

Choix d'équipement des armées : rôle croissant des données et nécessaire recomposition du champ de bataille

L'essentiel : Ne pas être encore en retard d'une guerre

Notre think tank se donne pour mission de définir les politiques publiques qui, accompagnant l'émergence de progrès scientifiques ou technologiques, permettront à la Nation d'en tirer le meilleur profit. Dans le cas présent il s'agit de la défense nationale et européenne.

*Les leçons à tirer de la guerre en Ukraine, ainsi que des guerres au Moyen Orient menées par les Etats-Unis en partenariat avec Israël, permettent d'actualiser notre vision stratégique à la lumière du **rôle croissant des données** dans les opérations militaires, non seulement sur les champs de bataille, mais aussi chez l'adversaire, ses intentions, ses moyens d'action ses approvisionnements, son intendance, ses centres de décision.*

*Il s'agit de voir, d'anticiper, d'agir en utilisant les armes adaptées. Il s'agit de **concevoir les capacités militaires dans leur relation aux données** dans des perspectives à la fois individuelles et collectives. L'objectif n'est plus d'avoir les équipements les plus sophistiqués possibles mais d'exploiter les données pour optimiser l'emploi de capacités parfois simples afin de porter efficacement un effet létal capable de contraindre la volonté de l'adversaire.*

Ainsi les Ukrainiens ont intensément développé de nouvelles capacités pour lesquelles les algorithmes et les données constituent une caractéristique essentielle. Il en est de même des Israéliens, voire même des Iraniens.

Au-delà de l'émergence de nouvelles capacités militaires, emmenées par la prolifération des drones en Ukraine, le champ de bataille d'aujourd'hui est profondément impacté par l'utilisation de plus en plus intensive de données. L'accès et l'utilisation de ces données remettent-ils en cause les besoins en équipements militaires et donc la manière de les concevoir ? Comment envisager l'émergence d'une guerre pilotée par les données ? Celles-ci sont devenues de plus en plus critiques pour réduire le brouillard de la guerre.

Identifier la bonne information au bon moment constitue un véritable défi. Les données deviennent un carburant qui peut modifier les fonctionnalités des équipements militaires. Ces enjeux expliquent pourquoi l'intelligence artificielle est devenue si importante pour gérer la rareté et l'hétérogénéité des données.

Une guerre axée sur les données est susceptible de transformer les besoins et les moyens de produire des effets militaires. Nous atteignons le point de bascule entre une guerre basée sur les plateformes et une guerre basée sur les données. L'efficacité militaire doit devenir le véritable objectif. Les données qui étaient considérées uniquement comme un moyen tendent de plus en plus à devenir une fin pour atteindre la supériorité militaire. Le développement de plateformes complexes et avancées telles que les avions de combat ou les chars de combat semble moins pertinent. Une guerre basée sur les données requiert des capacités différentes, plus distribuées et décentralisées, et pourrait conduire à déconstruire la conception des grandes plateformes.

*Cette nouvelle perspective est susceptible de déplacer le barycentre du marché de la défense **en remettant en cause le rôle central des grandes plateformes très sophistiquées, complexes et très coûteuses qui caractérisent aujourd'hui les projets d'équipement des armées, du Rafale au porte-avions France Libre.***

Jacques Roger-Machart
Administrateur

*

*

*

Les capacités militaires sont devenues de plus en plus technologiques depuis la Seconde Guerre mondiale. Cette tendance s'est intensifiée ces dernières années sous deux facteurs : le retour de la guerre conventionnelle, entre États (opposée à trois décennies d'opérations essentiellement d'interposition) et l'essor des innovations numériques civiles sur les plans logiciel et matériel (accélérant le renouvellement des ressources militaires).

Cette évolution pourrait remettre en cause les équilibres au sein de la base technologique et industrielle de défense, bouleversant un paysage relativement stable depuis plus d'un demi-siècle. Peut-on pour autant considérer que les nouvelles règles du jeu sont en mesure de bouleverser ce marché ? Ou bien ces innovations ne constituent-elles qu'une intensification de tendances préexistantes ?

Si l'on analyse l'évolution des 100 premières entreprises de défense, on ne constate pas de percée nette de la part de nouveaux entrants. Certes, les gros titres des médias font état de quelques start-ups comme Anduril aux États-Unis, Helsing en Allemagne ou Harmattan AI en France, mais on ne perçoit pas de changement rapide et radical au sein de la base industrielle de défense comme l'ont connu en peu de temps les secteurs civils, comme la téléphonie mobile ou la photographie. Beaucoup de bruit pour rien, alors ?

La question posée dans cette contribution consiste à analyser dans quelle mesure le rôle croissant des données dans les opérations militaires conduit à remettre en question l'approche actuelle de l'efficacité militaire et, par conséquent, la manière de concevoir les capacités militaires dans leur relation aux données dans des perspectives à la fois individuelles et collectives. Une transformation rapide et inattendue peut-elle se produire en raison de la migration du centre de gravité vers une primauté des données et de leur exploitation ?

1. La numérisation comme continuité des trajectoires technologiques existantes ?

La guerre en Ukraine met en évidence un marché concurrentiel très dynamique avec plusieurs innovations qui devraient perturber un marché qui était jusqu'à présent assez stable en termes d'acteurs malgré une innovation à forte intensité technologique. La numérisation des capacités militaires et du champ de bataille n'améliore pas seulement l'efficacité des moyens opérationnels, mais est susceptible de modifier l'équilibre des pouvoirs entre les entreprises en place et les nouveaux entrants potentiels.

La guerre en Ukraine démontre globalement la valeur des systèmes existants, avec néanmoins quelques remises en cause. Les Ukrainiens sont impatients de recevoir des systèmes d'artillerie (CAESAR de KNDS, K9 Thunder sud-coréen de Hanwha), des véhicules blindés (K10), des missiles de défense aérienne et des avions de chasse (par exemple, F-16, Mirage 2000, Gripen). Néanmoins, ces capacités traditionnelles s'accompagnent d'un développement intensif de nouvelles capacités pour lesquelles les algorithmes et les données constituent une caractéristique essentielle. L'intensité de l'innovation capacitaire a atteint un rythme nouveau et inattendu dans les conflits récents, remettant en question l'approche traditionnelle de l'innovation dans l'armement autour de trajectoires technologiques préexistantes.

On pourrait considérer que ces capacités innovantes s'inscrivent dans un continuum, puisque l'électronique a bouleversé le marché de la défense dans les années 1960. En effet, la technologie est devenue de plus en plus importante dans la définition de nouvelles capacités et la fin de la guerre froide n'a pas arrêté cette tendance (même si elle s'est ralentie pour des raisons budgétaires et de maturité technologique). La numérisation semble être la suite logique de la prédominance de l'électronique. Certains s'attendent même à ce que « l'intelligentisation » s'inscrive dans un tel continuum, considérant que l'utilisation de plus en plus intensive de l'intelligence artificielle (IA) ne change pas les règles du jeu mais, au contraire, renforce les tendances passées et, ainsi, sécurise la position des entreprises en place.

Cela reflète la perspective du côté de la demande. Du concept de guerre centrée sur le réseau (NCW) des années 1990 à l'approche multi-domaines d'aujourd'hui, il existe une forte continuité. Cette dernière traduit la volonté d'utiliser la numérisation comme un moyen d'améliorer les capacités existantes en développant des systèmes avancés exploitant de plus en plus de données, dans une approche en réseau mobilisant des algorithmes sophistiqués. En d'autres termes, il n'y a aucune raison de contester l'utilité des capacités majeures existantes.

Au contraire, leur place apparaît plus centrale que jamais dans la perspective du client. La confirmation par le Président de la République du nouveau porte-avions en est un bon exemple. Ce système très complexe est présenté comme essentiel pour la défense nationale car il est bien plus qu'un simple pont d'envol. Son rôle est aussi d'être un centre de commandement reposant sur ces moyens d'une grande complexité. De même, les futurs systèmes de combat aérien positionnent toujours l'avion de chasse habité comme la clé de voûte adossé à des millions de lignes de codes et, symétriquement, les chars de combat restent au cœur des futurs principaux systèmes de combat terrestre.

Les données sont le carburant qui nourrit une architecture aussi complexe. Elles contribuent apparemment à renforcer la logique de l'architecture capacitaire préexistante. Par exemple, l'OTAN reste centrée sur une approche système de capacités, considérée comme nécessaire et précieuse pour rassembler les systèmes afin de traiter conjointement une tâche, tout en faisant preuve de flexibilité. La défense multi-domaines intégrée semble totalement dépendante de plateformes majeures sophistiquées.

Il n'est donc pas surprenant que les entreprises en place restent prédominantes et concentrent leurs efforts sur la sécurisation de cette numérisation des matériels militaires. Il est par exemple intéressant de noter qu'en octobre 2024, Lockheed Martin a nommé un spécialiste en ingénierie logicielle à la tête de son programme F-35 Joint Strike Fighter. Chauncey McIntosh a supervisé le développement logiciel du système d'armes Aegis ainsi que la gestion des programmes de défense antimissile, de radar, de construction navale, d'énergie dirigée et d'intégration des systèmes de combat.

Cependant, de tels développements liés aux données entraînent de nombreux défis pour offrir les avantages promis. Le programme F-35 a dû faire face à de nombreux problèmes logiciels, ce qui n'est pas étonnant quand on sait que les logiciels embarqués totalisent au moins 24 millions de lignes de code.¹ La complexité croissante des principales plateformes entraîne d'énormes problèmes d'ingénierie système, ce qui remet en question la logique cherchant à intégrer de plus en plus de fonctionnalités dans des plateformes déjà complexes.

Un rapport du Government Accountability Office (GAO) aux Etats-Unis indiquait en juin 2026 que le taux de capacité de mission de la flotte américaine des F-35 (pourcentage du temps qu'un avion peut réaliser une de ses missions) s'était réduit de 67% en 2021 à 44% en 2025. Le taux de capacité totale sur la globalité des missions attendues avait, lui, baissé de 38% à 25%, ce qui signifie que seul un avion sur quatre remplissait le contrat opérationnel.

Par ailleurs, les tendances récentes en Ukraine et au-delà témoignent d'une réelle transformation. L'innovation va au-delà de l'approfondissement des trajectoires technologiques. La manière dont l'innovation est engendrée apparaît disruptive en elle-même. Au-delà de l'émergence de nouvelles capacités militaires, emmenées par la prolifération des drones en Ukraine, le champ de bataille d'aujourd'hui est profondément impacté par l'utilisation de plus en plus intensive des données. Cette tendance devrait s'accroître et s'amplifier dans les années à venir sous la double influence des leçons tirées des engagements récents, notamment en Ukraine, et de l'évolution des possibilités technologiques, notamment le déploiement de solutions d'IA.

¹ Le logiciel du F-35 lui-même comprend 8 millions de lignes. Si l'on ajoute l'avion et le logiciel qui constitue ALIS (une suite de programmes au sol utilisés pour la logistique, la maintenance, le briefing/débriefing de mission, etc.), on obtient 24 millions de lignes.

Le champ de bataille tend de plus en plus à se fondre avec un espace de données, qui peuvent être créées et collectées (pour assurer un niveau accru de connaissance du champ de bataille), exploitées en quasi temps réel (pour dominer l'ennemi) ou encore permettre une plus grande efficacité dans l'utilisation des capacités et des troupes déployées (notamment en alimentant des algorithmes d'intelligence artificielle afin de réduire le « brouillard de guerre »). La transparence du champ de bataille devient à la fois une opportunité et un risque, ce qui explique aussi le retour massif de la guerre électromagnétique pour réduire cette transparence ainsi que pour empêcher l'adversaire de pouvoir opérer librement sur le théâtre des opérations.

Si les capacités les plus récentes trouvent leur efficacité dans l'exploitation massive de données, il est important de s'interroger sur les transformations structurelles qui ne sont pas forcément perceptibles aujourd'hui, mais qui peuvent conduire à repenser la conception des capacités militaires. En effet, les tendances actuelles pourraient s'éloigner de la logique de la guerre réseau-centrée (concentration des flux d'information vers des plateformes de plus en plus sophistiquées à l'image du chasseur F-35 américain), entraînant des transformations profondes du marché des capacités militaires (au-delà même des armements).

2. La rupture induite par la place des données dans les opérations militaires

Comment envisager l'émergence d'une guerre pilotée par les données ? A première vue, il n'y a pas de disruption, juste une question de flux de données croissant de manière exponentielle avec lesquels les systèmes peuvent opérer de plus en plus efficacement, en particulier face à des adversaires qui n'ont pas accès à ces capacités. C'est en réalité une vraie rupture paradigmatique qu'il faut envisager.

En effet, depuis la guerre d'Irak et d'Afghanistan au début du siècle, nous avons assisté à une explosion de données résultant de la multiplication (en quantité et en variété) des capteurs. En apparence, rien n'a changé, si ce n'est qu'il faut s'adapter pour gérer et exploiter ces flux. D'où la conception du F-35 qui constitue un « cerveau dans les airs » plutôt qu'un avion de combat classique.

La gestion des flux de données est un enjeu de plus en plus important depuis au moins deux décennies. Il s'est amplifié du fait de la multiplication et de la performance des capteurs, de l'explosion de la bande passante et des systèmes de communication (y compris spatiaux) et des capacités pour les exploiter. Identifier la bonne information au bon moment constitue un véritable défi mais il est également complexe de surmonter l'hétérogénéité des données en termes de sources, de formats, de qualité... afin de parvenir à une fusion en quasi temps réel.

Ces enjeux expliquent pourquoi l'intelligence artificielle est devenue si importante. « Le recours à l'IA permettra à court terme de répondre à des délais de réponse encore plus serrés et de rendre les forces armées plus réactives face à des menaces de plus en plus mobiles et résilientes. Ces problèmes d'optimisation multi-contraintes NP-difficiles font partie des cas d'usage qui peuvent être résolus grâce aux dernières avancées de l'IA. »²

Des approches sophistiquées sont nécessaires pour faire face aux différences qui existent entre l'IA civile et l'IA pour les forces armées. Ces dernières doivent gérer la rareté et l'hétérogénéité des données, l'absence de « lacs de données » entre parties prenantes (pour des raisons de protection et de secret), l'incertitude ou même de l'imprévisibilité du contexte opérationnel, les risques de désinformation et de manipulation...

Il est vrai que l'ère des données est une conséquence de l'amélioration des systèmes existants. Les données sont devenues de plus en plus critiques pour réduire le brouillard de la guerre. Néanmoins, les forces armées sont confrontées aux défis de l'info-obésité, ce qui signifie qu'elles s'attendent à ce que les capacités de nouvelle génération soient capables d'absorber des quantités presque illimitées de données afin d'améliorer leur efficacité.

² Entretien avec Yonathan Teboul (alors directeur de la stratégie digitale du groupe MBDA), Marine & Océans, janvier 2023, page 18.

Cependant, l'exemple du F-35 souligne les limites d'une telle complexification des plateformes existantes, qui apparaissent de plus en plus baroques, pour reprendre l'expression de Mary Kaldor. Même l'intelligence artificielle semble être considérée principalement comme un moyen de digérer ces flux croissants de données.

On peut parler d'un fantasme de la guerre réseau centrée depuis les années 1990. Certes, en théorie, la capacité à accéder et à traiter de larges flux de données permettrait de dominer les adversaires et de dissiper le brouillard de la guerre. Cependant, pour parvenir à un tel résultat, la complexité des capacités associées risque de devenir insurmontable. En effet, de tels systèmes très complexes reposant sur des technologies avancées et une architecture centralisée engendrent des problèmes d'ingénierie et de développement quasiment impossibles à surmonter. Elles devraient gérer trop de données, ce qui conduirait à l'incapacité d'exploiter convenablement ces dernières en raison de la saturation, du temps de latence, des besoins énergétiques, des capacités embarquées de calcul...

A terme, de telles machines sophistiquées échoueraient dans des environnements non permissifs car les contre-mesures sont de plus en plus capables de brouiller les communications ou de tromper et de perturber les capteurs, imposant une pénurie de données qui remettrait en cause l'utilisation optimale de capacités aussi complexes. Le développement de capacités omniscientes nécessiterait une domination militaire incontestée. C'était certainement le cas depuis les années 1990 jusqu'au début des années 2010, mais la guerre en Ukraine, et même déjà celle en Syrie, a révélé la perte progressive de cette domination technologique. L'égalité des chances qui en résulte a un impact sur la conception des capacités et la doctrine opérationnelle correspondante. De fait, la tendance à l'hypercentralisation sur des plateformes avancées comme le F35 pourrait être remise en question.

Les environnements non permissifs et les défis techniques liés aux capacités de dernière génération nous amènent à nous interroger sur la manière de distribuer les données et de les exploiter pour regagner la supériorité militaire. Le rôle croissant de l'intelligence artificielle dans les capacités de défense ne doit pas nous empêcher de comprendre la nature fondamentale de la transition en cours. En effet, les logiciels sont devenus un élément de plus en plus essentiel des capacités de défense. Cependant, cela représente le phénomène apparent qui cache une transformation plus profonde : la centralité des données dans l'efficacité des opérations militaires.

Le PDG de la start-up européenne d'IA Helsing, Gundbert Scherf, a souligné que l'efficacité des forces armées ne dépend plus en premier lieu du type d'armes dont elles disposent, mais des logiciels qui les utilisent. La défense devient de plus en plus une question de logiciels. Les forces armées sont aujourd'hui confrontées à un paradoxe. Les champs de bataille apparaissent de plus en plus transparents, comme l'illustrent les guerres en Ukraine ou en Iran.

Cependant, sur le terrain, l'accès à l'information apparaît de plus en plus remis en cause. Ainsi, au niveau opérationnel, une prise de décision hautement centralisée basée sur la connaissance de l'information ne peut plus être efficace. Les données doivent être exploitées sur le terrain de manière locale et distribuée plutôt que gérée de manière hiérarchique et centralisée. Cela explique pourquoi l'autonomie est au cœur du déploiement de l'IA : les forces armées et leurs capacités doivent pouvoir continuer à opérer même dans un environnement hautement contesté, du moins dans un contexte de guerre conventionnelle.

Le paradoxe est alors le suivant : une guerre centrée sur les données, souhaitée depuis des décennies par les forces armées pour parvenir à une pleine connaissance opérationnelle, conduit à questionner la pertinence de l'architecture des organisations militaires fondée sur la concentration des décisions et une approche hiérarchique stricte... qui a par exemple constitué le fondement du concept de guerre réseau-centrée il y a trois décennies. Une guerre centrée sur les données n'a pas *de deus ex machina* mais ressemble plutôt à l'organisation d'insectes sociaux comme les fourmis ou les termites.

En réalité, les données ne peuvent pas être utilisées uniquement comme une ressource brute. Une guerre véritablement centrée sur les données nécessite de reconsidérer en profondeur la manière dont les données représentent un levier pour atteindre des objectifs militaires. Comment organiser une hiérarchie de données et les gérer comme un atout clé ? En fait, la valeur des données est hétérogène et leur utilisation doit refléter le bénéfice attendu. Cela signifie qu'il n'est pas nécessaire de concentrer les données sur des plateformes majeures. Au contraire, il faut réfléchir à la manière de lier un type de données à une capacité donnée pour optimiser non seulement l'efficacité de cette capacité mais aussi sa capacité à atteindre l'effet militaire attendu dans une approche coordonnée entre les forces sur le théâtre des opérations.

Cette nouvelle perspective pose la question du niveau de pertinence et de la valeur : quelles données pour quels résultats ? Quel niveau d'accès ? Quels types de partages permettent de garantir la pertinence des actions entre les niveaux tactique, opératif et stratégique ? Ces questions conduisent à s'interroger sur la gouvernance adéquate des données et de leur exploitation pour en tirer la meilleure valeur possible au regard de l'effet militaire final recherché.

Cela conduit également à s'interroger sur l'usage final des données au-delà de la prise en compte traditionnellement envisagée. Les données deviennent un carburant qui peut modifier les fonctionnalités des équipements militaires en soi (mission-designed ?), leur capacité à faire face à un environnement contesté (autonomie) et à opérer collectivement afin de réaliser ensemble des effets qui dépassent leurs seules capacités individuelles (swarming, partage de données, etc.).

3. La véritable rupture induite par l'IA

Une guerre centrée sur les données est susceptible de transformer les besoins et les moyens de produire des effets militaires. Cette évolution constitue une approche visant à surmonter la contradiction entre qualité et quantité qui se pose depuis des décennies, illustrée par la « loi d'Augustine » (qui explique l'accroissement exponentiel du coût des matériels entre générations de capacités militaires depuis la deuxième guerre mondiale), mais qui est devenue plus aiguë au regard des leçons tirées de l'Ukraine ou de l'Iran : la quantité compte pour faire face à une guerre conventionnelle de grande ampleur.

Alors que nous atteignons le point de bascule entre une guerre basée sur les plateformes physiques lourdes et une guerre basée sur les données, la logique essentielle du développement des capacités doit évoluer afin de maximiser les bénéfices apportés par les données. Ceci devrait, logiquement, conduire à réévaluer sous cette perspective nouvelle la dynamique basée sur la prééminence de plateformes complexes et avancées telles que les avions de combat ou les chars de combat. En effet, toute la planification des capacités reste organisée autour de ces plateformes en tant que telles, tandis que la capacité à produire des effets militaires finaux pousserait à exploiter les données via des algorithmes d'IA qui permettent aux forces armées de prendre des décisions plus rapides et plus efficaces et d'optimiser l'engagement des ressources sur le champ de bataille.

Une telle rupture est apparue comme nécessaire avant même l'avènement de l'ère des données militaires. En effet, la sophistication des grandes plateformes a conduit, selon la loi d'Augustine, à une diminution de la taille des flottes, de moins en moins capables de couvrir de vastes champs de bataille. Cela a conduit à favoriser des systèmes très complexes, mais au détriment de la capacité à soutenir une guerre intense et longue sur un large territoire par un effet de masse, d'attrition et de résilience. Ce paradoxe a été accepté en raison du mythe de « l'arme décisive » (*Wunderwaffen*) illustrée par les évolutions récentes des avions de combat, mais qui n'ont malheureusement pas l'effet magique tant espéré pour décider, à elle seule, du sort de la guerre. Cependant, l'épreuve de vérité reste le champ de bataille et la guerre d'Ukraine fournit la démonstration que les plateformes très complexes, même très

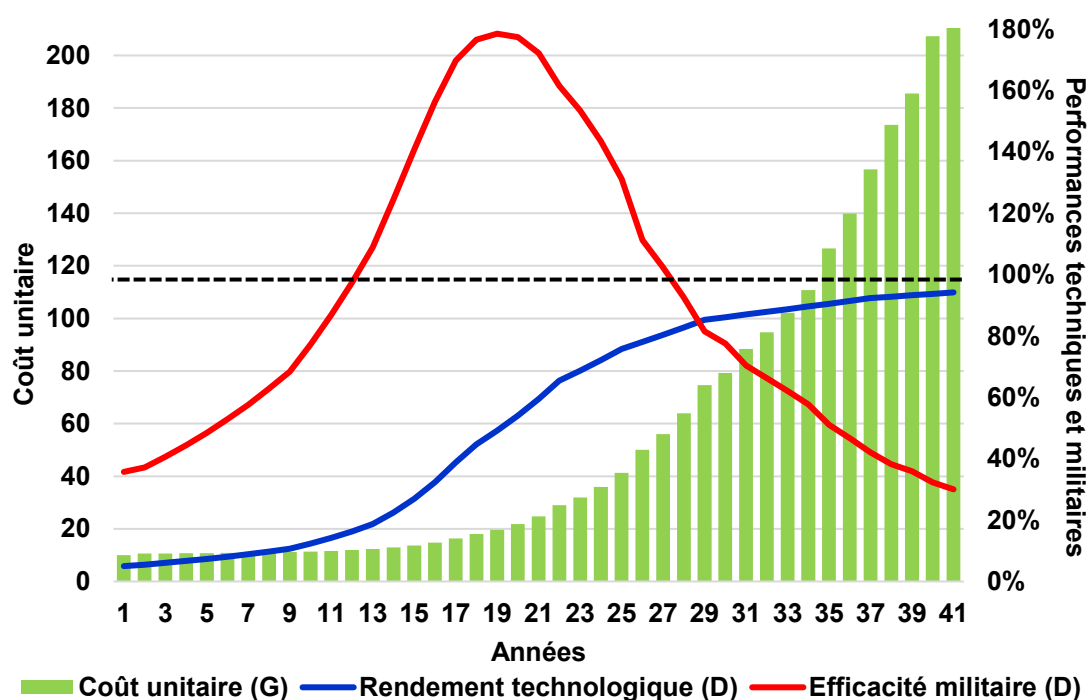
performantes, ne suffisent pas à réussir une guerre longue et intense car elles ne peuvent être disponibles qu'en très petite quantité.

A l'inverse, s'intéresser à l'optimisation des bénéfices des données peut changer la perspective en découplant les performances des plateformes et leur capacité à produire des effets militaires. En d'autres termes, l'IA et les autres algorithmes pilotés par les données ne constituent pas un moyen d'améliorer les performances intrinsèques de ces plateformes, comme on l'espérait auparavant, mais ils ouvrent la possibilité de reconsidérer la manière de mener les opérations, avec de nouveaux types de capacités et de nouveaux concepts opérationnels pour les engager.

La guerre nourrie par les données conduit à considérer les objectifs de résultats plutôt que les moyens pour les atteindre (approche centrée sur les plateformes, ce qui permet de s'appuyer sur des solutions moins gourmandes en technologie et des capacités plus simples. Dans une certaine mesure, c'est la seule solution pour surmonter les contradictions visibles à travers la guerre en Ukraine. Les performances avancées des capacités majeures réduisent la taille de la flotte et, par conséquent, la capacité à couvrir un vaste théâtre.

A l'inverse, il est possible d'acquérir de grandes quantités de capacités avec des performances limitées, mais un taux d'attrition élevé, voire très élevé limite la capacité à apporter un effet militaire décisif (même si cela permet de figer une zone de contact et d'y empêcher toute manœuvre décisive pour réintroduire de la mobilité pour rompre l'équilibre des rapports de force). L'équation doit alors être modifiée pour introduire une approche orientée vers les résultats, où l'efficacité militaire doit devenir le véritable objectif, comme le décrit cette simulation très simple.

Trilemme entre performance, coût et quantité



Source : Le juste prix des matériels militaires, un équilibre difficile à trouver, *DSI Défense Sécurité Internationale*, n°163, janvier-février 2023, pages 24-26.

En poursuivant ce petit exercice de pensée, nous entrevoyons l'existence d'un niveau de performance globale excédant celui d'une architecture centrée sur des plateformes très sophistiquées, donc trop chères et rares, pour être en mesure de saturer le gigantesque no-

man's land entre Ukraine libre et forces russes et, de surcroît, vulnérables individuellement à une attaque par une grande concentration de drones. C'est précisément ce à quoi a conduit le théâtre ukrainien. Certes, la situation est plus complexe que cela et il semble difficile de conclure qu'une flotte aérienne puissante serait inutile à l'Ukraine. Il n'en reste pas moins que dans ce contexte d'absence d'une telle flotte et d'insuffisance de munitions, ce nouvel équilibre où les drones prédominent les chars a émergé.

La représentation graphique ci-dessus va de pair avec notre expérience de pensée.

L'analyse ne doit pas regarder uniquement l'*input* (prix d'achat unitaire), mais aussi l'*output* que permet une capacité donnée (effet militaire final obtenu par unité employée) afin de comprendre si les armées paient le juste prix. Celui-ci est néanmoins difficile à établir car plusieurs paramètres sont en jeu : la contrainte budgétaire, les stocks attendus pour couvrir un théâtre militaire et les performances nécessaires pour, au minimum, combattre à armes égales avec l'adversaire. Ces différents paramètres sont, bien entendu, contradictoires entre eux dans la prise de décision, conduisant ainsi les pays occidentaux à avoir des « armées bonsaï » par une surpondération de la performance technique.

La guerre fondée sur les données devient de plus en plus importante, car c'est la seule solution pour combiner masse et efficacité. Les données ne sont pas en premier lieu un moyen d'améliorer les performances intrinsèques des capacités. Il faut inverser la logique : les capacités deviennent un instrument pour aider une approche opérationnelle basée sur les données afin de produire des effets militaires spécifiques.

L'exploitation des données vient améliorer les performances de systèmes « low cost » (munitions, drones, etc.) non par eux-mêmes mais dans leur emploi sur le théâtre des opérations. Plutôt que de chercher à améliorer des capacités majeures (en les complexifiant), les données et les algorithmes accroissent la valeur opérationnelle des composants bien plus simples tout en conservant l'effet militaire final recherché. La létalité et la précision des frappes sont préservées pour un coût moindre et des volumes bien plus importants : c'est le cœur de la révolution apportée par la guerre centrée sur les données.

De plus, l'intelligence artificielle apparaît comme un levier pour optimiser l'exploitation des données sur tout leur spectre et pour toute la gamme des usages possibles. Dans leur article fondateur « Des Minotaures, pas des Centaures : l'avenir des équipes habitées-sans pilote »³, Robert J. Sparrow et Adam Henschke démontrent clairement que la plupart des acteurs de la défense ne perçoivent pas les véritables perturbations résultant d'une guerre à forte intensité d'IA.

« La figure du centaure implique que lorsque les humains coopèrent avec des robots ou des IA, ce sont les humains qui seront aux commandes de l'équipe. La manière précise dont ils seront aux commandes reste ouverte. Scharre a introduit l'idée de la guerre des centaures en utilisant des exemples où les êtres humains sont dans la boucle et sur la boucle (...) nous pensons, contrairement à Scharre, que de nombreuses collaborations entre humains et machines seront plus précisément décrites comme des minotaures (des systèmes autonomes dirigeant des humains) que comme des centaures (des humains dirigeant des systèmes autonomes) parce que les machines des équipes seront effectivement aux commandes. »

Alors que Sparrow et Henschke ne s'intéressent qu'à l'impact de l'IA sur les dispositifs militaires, nous proposons d'étendre leur analyse disruptive pour passer d'une perspective IA à une perspective centrée sur les données. Une fois que les données sont placées au centre de l'organisation des opérations militaires plutôt que sur les grandes plateformes, il est possible d'optimiser les opérations en pensant aux effets militaires recherchés plutôt qu'aux moyens disponibles en tant que tels.

³ Sparrow, R.J., Henschke, A. (2023) Minotaurs, Not Centaurs: The Future of Manned-Unmanned. *The US Army War College Quarterly: Parameters* 53(1): 115-130.

En procédant à une telle révolution, il est possible de surmonter l'obsession pour des capacités de plus en plus sophistiquées, y compris des technologies avancées et des fonctionnalités supplémentaires. Cela conduit aussi à réfléchir à des capacités plus simples en elles-mêmes (mais non moins innovantes, même technologiquement) qui permettraient, de manière combinée, de porter les effets militaires recherchés tout en ayant un coût suffisamment faible pour redonner de la masse aux armées. En d'autres termes, la révolution des données dans les affaires militaires perturberait les caractéristiques fondamentales qui déterminent la loi d'Augustine et résoudrait le nœud gordien performance/quantité.

Conclusion

Le rôle des données dans la dynamique des marchés de la défense semble sous-estimé. La plupart des acteurs considèrent que les données constituent déjà une dimension clé et que les défis portent sur la manière d'accéder aux flux de données, de les gérer et de déterminer les moyens nécessaires pour les exploiter. Ce sentiment de continuité occulte le caractère radical des données dans la guerre d'aujourd'hui et, plus encore, de demain. Les données étaient considérées uniquement comme un moyen, mais elles tendent de plus en plus à devenir une fin pour atteindre la supériorité militaire.

Cette nouvelle perspective est susceptible de déplacer le barycentre du marché de la défense en remettant en cause le rôle central des grandes plateformes très sophistiquées et complexes qui caractérisent aujourd'hui l'équipement des armées, du Rafale au porte-avions « France Libre ». Ceci ne veut pas dire que ces plateformes sont inutiles, mais leur poids relatif va évoluer avec des moyens complémentaires, en particulier des drones, qui permettront de réaliser plus de missions simples.

Il est important de développer ces capacités et les algorithmes qui les mettront en œuvre, pour jouer à armes égales ou même dominer de nouveau nos adversaires. Ceci suppose de réfléchir aux équilibres dans l'allocation du budget. Il ne faut pas que les capacités historiques absorbent une part excessive des ressources de manière à ouvrir des fenêtres d'opportunité pour monter en maturité sur les moyens de la guerre fondée sur les données et accompagner leur appropriation par les armées, à l'aune de la cavalerie blindée ou de l'aviation de guerre dans l'entre-deux-guerres.

Une guerre basée sur les données requiert des capacités différentes, plus distribuées et moins centralisées, et pourrait conduire à reconsidérer la manière d'envisager et de concevoir des grandes plateformes, notamment à vocation centralisatrice. Cela est susceptible d'ouvrir le marché à de nouvelles solutions innovantes conçues autour des données plutôt que de s'appuyer dans leurs missions principales sur les données en tant que ressources périphériques. C'est la raison pour laquelle une guerre basée sur les données pourrait être une dynamique véritablement transformatrice, similaire à l'essor de l'électronique dans les capacités de défense.

Enfin, il est aussi important de prendre en considération la guerre au-delà du champ de bataille. La désinformation et la guerre informationnelle sont des dimensions qui impliquent des données au-delà des aspects purement militaires mais qui peuvent influencer sur la volonté de poursuivre le combat. Cette dimension doit être pleinement prise en considération mais constitue un sujet en soi, au-delà de la présente note.

Renaud BELLAIS

Chercheur associé au CESICE, Université Grenoble Alpes, et co-directeur de l'Observatoire de la défense, Fondation Jean Jaurès

Diplômé de l'Institut d'Études Politiques de Lille et docteur HDR en sciences économiques, Renaud Bellais est Group chief defence economist de MBDA depuis 2023 après un parcours professionnel à la DGA et dans le groupe Airbus depuis 2000. Il est chercheur associé au CESICE, Université Grenoble Alpes. Il assume une chronique sur l'économie de défense dans la revue *DSI Défense & Sécurité Internationale*. Depuis 2021, il assure la codirection de l'Observatoire de la défense de la Fondation Jean Jaurès (Paris).

Publications récentes (sélection)

Burden Sharing: Misunderstandings, Issues and Stakes Inside the Atlantic Alliance, *Canadian Military Journal*, vol. 25, n°4, automne 2025.

[avec Hélène Conway-Mouret et Thibault Delamare], Pour une dissuasion stratégique européenne, *La Tribune*, 8 septembre 2025.

Golden Dome, le retour trumpien de la « Guerre des étoiles » de Ronald Reagan, *DSI Défense Sécurité Internationale*, n°179, septembre-octobre 2025, pages 22-26.

Industrie de défense : une surprenante transformation pour l'Union européenne in Sylvain Kahn et Théo Verdier (coord.), *2005-2025 : les vingt années qui ont transformé l'Europe La méthode de l'Union face aux crises*, Paris, Fondation Jean Jaurès, 2025, pages 15-19.

Se préparer à la guerre. Quels enjeux pour la politique industrielle de défense ? in Delphine Deschaux-Dutard (dir.), *La guerre en Ukraine, facteur d'intégration ou de désintégration européenne et internationale ?*, Mare & Martin, 2025, pages 151-164.

Market Structures, Competition and Innovation: Grounds for an Alternative Defence Industrial Policy, *Defence and Peace Economics*, vol. 35, n°4, 2024, pages 448-463.

The future of cooperative programmes in Europe, paradox of a hybrid market, *The Economics of Peace and Security Journal*, vol. 18 n°1, avril 2023, pages 76-91.