LA CAPTURE SILENCIEUSE

Anatomie d'une stratégie d'hégémonie décisionnelle au sein des commandements contemporains

Comment conquérir un état-major sans jamais déclarer la guerre

par le Colonel Bruno de SAN NICOLAS, Stratégie numérique

Avant de lire ce qui suit, répondez à cinq questions.

- Vos officiers évaluent-ils la valeur militaire d'un système essentiellement à l'aune de la fluidité de son interface ?
- Vos équipes seraient-elles capables de planifier une manœuvre complexe sur carte papier en moins de trente minutes si le système était indisponible ?
- Vos décisions d'état-major sont-elles davantage cadencées par le rythme de rafraîchissement de l'écran que par vos objectifs stratégiques ?
- Votre organisation serait-elle en mesure de migrer vers une plateforme alternative en moins de six mois sans perte opérationnelle significative ?
- Ressentez-vous un soulagement à l'idée que le système « partage » la responsabilité d'une décision en cas d'échec ?

Si trois de ces réponses ou plus sont affirmatives, la capture est avérée. Ce n'est pas un jugement sur la qualité des hommes. C'est le diagnostic d'un environnement cognitif qui a été progressivement et méthodiquement orienté en faveur d'un acteur extérieur. Ce document décrit comment.

AVANT-PROPOS

Il est des transformations qui s'opèrent au grand jour — avec appels d'offres, délais réglementaires, évaluations contradictoires et décisions souveraines documentées. Et il en est d'autres qui s'opèrent de la même façon qu'un poison lent : invisiblement, progressivement, avec le goût du médicament.

L'histoire que ce document décrit — sans nommer ses acteurs, parce qu'elle se répète — est celle d'une plateforme algorithmique de ciblage, développée dans le contexte des guerres américaines post-2001, progressivement imposée au cœur d'un grand commandement multilatéral occidental, en moins de dix ans, sans jamais avoir fait l'objet d'une décision souveraine authentique de la part des nations qui la subissent aujourd'hui.

Ce n'est pas une théorie du complot. C'est une ingénierie du fait accompli. La différence est décisive : la première suppose un secret ; la seconde n'en a nul besoin. Elle se déroule à la lumière du jour, avec toute la transparence nécessaire — celle qui éblouit plutôt qu'elle ne révèle.

Deux objections méritent d'être adressées d'emblée. La première : les procédures d'acquisition militaires existent précisément pour prévenir ce type d'infiltration. C'est exact. Ce document explique les trois mécanismes structurels qui les rendent inopérantes dans ce cas précis. La seconde : la performance opérationnelle du système est réelle. C'est également exact. Ce document explique pourquoi cela ne suffit pas. À qui appartient, en dernier ressort, le jugement sur ce fonctionnement ? Voilà ce qu'il convient d'examiner.

Les éléments factuels cités proviennent d'enquêtes journalistiques de référence et de publications doctrinales.

Ils sont traités ici comme matériaux analytiques, non comme plaidoyer. Le lecteur est invité à les interroger : c'est exactement ce que l'article lui demande d'apprendre à faire.

PARTIE I — LA MÉCANIQUE DE LA CAPTURE

La stratégie de pénétration d'un commandement militaire par un système d'information à dominante privée obéit, dans sa forme la plus accomplie, à quatre phases distinctes. La force du dispositif tient moins à chaque phase prise isolément qu'à leur convergence. Pris séparément, chaque élément semble défendable. Réunis, ils constituent l'un des dispositifs de capture institutionnelle les plus efficaces jamais déployés contre une organisation militaire.

Phase 1 — L'insurrection par le bas : contourner avant d'être autorisé

Le premier vecteur d'entrée n'est pas la porte principale — celle des procédures d'acquisition, des comités de normalisation, des avis juridiques. C'est la frustration des opérateurs.

Dans toute grande organisation militaire coexistent des officiers qui vivent la lenteur bureaucratique comme une menace opérationnelle en soi. Brillants, opiniâtres, convaincus que les systèmes officiels sont dangereusement obsolètes, ils constituent le profil-cible idéal pour une première phase d'introduction. Sharon Weinberger, dans son enquête de référence sur la genèse des premières plateformes de ciblage algorithmique américaines, décrit cet officier

comme quelqu'un qui « ne prend pas non pour une réponse et casse un peu de verre », bénéficiant d'une couverture institutionnelle suffisante au sommet pour opérer sans en référer à quiconque[1].

La méthode repose sur deux leviers complémentaires : la reprogrammation de fonds existants, qui permet de financer le dispositif sans déclencher les seuils d'approbation formelle, et le cadrage en « expérimentation », qui repousse le déclenchement des procédures d'acquisition bien au-delà du seuil de dépendance effective[1]. Des ingénieurs de l'éditeur arrivent sur site. Un générateur est livré sans facture. Des serveurs transitent sur des vols militaires. En huit semaines — le chiffre est documenté — 250 utilisateurs dans 30 sous-groupes opérationnels utilisent le système quotidiennement[1].

C'est précisément pourquoi les procédures existantes n'ont pas pu jouer leur rôle : elles sont conçues pour encadrer une décision ponctuelle, non pour intercepter une convergence de micro-initiatives formellement anodines. À ce stade, la question de l'autorisation d'emploi est déjà périmée. Le système n'est plus un objet d'évaluation. Il est une infrastructure.

> *« La décision souveraine n'a pas été prise. Elle a été prise par inadvertance, fragment par fragment, sans jamais que personne n'ait eu à approuver l'ensemble. »*

Le dispositif possède une propriété saisissante : il inverse le rapport de preuve. Ce n'est plus à l'éditeur de démontrer que son système mérite d'être adopté. C'est à l'organisation de justifier pourquoi elle envisagerait d'abandonner ce qui fonctionne déjà. Revenir en arrière, une fois que 250 personnes ont reconstruit leurs routines de travail autour du système, c'est une révolution d'une difficulté proprement rédhibitoire.

Phase 2 — La séduction par le design et le cadrage de l'urgence

Ces deux vecteurs sont souvent analysés séparément. Ils forment en réalité les deux faces d'un même mécanisme d'érosion du jugement.

L'interface comme présomption de supériorité
L'interface — les animations fluides, les tableaux de bord dynamiques, les couches de données superposées sur cartographie haute résolution — ne produit pas seulement du confort d'usage. Elle produit un effet cognitif immédiat que la recherche comportementale désigne sous le terme d'effet de halo[2] : si l'outil est beau, il est présumé efficace. Si l'interface est fluide, la donnée est présumée fiable. Si le tableau de bord est imposant, la décision est présumée éclairée.

Le problème n'est pas qu'un outil soit bien conçu. Le problème est la conversion implicite de l'élégance de l'interface en preuve de valeur militaire. Une organisation de commandement peut alors confondre quatre choses profondément distinctes : la qualité de présentation, la qualité des données, la qualité du traitement algorithmique, et la qualité de la décision. Ce glissement conditionne l'ensemble de la relation que l'état-major va entretenir avec le système pendant les années qui suivent.

Il convient ici d'interroger les chiffres cités par l'éditeur — et reproduits sans distance par la plupart des observateurs : le passage de moins de 100 à 1 000 cibles identifiées par jour par vision par ordinateur, puis à 5 000 après intégration de grands modèles de langage[1]. Ces chiffres semblent imparables. Sauf que la question de ce que recouvre le terme « cible » dans ce contexte — identification ? désignation ? priorisation ? — et celle de la fiabilité, de la traçabilité et de la gouvernance de ces identifications restent, elles,

obstinément sans réponse publique. Reproduire ces chiffres sans les interroger, c’est déjà subir le mécanisme que ce document décrit.

Le cadrage de l’urgence comme compresseur de jugement
Le monde opérationnel est effectivement marqué par la contraction des délais, la pression du tempo et la montée des vulnérabilités. L’adversaire technologique investit. Les écarts de capacité se creusent. Tout ceci est vrai. C’est précisément ce qui rend l’argument d’urgence si efficace et si dangereux.

L’urgence possède une propriété singulière : elle réduit la disponibilité psychologique et institutionnelle à la contradiction. Plus l’urgence est invoquée, plus demander du temps paraît suspect. Plus la menace est rappelée, plus exiger une évaluation approfondie semble déplacé. Le débat se transforme : il ne porte plus sur la profondeur réelle de la capacité, ses dépendances, ses coûts cachés. Il porte sur la volonté supposée de s’adapter. L’évaluation technique devient une épreuve de loyauté au rythme du moment.

Ce mécanisme peut être décrit comme le cadrage de la contingence zéro[3] : instiller la conviction que sans cette technologie, le prochain conflit sera perdu avant même d’avoir commencé. La peur de l’obsolescence est, dans le domaine militaire, le moteur de décision le plus puissant qui soit — et le plus manipulable.

> ***POINT METHODOLOGIQUE*** *La première expérimentation opérationnelle réelle du système est décrite par les participants eux-mêmes comme « décevante »[1]. L’adhésion institutionnelle précède donc la maturité technique. C’est la marque caractéristique d’un biais d’adoption réussi.*

Phase 3 — La normalisation cognitive : formation de masse et communication stratégique

Les deux phases précédentes ont créé la dépendance opérationnelle. La troisième la consolide en la rendant culturelle.

La formation comme reconfiguration des routines de jugement
Former massivement, tôt et vite, ce n'est pas seulement apprendre à se servir d'un outil. C'est acculturer une organisation à une nouvelle grammaire de travail. Les personnels formés n'apprennent pas seulement des gestes : ils apprennent des catégories d'analyse, des formats de représentation, des réflexes d'interrogation, des attentes implicites sur ce qu'il convient de regarder, montrer, comparer, signaler au chef. La formation ne transmet pas un usage ; elle reconfigure les routines de jugement.

Ce phénomène prend une dimension systémique dans un commandement multilatéral. Lorsqu'une alliance regroupe des nations aux traditions doctrinales, aux cultures stratégiques et aux intérêts géopolitiques parfois divergents et forme massivement leurs état-majors sur une plateforme unique, elle n'améliore pas seulement ses capacités opérationnelles : elle homogénéise sa pensée stratégique autour de la logique propriétaire d'un seul éditeur. Ce n'est plus de l'interopérabilité. C'est de la standardisation cognitive.

La rapidité du phénomène est révélatrice : au printemps 2025, une version du système commence à être utilisée par la structure concernée[1]. En octobre 2025, dix nations membres avaient déjà signalé leur intention de l'adopter dans leurs propres armées[1]. La progression est foudroyante et auto-entretenue. La décision est nationale en apparence, collective en pratique, aucunement souveraine.

La communication stratégique comme préemption du débat
La communication institutionnelle autour du système — interne et externe — ne cherche pas seulement à convaincre. Elle cherche à rendre le débat coûteux.

En interne, elle produit de l'adhésion en associant la capacité à des valeurs cardinales : gain de temps, réduction de la friction, protection des forces, supériorité décisionnelle, transformation de l'état-major. En externe, elle projette une image de modernité et de sérieux doctrinal. À partir d'un certain seuil, le projet cesse d'être un objet d'évaluation : il devient un récit institutionnel. Contester un récit institutionnel change de nature : ce n'est plus seulement questionner une solution, c'est fragiliser une trajectoire de transformation publiquement assumée.

Ce dispositif bénéficie d'un vecteur particulier : la mobilité de cadres supérieurs entre des postes d'autorité dans la structure concernée et des responsabilités chez le fournisseur, sans que le cadre déontologique applicable ait été clairement documenté dans les cas signalés[4]. Ce mouvement crée une boucle de rétroaction : l'organisation informe l'éditeur, qui s'en sert pour crédibiliser son offre auprès des nations suivantes.

Phase 4 — Le verrouillage ontologique : quand l'outil devient le prisme du réel

La phase finale est la moins visible et la plus décisive. Elle ne possède pas de date d'entrée en vigueur. Il n'y a aucune procédure, aucune signature, aucun comité. Elle s'installe silencieusement, et c'est lorsqu'on s'en aperçoit qu'il est généralement trop tard.

L'ontologie d'un système d'information militaire désigne sa grammaire logique : la manière dont il définit les entités pertinentes, les relations entre elles, ce qui compte comme information exploitable et ce qui ne compte pas, ce qui est

affiché et ce qui reste invisible. Celui qui maîtrise l'ontologie d'un système maîtrise la perception du réel de ceux qui l'utilisent. Il est le dictionnaire invisible de la guerre.

La conséquence est grave : ce qui n'est pas modélisé dans le système — la nuance culturelle, le signal faible, le doute stratégique, l'intuition du terrain, la résistance locale non quantifiable — cesse progressivement d'exister pour le commandement. L'état-major ne voit plus le monde : il voit la représentation du monde que lui propose l'éditeur. Et comme cette représentation est cohérente, fluide, rapide, elle est perçue comme supérieure à toute représentation alternative, fût-elle plus juste.

Bachelard décrivait en 1938 ce qu'il appelait l'obstacle épistémologique : la tendance de la connaissance établie à se protéger contre les remises en cause extérieures[5]. Appliqué à un état-major numériquement transformé, cet obstacle prend une forme inédite : l'outil ne résiste pas à la contradiction. C'est l'organisation elle-même qui résiste — au nom de l'outil.

PARTIE II — LA VULNÉRABILITÉ STRATÉGIQUE INVISIBLE

L'image la plus souvent utilisée pour nommer les conséquences de ce processus est celle du vendor lock-in contractuel. Elle est juste, mais réductrice. Elle ne décrit que la surface d'un problème qui est, en profondeur, de nature stratégique et identitaire.

Un verrouillage à six dimensions

1. **Vendor lock-in contractuel** : lorsqu'un état-major intègre plus de 150 flux de données et le travail de plus de 50 entreprises dans une plateforme unique[1], le coût de sortie n'est plus technique. Il est organisationnel, doctrinal, budgétaire et politique.
2. **Workflow lock-in** : l'état-major adapte ses procédures, ses briefings, ses points de situation à la logique interne de l'outil. Ce n'est plus seulement le logiciel qui est adopté ; ce sont ses manières de voir et de travailler.
3. **Data lock-in** : les flux, les ontologies, les référentiels sont absorbés par l'environnement de l'éditeur. L'organisation perd progressivement la capacité de distinguer la donnée de son contenant, et de penser la portabilité réelle de ses propres actifs informationnels.
4. **Training lock-in** : une fois l'ensemble de l'état-major formé, la masse des compétences accumulées crée une inertie favorable au maintien du système, même lorsque ses limites deviennent plus manifestes.
5. **Doctrinal lock-in** : lorsqu'un outil structure la façon dont les officiers conçoivent la préparation, la situation, la synchronisation, la priorisation des options, il influence la doctrine de fait – sans jamais avoir été reconnu comme tel.
6. **Cognitive lock-in** : le plus grave. L'état-major commence à confondre la structure fournie par l'outil avec la structure du réel. La dépendance n'est plus seulement industrielle. Elle touche la liberté intellectuelle de l'organisation.

L'homogénéisation comme vulnérabilité

stratégique

Il existe une conséquence systémique rarement formulée et pourtant décisive. Elle est, de loin, la plus grave sur le plan de la théorie militaire.

Lorsque la pensée stratégique de plusieurs nations alliées est homogénéisée autour d'une même logique propriétaire, elle devient prévisible. Un adversaire qui comprend l'ontologie du système — ce qu'il voit, ce qu'il ne voit pas, comment il hiérarchise l'information, comment il attribue les entités, comment il présente les options au décideur — dispose de quelque chose de bien plus précieux qu'un renseignement ponctuel : il dispose d'une carte de la structure cognitive du commandement adverse. C'est ce qu'Arquilla et Ronfeldt nommaient déjà, en 1997, la vulnérabilité propre aux organisations militaires opérant en environnement d'information structurée[6].

> *« Comprendre l'ontologie de l'outil de votre adversaire, c'est connaître les angles morts de sa pensée stratégique.»*

L'atrophie silencieuse du jugement autonome

Lorsqu'un système capte progressivement les fonctions de synthèse, de fusion, de priorisation et de préparation des options, l'état-major peut être tenté de sous-investir dans les savoir-faire humains qui lui permettaient d'exercer un jugement autonome sur ce système.

Le paradoxe est cruel : plus un outil semble rendre l'état-major intelligent, plus il fragilise, à terme, l'autonomie intellectuelle qui lui permettrait de juger lucidement cet outil. Une armée incapable de fonctionner sans son interface n'est pas une armée transformée. C'est une armée captive. Un bon état-major ne vaut pas seulement par les outils qu'il

possède, mais par les compétences qu'il conserve lorsque ces outils dégradent, se contredisent, ou ne couvrent plus le cas réel.

PARTIE III — LA CONTRE-OFFENSIVE

Pourquoi les garde-fous ont failli

Trois mécanismes structurels expliquent l'insuffisance des procédures existantes dans ce type de configuration — trois mécanismes que la Phase 1 a précisément conçus pour exploiter.

D'abord, la fragmentation de la décision. Aucun acteur individuel n'a pris la décision d'adopter le système. Chaque étape était défendable prise isolément : une expérimentation pilote, un contrat de régularisation, une formation complémentaire, une extension de déploiement. Les procédures d'acquisition sont conçues pour s'appliquer à des décisions. Elles s'appliquent mal à des convergences.

Ensuite, l'asymétrie temporelle. La dépendance se construit en semaines. L'évaluation institutionnelle prend des mois. Quand les comités compétents sont en mesure de se prononcer, le système est déjà en production depuis suffisamment longtemps pour que toute conclusion négative soit opérationnellement irréalisable.

Enfin, et c'est le mécanisme le plus difficile à corriger : l'alignement des incitations individuelles. Les officiers qui ont soutenu et promu le système ont construit leur réputation sur son succès. Les équipes formées ont investi dans sa maîtrise. Les directions concernées ont engagé leur crédit institutionnel sur sa mise en œuvre. Une évaluation négative n'est plus seulement un jugement technique : c'est une menace pour les trajectoires professionnelles de ceux qui ont porté

le projet. Le biais d'adoption est aussi un biais de survie institutionnelle.

Six contremesures, conditionnées à leur économie politique

Les contremesures suivantes ne sont efficaces que si leur économie politique est résolue simultanément. Proposer des procédures sans aborder les résistances structurelles à leur application, c'est reproduire l'erreur d'analyse que ce document dénonce.

A. **Séparer évaluation et narration**
   Aucune capacité structurante ne devrait être communicable avant d'avoir été évaluée. En pratique : créer une distinction institutionnelle stricte entre la phase d'expérimentation — réservée, contradictoire, conduite avec des évaluateurs indépendants de la chaîne d'acquisition — et la phase de communication, publique et ultérieure. Toute organisation qui communique sur un système avant d'en avoir stabilisé le jugement se condamne, par avance, à ne pouvoir conclure qu'en sa faveur. C'est la création d'un coût cognitif irrécupérable avant même que l'investissement soit réalisé. La condition politique de cette séparation : que le dirigeant qui commande l'évaluation ne soit pas celui qui bénéficiera de son succès.
B. **Instituer un Red Team permanent de l'adoption**
   Pour chaque système structurant, une équipe dédiée — indépendante, permanente, disposant d'un droit formel de contradiction — a pour mandat exclusif de démontrer les limites du système, ses dépendances, ses angles morts, ses hypothèses cachées. Elle ne doit pas être composée de sceptiques systématiques, mais des meilleurs experts disponibles, avec pour seule directive d'éprouver le système jusqu'à le faire céder. La condition politique : que ses conclusions aient une valeur contraignante, et

non simplement consultative.

C. **Protéger les compétences de mode dégradé**
   Toute organisation qui adopte un système d'information structurant doit maintenir, de manière obligatoire et régulière, des exercices de fonctionnement sans ce système : planifier une manœuvre complexe sur carte papier, conduire un point de situation sans tableau de bord, développer une appréciation de situation sans couche de données algorithmique. Dans un théâtre adverse, le système d'information du commandement est la première cible. Une organisation incapable de fonctionner sans son interface a sous-traité sa résilience à un acteur privé extra-institutionnel.

D. **Encadrer la mobilité des cadres supérieurs**
   La rotation entre postes d'autorité d'acquisition et responsabilités chez les fournisseurs concernés constitue l'un des vecteurs d'influence institutionnelle les plus puissants et les moins visibles. Les mécanismes de pantouflage sont bien documentés dans l'espace civil. Leur extension aux domaines de la sécurité et de la défense nécessite des périodes de carence explicitement calibrées sur la durée des décisions d'acquisition auxquelles le cadre concerné a participé.

E. **Adopter une doctrine de souveraineté opérationnelle de continuité**
   Comme préalable à toute décision d'adoption d'un système extérieur, poser systématiquement la question suivante : si ce système devenait indisponible demain — pour des raisons commerciales, techniques, politiques ou adversaires — quelle est notre capacité résiduelle de commandement ? Cette question, d'apparence simple, est en pratique presque jamais posée au moment de la décision d'adoption. Elle est posée, quand elle l'est, lorsque le système est déjà en production depuis suffisamment longtemps pour que la réponse honnête soit : « Nous ne savons plus. »

F. **Auditer régulièrement l'ontologie**

> Quelles entités le système modélise-t-il ? Lesquelles ignore-t-il ? Quels signaux sont amplifiés ? Quels biais sont intégrés dans les algorithmes d'attribution et de priorisation ? Cette question n'est pas une question d'ingénierie. C'est une question de doctrine. Elle ne relève pas du service informatique ; elle relève du commandement. Si le commandement est incapable d'y répondre avec précision, le verrouillage ontologique est déjà installé.

CONCLUSION — Ce que le général doit savoir que l'écran ne lui dira pas

La dépendance décrite dans ce document n'est pas un sujet informatique. Ce n'est pas un sujet juridique. Ce n'est pas même un sujet budgétaire. C'est un sujet de philosophie du commandement.

La question n'est pas « est-ce que l'outil fonctionne ? ». La réponse à cette question est oui — et elle est accessoire. La question est : au terme de quatre phases méthodiquement menées, l'organisation conserve-t-elle la capacité de juger l'outil qui la juge ?

L'histoire de l'art militaire est ponctuée de commandements qui ont perdu leur liberté de jugement — non sous la pression directe de l'ennemi, mais sous celle de leurs propres cadres cognitifs, de leurs propres outils de représentation, de leurs propres certitudes transformées en dogmes. La ligne Maginot n'était pas seulement un dispositif physique : c'était une structure mentale qui avait réduit la capacité du commandement à envisager l'alternative. Les systèmes d'information changent. Le mécanisme, lui, est aussi vieux que la guerre.

> *« Le véritable chef n’est pas celui qui possède l’outil le plus rapide. C’est celui qui conserve la liberté de l’éteindre pour recommencer à penser. »*

Le cas analysé dans ce document n’est pas un cas historique. C’est un cas en cours. Et son issue dépend d’une seule capacité institutionnelle, à laquelle aucune procédure ne peut se substituer : la volonté d’un état-major de maintenir, face à l’outil qui le séduit, la distance critique qui lui permet de décider que l’écran a tort.

Une dernière question s’impose, que ce document ne résoudra pas mais qu’il serait imprudent de ne pas formuler. Si le diagnostic est juste, se pose nécessairement la question de l’alternative souveraine. Des tentatives existent : initiatives de cloud européen de défense, projets d’IA multilatérale pilotés par des structures de commandement autonomes, réflexions doctrinales en cours dans plusieurs capitales. Aucune n’a à ce jour atteint la maturité opérationnelle du système décrit dans ce document. Ce n’est pas une raison pour se déclarer vaincu : c’est une raison pour traiter cet écart comme ce qu’il est réellement — une urgence stratégique. Et le temps pour l’adresser sérieusement se comprime à mesure que la dépendance s’approfondit.

 La Capture Silencieuse

NOTES ET RÉFÉRENCES

[1] Weinberger, Sharon. Project Maven: A Marine Colonel, His Team, and the Dawn of AI Warfare. Publication annoncée en 2026. Toutes les données factuelles citées — 250

utilisateurs en huit semaines (Camp Leatherneck, Afghanistan, 2011) ; montée en capacité de cent à cinq mille cibles analysées par jour avec intégration de grands modèles de langage ; début d'utilisation par la structure concernée au printemps 2025 ; dix nations en attente en octobre 2025 — sont tirées de cette enquête. L'auteure, ancienne rédactrice en chef de Defense One et de Jane's, a conduit plusieurs centaines d'heures d'entretiens avec officiers, ingénieurs, contractants et responsables politiques.

[2] Kahneman, Daniel. Thinking, Fast and Slow. Farrar, Straus and Giroux, 2011. Chapitre 7 (« The Magic of Priming ») et chapitre 12 (« The Science of Availability ») : sur l'effet de halo et son rôle dans les jugements rapides sous incertitude. Cialdini, Robert B. Influence : Science and Practice. 5e édition, Pearson, 2009 : sur les biais d'autorité et de similitude dans les contextes de décision organisationnelle.

[3] Le « cadrage de la contingence zéro » est une catégorie analytique utilisée ici pour décrire la présentation d'une technologie comme condition sine qua non de la survie opérationnelle. Voir plus largement : Payne, Kenneth. I, Warbot: The Dawn of Artificially Intelligent Conflict. Hurst, 2021. Brooks, Rosa. « Drones and the International Rule of Law ». Georgetown Journal of International Law, 2014. Roff, Heather. « The Strategic Robot Problem: Lethal Autonomous Weapons in War ». Journal of Military Ethics, 2014.

[4] Sur les mécanismes de mobilité croisée entre secteur de défense et industrie privée (revolving door) : Hartung, William D. Prophets of War: Lockheed Martin and the Making of the Military-Industrial Complex. Nation Books, 2011. Pour le cadre déontologique applicable aux organisations multilatérales de défense, se reporter aux dispositions pertinentes des règlements intérieurs sur les conflits d'intérêts et les périodes de carence.

[5] Bachelard, Gaston. La Formation de l'esprit scientifique. Vrin, 1938. Concept d'obstacle épistémologique : la connaissance établie comme résistance active à la connaissance nouvelle.

[6] Arquilla, John et Ronfeldt, David (dir.). In Athena's Camp: Preparing for Conflict in the Information Age. RAND Corporation, 1997. Notamment le chapitre sur la vulnérabilité cognitive des organisations militaires en environnement d'information structurée. Boyd, John R. A Discourse on Winning and Losing. Non publié, 1987 :

cycles OODA et conditions de la supériorité décisionnelle. Thaler, Richard H. et Sunstein, Cass R. Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press, 2008.

Document de doctrine et d’analyse stratégique