratégique entre deux firmes aux activités défense complémentaires inaugure alors le basculement d'une recherche d'ouverture internationale en s'adossant à un grand acteur du secteur vers une coopération régionale renforcée et pragmatique, de façon à faire face à une concurrence accrue sur les marchés nationaux comme internationaux.

ADRIEN CARALP
Docteur en économie de l'EHESS,
diplômé de l'IEP d'Aix-en-Provence
adrien.caralp@ehess.fr

Notes

1.Alfred CHANDLER, *Strategy and Structure. Chapters in the history of the American industrial enterprise,* Beard Books, 1962, 480 p. ; Patrick FRIDENSON, Pascal GRISET, *Entreprises de hautes technologies. Etat et souveraineté depuis 1945*, IGPDE, 2013, 300 p.

2.Patria, *Annual Report 2011*, Helsinki, p.8.

3.Valmet, « History », http://www.valmet.com/about-us/valmet-in-brief/history/.

4.Patria, *Annual Report 2011*, *op. cit.*, p.12.

5.Global Security, « Finavitec », http://www.globalsecurity.org/military/world/europe/finavitec.htm.

6.Santos HEINI, « The road to Patria », *Patria Focus*, 2011, n° 2, p. 17-21, p.18.

7.Pävi BRINK, « XA-vehicle, a.k.a. Pasi, well-known from the field », *Patria Focus*, 2010, n° 2, p.22.

8.« History of the XA-series armoured wheeled vehicle, "Pasi", at home and abroad », *Patria Focus*, 2005, n° 3, p.14.

9.« Patria - the Finnish military vehicle supplier of the cutting edge », *Patria Focus*, 2004, n° 2, p.8.
10.Terhi PALMU, « 120 Krh/40 », *Patria Focus*, 2010, n° 1, p.22.
11.« Focus: weapon systems », *Patria Focus*, 2004, n° 3, p.5.
12.Christopher FOSS, « Finland builds up artillery capability », *Jane's Defence Weekly*, 20 juin 2001.
13.Global Security, « Patria Group », http://www.globalsecurity.org/military/world/europe/patria.htm
14.Jean-Pierre NEU, « EADS avance un pion en Scandinavie », *Les Echos*, 7 février 2001.
15.*Ibid.*
16.Agence France Presse, « Slovenia to go forward with Finland defense deal », *Defense News*, 5 septembre 2008.
17.Jiri KOMINEK, « Patria publishes findings on alleged Czech corruption », *Jane's Defence Weekly*, 7 octobre 2010.
18.Patria, *Annual Review 2009*, Helsinki, p.5.
19.Lapua, « History », http://www.lapua.com/en/lapua/history-of-lapua.html .
20.John BERG, « Raufoss share in Nammo for sale », *Jane's Defence Weekly*, 26 janvier 2000.
21. Nammo, *Annual Report 2008*, Raufoss, 71 p., p.4.
22.Guy ANDERSON, « Patria increases stake in Nammo », *Jane's Defence Industry*, 1er mars 2006.
23.Nammo, *Annual Report 2013*, Raufoss, 2013, p.3.
24.G. O'DWYER, « Industry consolidates as Nordic states unify on defense », *Defense News*, 11 novembre 2016
25.https://www.ttu.fr/kongsberg-rachete-499-de-patria/

Le Traité d'interdiction des armes nucléaires : vers une remise en cause des doctrines nucléaires ?

Des citoyens, scientifiques ou diplomates militent depuis l'invention des armes nucléaires pour leur interdiction et destruction, à l'instar d'autres armes considérées comme moralement répréhensibles, telles que les armes chimiques ou les armes biologiques. Ce mouvement ancien a connu un succès historique le 7 juin 2017. 122 Etats rassemblés à New York ont en effet voté en faveur d'un texte interdisant les armes nucléaires. Ce texte entrera en vigueur lorsque 50 Etats l'auront ratifié, une perspective réaliste courant 2019[1]. Cette nouvelle norme signale le rejet clair des armes nucléaires par une partie importante de la communauté internationale, même si elle est loin de faire l'unanimité, y compris parmi les Etats qui ne disposent pas de capacités nucléaires.

Dans quelle mesure impactera-t-elle les doctrines, stratégies, arsenaux des Etats qui font confiance à la dissuasion nucléaire pour assurer leur sécurité ? Beaucoup d'inconnues planent naturellement sur l'avenir de ce Traité. Pour autant, il est d'ores et déjà possible d'anticiper à court terme ses potentiels effets. Au niveau politique, des pressions pour l'instant très modestes sont exercées en faveur du désarmement dans les pays dotés. En matière de sécurité, des coopérations militaires pourraient être remises en cause pour les pays signataires, et pour ce qui est des industries, des campagnes de désinvestissement pourraient être organisées dans le cadre de ce nouvel outil juridiquement contraignant.

Un mouvement en réaction aux difficultés du désarmement étape par étape

En raison de leurs effets destructeurs potentiellement planétaires, et du fait qu'elles ne sont légalement possédées que par un petit groupe d'Etats, les armes nucléaires ont toujours fait l'objet de mouvements politiques et populaires en faveur de leur abolition voire de leur interdiction. Dès l'adoption du Traité de Non-prolifération (TNP), il est fait état dans l'Article VI d'une obligation pour les cinq puissances nucléaires reconnues de « *poursuivre de bonne foi des négociations sur des mesures efficaces relatives à la cessation de la course aux armements nucléaires à une date rapprochée et au désarmement nucléaire et sur un traité de désarmement général et complet sous un contrôle international strict et efficace* ». La mise en place de cette obligation a été réalisée de manière inégale. Dans le contexte de la fin de la guerre froide, des réductions majeures ont été observées, notamment aux Etats-Unis et en Russie, permettant de passer d'environ 70 000 têtes nucléaires au cœur de l'affrontement Est/Ouest à environ 14 900 aujourd'hui[2]. En France, des réductions unilatérales ont permis de passer de 540 têtes à moins de 300, mais aussi de faire disparaître la composante terrestre, de renoncer aux essais nucléaires de manière irréversible et d'arrêter la production de matières fissiles[3].

Des progrès en matière de désarmement ont donc été réalisés au niveau unilatéral, bilatéral mais aussi multilatéral avec l'adoption d'un traité d'interdiction des essais nucléaires (TICE), selon une logique graduelle. Ce processus, connu sous le nom de « désarmement par étapes », a été validé par l'ensemble des membres du Traité de non-prolifération lors des conférences d'examen de 2000 et de 2010, avec l'adoption consensuelle de plans d'actions en faveur du désarmement.

Néanmoins, il connaît des difficultés depuis cette date et est de plus en plus contesté. En effet, les réductions au sein des arsenaux nucléaires mondiaux se ralentissent. Certaines initiatives multilatérales ne tiennent pas leurs promesses[4]. Les démarches bilatérales sont considérablement freinées par un renouveau des tensions nucléaires, en particulier entre l'OTAN et la Russie, et la remise en cause d'un certain nombre d'accords de maîtrise des armements. Certains acteurs, Etats et ONG, amplifient leurs critiques des Etats nucléaires, estimant que leurs efforts en matière de désarmement sont insuffisants et que l'Article VI du TNP n'est pas respecté. C'est dans ce contexte qu'un mouvement en faveur d'une nouvelle norme juridiquement contraignante a émergé dans les années récentes.

5 grandes dates ayant conduit à l'adoption du Traité d'interdiction des armes nucléaires (TIAN)

- Décembre 2014 : au terme de trois conférences internationales, l'Autriche s'engage à promouvoir un instrument juridiquement contraignant d'interdiction des armes nucléaires.
- Août 2016 : un groupe de travail créé par l'Assemblée générale des Nations Unies recommande l'adoption d'un instrument contraignant interdisant les armes nucléaires.
- Octobre 2016 : le Premier Comité des Nations Unies autorise la formation d'une convention pour négocier un Traité d'interdiction des armes.
- Mars 2017 : Premier cycle de négociations à l'ONU.
- 7 juillet 2017 : adoption du Traité à l'ONU à New York par 122 Etats.

Un partenariat entre quelques Etats moteurs et la société civile

Devant le ralentissement des réductions d'arsenaux, les blocages observés autour du désarmement multilatéral et la persistance des crises de prolifération, une contestation de plus en plus forte se cristallise autour de l'ordre nucléaire hérité de la guerre froide. Cette opposition, alimentée par une volonté de rompre avec la domination des puissances nucléaires du Nord, est menée par les pays non-alignés (NAM), mais aussi certains Etats traditionnellement opposés aux armes nucléaires tels que la Nouvelle-Zélande, le Mexique, certains pays scandinaves ou encore l'Autriche. Elle est amplifiée par un renouvellement du discours des ONG abolitionnistes. Celles-ci refusent de considérer les armes nucléaires sous un angle sécuritaire pour privilégier une approche basée sur le droit humanitaire. Cette stratégie bénéficie des retours d'expérience de plusieurs campagnes réussies, ayant permis l'adoption de la Convention d'interdiction des armes à sous-munition et la Convention d'Ottawa sur les mines antipersonnel.

L'action combinée de quelques Etats et des ONG a permis l'organisation de trois conférences à Oslo (mars 2013), Nayarit (février 2014) et Vienne (décembre 2014). Si l'objectif de ces trois conférences était d'évoquer l'impact humanitaire des armes nucléaires de manière ouverte, les débats ont largement porté sur la perspective d'une convention d'interdiction. A l'issue de la dernière session, le gouvernement autrichien a publié un engagement formel à « combler le vide juridique » concernant la prohibition et l'élimination des armes nucléaires[5]. Lors de la conférence d'examen du TNP de 2015, les Etats membres se sont opposés sur la question du désarmement, et en particulier sur l'importance de ce nouveau mouvement sur « les conséquences humanitaires ». Devant son échec, un groupe de travail a été créé à l'ONU pour « avancer sur les négociations de désarmement nucléaire multilatéral ». En août 2016, ce groupe a recommandé l'ouverture de négociations sur l'adoption d'une norme juridiquement contraignante[6], une recommandation validée par la Première commission des Nations Unies en octobre 2017 puis par l'Assemblée Générale le 23 décembre 2017[7].

Deux sessions de négociations ont ensuite été tenues à New York dans le cadre des Nations Unies, tout d'abord du 27 au 31 mars 2017 puis du 15 juin au 7 juillet 2017, permettant d'aboutir à l'adoption d'un texte définitif le 7 juillet de la même année. Plusieurs Etats ont été particulièrement moteurs pour soutenir les démarches diplomatiques : l'Autriche, où s'était tenue la dernière conférence humanitaire, le Mexique, l'Afrique du Sud, la Nouvelle Zélande, le Brésil… Ils ont été appuyés par des ONG très actives pour promouvoir leur version du Traité, et en particulier l'ICAN, collectif monté dans l'objectif justement d'aboutir à une norme d'interdiction.

Un traité a minima qui insiste sur un objectif politique plus que sur des considérations techniques

Les Etats qui se sont retrouvés à New York en mars 2016 avaient une idée commune : adopter une norme juridiquement contraignante interdisant les armes nucléaires[8]. Néanmoins, ils avaient des visions assez divergentes du texte à atteindre, et des modalités essentielles telles que les activités prohibées et les mesures de vérification exigées[9]. Sous l'impulsion de la Présidente costaricaine Elayne Whyne-Gomez, des Etats les plus investis et des ONG, il a finalement été décidé de privilégier un instrument simple, aussi consensuel que possible, et rapide à négocier pour permettre son adoption en 2017. Les diplomates ne souhaitaient en effet pas revenir à l'Assemblée générale à la fin de l'année pour réclamer un nouveau mandat de négociation, et craignaient que la visibilité médiatique de l'initiative ne soit diluée par un processus de rédaction trop long[10].

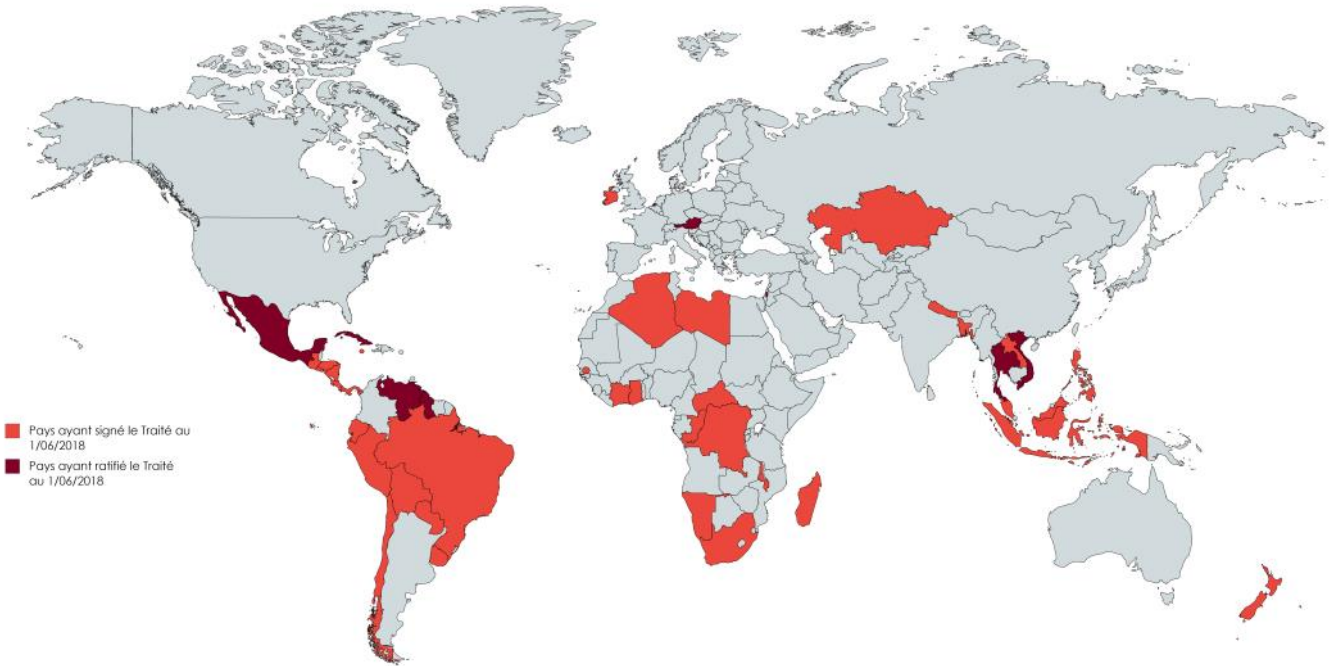
En termes de contenu, le Traité d'interdiction des Armes nucléaires (TIAN) prohibe entre autres la fabrication, la possession, l'emploi ou le transfert des armes nucléaires. Il interdit également d'aider un Etat à conduire ces activités. Deux processus sont ouverts pour rejoindre le Traité. Pour les Etats non-dotés, la signature et la ratification peuvent être immédiates à condition d'adopter des accords de garantie généralisés avec l'Agence internationale de l'Energie Atomique (AIEA). Les possesseurs actuels d'armes nucléaires peuvent rejoindre le Traité tout en lançant l'élimination de leurs armes avec l'aide d'une « autorité internationale compétente », dont la nature n'est pas spécifiée, ou d'un autre Etat. Ils peuvent également éliminer préalablement leurs armes en interne avant la ratification du Traité. Les négociateurs ont prévu des conventions des Etats parties pour affiner les procédures à mettre en place dans ces deux cas de figure, qui restent aujourd'hui très floues. Par ailleurs, ils ont renoncé à intégrer des mesures concrètes de vérification à l'intérieur du Traité : s'accorder sur de telles mesures aurait été très long et complexe, et aurait potentiellement rendu impossible l'adoption d'un texte dans les délais prévus.

Le texte intègre également une obligation d'assistance aux victimes et de réparations environnementales, signe de son inscription dans le cadre du droit humanitaire. Au niveau formel, il ne met pas en place une nouvelle organisation internationale, se contentant de prévoir des réunions bisannuelles sur les conditions de mise en œuvre ainsi que des conférences d'examen tous les six ans.

La version du texte publiée le 7 juillet présente plusieurs atouts. Son préambule dense reprend les préoccupations d'une grande variété d'Etats présents aux négociations. La liste des obligations détaillée dans les articles, plus courte, permet de faire apparaître une norme claire sans se perdre dans des considérations techniques potentiellement sources de conflits. Ses faiblesses sont largement liées à ce choix politique. En effet, la procédure de signature pour les Etats nucléaires n'est guère limpide et donne l'impression que la question n'a pas été étudiée. Le choix de baser le Traité sur les accords

Les activités prohibées par le Traité (Article 1)

- Mettre au point, mettre à l'essai, produire, fabriquer, acquérir, posséder ou stocker des armes nucléaires.
- Transférer des armes nucléaires ou accepter le transfert d'armes nucléaires.
- Employer ni menacer d'employer des armes nucléaires.
- Aider, encourager, demander ou recevoir de l'aide ou inciter à des activités interdites par le Traité.
- Autoriser l'implantation, l'installation ou le déploiement d'armes nucléaires ou autres dispositifs explosifs nucléaires sur son territoire.



de garantie avec l'AIEA est peu ambitieux : 132 Etats ont déjà conclu un Protocole Additionnel avec l'Agence viennoise, un outil développé ultérieurement et beaucoup plus fiable pour assurer la détection d'un programme nucléaire clandestin[11]. Par ailleurs, certains Etats se sont inquiétés de l'articulation entre ce nouvel instrument et le Traité de non-prolifération (TNP), qui est jusqu'à maintenant la principale régulation de l'ordre nucléaire mondial. En effet, l'article 18 du TIAN estime que le Traité ne doit pas nuire aux obligations des Etats en vertu d'accords internationaux existants, mais seulement dans la mesure où ces obligations sont compatibles avec le TIAN[12].

Une nouvelle norme diversement reçue par la communauté internationale

L'adoption du texte du Traité est perçue de manière diamétralement opposée. D'un côté, les Etats engagés dans le processus saluent un événement historique[13]. Le 20 septembre 2017, le Traité a été ouvert à signature et les premiers Etats ont déposé leurs instruments de ratification (voir carte des Etats ayant signé et ratifié le TIAN). Par ailleurs, l'ICAN, très active pour favoriser l'adoption du TIAN depuis sa création en 2007, a reçu le Prix Nobel de la Paix à l'automne 2017 permettant de donner une certaine visibilité à la cause abolitionniste et au Traité récemment adopté.

De l'autre, les Etats nucléaires pointent les faiblesses du TIAN et soulignent son inadéquation à l'environnement stratégique actuel. Aux Etats-Unis et en Europe, un lobbying intense est mené pour dissuader les partenaires internationaux de rejoindre le régime. Cet exercice de conviction est particulièrement actif au sein de l'OTAN et à destination des pays coopérant avec l'Alliance comme la Suède ou la Finlande.

Outre stigmatiser l'arme nucléaire et renforcer le tabou contre sa possession et son utilisation, les négociateurs avaient pour objectif de faire pression sur les opinions publiques pour induire des changements de politiques, notamment dans les pays alliés des Etats nucléaires. Les pays de l'OTAN, et en effet ceux qui accueillent des armes nucléaires américaines sur leur territoire[14], sont considérés comme des cibles de premier choix pour ces pressions en raison d'une opposition traditionnelle de la population au nucléaire de manière large. De fait, le nombre de ratifications augmente progressivement, ce qui est logique au vu d'un Traité de ce type, mais le TIAN est rejeté avec une certaine fermeté dans plusieurs pays européens où le débat est sans doute moins important que ce qui pouvait être attendu. Ainsi en Allemagne, aux Pays-Bas ou en Norvège (pays où la première conférence sur l'impact humanitaire avait été organisée en 2013), les gouvernements expliquent clairement pourquoi leur pays ne souhaite pas rejoindre le TIAN[15]. Il est intéressant de noter que les partis d'opposition traditionnels dans ces pays comme dans d'autres ne soutiennent pas plus la perspective d'une adhésion. Par ailleurs, hors des frontières de l'OTAN, des pays ayant soutenu le Traité à l'ONU hésitent désormais à le ratifier. La Suisse estime qu'il pourrait nuire au TNP et regrette l'absence de procédures de vérification[16] et la Suède s'inquiète des répercussions sur ses coopérations avec l'Alliance Atlantique[17].

Les positions semblent donc se cristalliser sur la pertinence ou non du TIAN, sans que la question ne revête une importance politique majeure. Peu de débats publics sont en effet observés à ce sujet dans les différents pays qui envisagent de ratifier – ou de rejeter – le Traité. Pour autant, cette différence de vue se répercute sur l'ensemble des discussions ayant trait à la non-prolifération. Ainsi, lors du comité préparatoire à la conférence d'examen du TNP de 2018, de fortes oppositions ont été notées à ce sujet. Au vu de ce désaccord, beaucoup doutent de la capacité de la communauté internationale à s'accorder sur des mesures relatives à l'avenir du TNP lors de la prochaine conférence d'examen, en 2020[18].

Quelles potentielles conséquences pour le TIAN ?

Dans l'éventualité très probable où il entre en vigueur, le TIAN sera une norme juridique rendant les armes nucléaires illicites pour les pays l'ayant signé. Très expressément, les Etats nucléaires ont manifesté leur désaccord avec le texte dès son adoption, pour éviter que puisse se former une règle d'application globale selon les principes du droit coutumier. Il ne va donc pas contraindre ces Etats dans le court terme à réduire ou éliminer leurs arsenaux[19]. Au-delà des conséquences politiques, et notamment des tensions mentionnées sur le régime de non-prolifération et des blocages générés au niveau du TNP, le TIAN pourrait

cependant avoir des répercussions dans plusieurs domaines.

A l'évidence, le Traité est incompatible avec les doctrines de sécurité des neuf Etats nucléaires et de leurs alliés sous parapluie nucléaire[20]. Même parmi les autres Etats, certains devront s'interroger sur des pratiques en cours. Ainsi, les îles Marshall et le Kazakhstan louent des installations sur leur territoire, respectivement aux Etats-Unis et à la Russie, qui servent à perfectionner des missiles porteurs d'armes nucléaires.

D'autres, comme la Suède ou la Finlande, sont impliqués dans des coopérations militaires avec des Etats nucléaires. Elles se concrétisent par des exercices conjoints ainsi que par des investissements partagés sur des plateformes interopérables, potentiellement remis en cause en cas de signature par l'interdiction de « porter assistance » à des activités prohibées. Les négociateurs du Traité ont rejeté la proposition d'interdire le « transit » d'armes nucléaires. De potentielles difficultés seront donc évitées, en particulier en termes de surveillance des espaces aériens et maritimes. Néanmoins, des pays pourront sans doute utiliser le Traité pour interdire le passage de navires de pays nucléaires dans leurs eaux territoriales. Des collectivités locales ont déjà refusé de recevoir des sous-marins nucléaires, comme la ville de Naples[21].

Au niveau industriel, le Traité sera sans doute utilisé par les associations militantes pour relancer les campagnes de boycotts des entreprises travaillant dans le domaine du nucléaire. Ces initiatives existent déjà, notamment la campagne « Don't Bank on the Bank », qui recense les entreprises travaillant dans la production d'armements nucléaires et les différentes institutions financières qui les soutiennent. Dans un monde globalisé, les grandes entreprises du secteur possèdent souvent des filiales dans des pays intéressés par la ratification du TIAN[22]. Dans quelle mesure ces entreprises pourront-elles être impactées par le nouvel instrument ? Cela dépendra des lois de ratification nationales qui seront adoptées dans chaque pays. Il est à noter également que le Traité interdit de « porter assistance », mais pas explicitement de « financer » les programmes nucléaires, contrairement à ce qui était demandé par certains Etats et les ONG. Pour certains d'entre eux, le financement est naturellement compris dans la formulation retenue par le TIAN. Pour autant, il est possible que cette omission réduise la portée concrète du Traité pour les industriels du nucléaire militaire. Certains Etats signataires accueillent en effet des filiales de grands groupes travaillant sur le nucléaire de défense. On peut se demander s'ils retiendront une définition extensive du texte du Traité qui pourrait remettre en cause l'implantation de ces filiales et engendrer des pertes de revenus et d'emplois dans leur pays[23].

De manière plus hypothétique, on pourrait imaginer que les Etats signataires décident d'adopter des sanctions contre les entités et individus responsables de programmes nucléaires. Cette perspective est cependant extrêmement peu probable au vu des poids économiques et diplomatiques relatifs des différents acteurs concernés.

Conclusion

Dans un climat de fortes tensions entre puissances nucléaires, le ralentissement du désarmement à l'échelle mondiale a conduit à l'adoption d'une nouvelle norme, réclamée depuis des décennies par les communautés militantes. Elle permettra de combler le soi-disant « vide juridique » et de rendre illicites les armes nucléaires. Rejeté en bloc par les pays dotés et leurs alliés, ce Traité n'aura pas de conséquences immédiates en termes de réductions des arsenaux. Sa capacité à stigmatiser ces armes et en renforcer le tabou sera sans doute réduite au vu du peu de débat autour de ces questions dans les Etats dotés. Des conséquences concrètes et immédiates en termes militaires et industriels sont possibles mais de portée limitée. Pour autant, l'adoption du TIAN et sa possible entrée en vigueur dans les années qui viennent restent des événements significatifs. Tout d'abord, le Traité signale l'importance croissante du droit humanitaire et des initiatives légales visant à protéger les civils lors de conflits armés. Ensuite, il démontre la volonté pour les pays du Sud de peser davantage sur les questions de sécurité, de contester l'ordre établi à l'issue de la seconde guerre mondiale et confirmé à la fin de la guerre froide, et de ne plus dépendre des décisions des principales puissances. Enfin, il illustre l'antagonisme profond qui divise la communauté internationale sur le bien-fondé de la dissuasion nucléaire, perçue comme indispensable par certains pour garantir la stabilité internationale, et repoussante par d'autres qui se concentrent sur les effets destructeurs de ces armes.

EMMANUEL MAÎTRE
Chargée de recherche, FRS
e.maitre@frstrategie.org

Notes

1.Au 1er juin 2018, 10 Etats ont ratifié le texte : Autriche, Cuba, Guyana, Mexique, Palau, Palestine, Saint-Siège, Thaïlande, Venezuela, Vietnam.
2.« Status of World Nuclear Forces », *Federation of American Scientists*, avril 2015.
3.Maldera Nicolas, *Quelles évolutions pour la dissuasion nucléaire française ?*, Fondation IFRAP, 6 juillet 2016.
4.TICE pas encore en vigueur, impossibilité de négocier un Traité d'interdiction de la production de matière fissile.
5.Pledge presented at the Vienna Conference on the Humanitarian Impact of Nuclear Weapons by Austrian Deputy Foreign Minister Michael Linhart, 9 décembre 2014.
6.Report of the Open-ended Working Group taking forward multilateral nuclear disarmament negotiations, Genève, août 2016.
7.« Taking Forward Multilateral Nuclear Disarmament Negotiations », résolution de l'Assemblée Générale des Nations Unies A/RES/71/258, 23 décembre 2017.
8.Mis à part Singapour (qui s'est abstenu) et les Pays-Bas (qui ont voté contre le texte adopté), les autres Etats membres de l'OTAN et les Etats dotés n'ont pas participé aux négociations.
9.Maître Emmanuelle, « Vers un Traité d'Interdiction Nucléaire », *Bulletin n° 42,* Observatoire de la Dissuasion, FRS, avril 2017.
10.Maître Emmanuelle, « Adoption d'un Traité d'interdiction des Armes nucléaires », *Bulletin n°45*, Observatoire de la dissuasion, FRS, juillet 2017.
11.Lewis Jeffrey, « Safeguards Challenges in the Nuclear Weapons Ban », *Arms Control Wonk*, 10 juillet 2017.
12.Berger Andrea, « Understanding the New Nuclear Weapons Ban », *NTI*, 2 octobre 2017.
13.First Committee « General debate on all disarmament and international security agenda items », Statement by Austria delivered by Robert Gerschner, Director, Disarmament Department, Austrian Ministry for Europe, Integration and Foreign Affairs New York, 3 octobre 2017.

« *The new Treaty on the Prohibition of Nuclear Weapons is a historic achievement which Austria takes pride to have helped come about*. »

14.Allemagne, Belgique, Italie, Pays-Bas, Turquie.

15.Voir notamment l'intervention d'Heiko Maas, Ministre des Affaires étrangères allemand : « Je tiens à dire pourquoi nous ne signons pas le Traité de prohibition des armes nucléaire. À notre avis, il est plus logique d'adopter des mesures progressives de désarmement pour renforcer le TNP en tant que pierre angulaire de l'architecture du désarmement nucléaire et de la non-prolifération. Une interdiction immédiate des armes nucléaires sans mécanisme de vérification absolument fiable – qui manque manifestement visiblement – ne serait pas cohérente avec cet objectif, à notre avis. Un traité sur les armes nucléaires qui n'implique pas les États dotés d'armes nucléaires – c'est le problème à ce stade – et donc ne prend pas en compte l'environnement de sécurité, à notre avis n'est pas efficace, et donc nous n'avons pas choisi de le rejoindre jusqu'à présent », Deutscher Bundestag, Stenografischer Bericht, 22. Sitzung, Berlin, Mittwoch, den 21. März 2018, Plenarprotokoll 19/22, 21 mars 2018.

16.Sanders-Zakre Alicia, « Legislatures Act on Ban Treaty », *Arms Control Today*, mai 2018.

17.Örtengren Emanuel et Salmi Senni, « Sweden and Finland at Odds Over UN Nuclear Weapons Ban Treaty », *Center for Transatlantic Relations*, SAIS, 15 août 2017.

18.Cronberg Tarja et van der Meer Sico, « Working Towards a Successful Policy Brief NPT 2020 Review Conference », *Policy Brief*, Clingendael Institute, septembre 2017.

19.Harries Matthew, « The ban treaty and the future of US extended nuclear deterrence arrangements », in eds. Shatabhisha Shetty et Denitsa Raynova, Break*through or Breakpoint? Global Perspectives on the Nuclear Ban Treaty*, European Leadership Network, décembre 2007.

20.Cela concerne officiellement les 28 Etats de l'OTAN, le Japon et la Corée du Sud. De manière moins tranchée, un certain nombre d'alliés américains pourraient bénéficier de la dissuasion élargie de manière implicite, en Asie (Australie, Taiwan) ou au Moyen-Orient (Arabie Saoudite, …)

21.O'Connor Tom, « U.S. Nuclear Submarine that Attacked Syria 'Not Welcome' Back to Naples, Italy », *Newsweek*, 17 avril 2008.

22.Naval Group en Malaisie, Irlande et Brésil, BAE Systems en Suède et Afrique du Sud, Lockheed Martin en Nouvelle Zélande, …

23.Dall Emil, « A Balancing Act: NATO States and the Nuclear Ban Treaty », in eds. Shatabhisha Shetty et Denitsa Raynova, Break*through or Breakpoint? Global Perspectives on the Nuclear Ban Treaty*, European Leadership Network, décembre 2007.

FONDATION pour la RECHERCHE STRATÉGIQUE

Directeur de la FRS : Xavier Pasco
Responsable Publications/Evènements : Marylène Pion (m.pion@frstrategie.org)
Rédacteur en chef *Défense&Industries* : Hélène Masson, maître de recherche, en charge du Pôle Défense&Industries (h.masson@frstrategie.org)
Fondation pour la recherche stratégique - 4 bis rue des Pâtures - 75016 Paris

www.frstrategie.org

ISSN : 2274-598X