ÉTUDES
DE L'IFRI

LABORATOIRE DE RECHERCHE SUR LA DÉFENSE FOCUS STRATÉGIQUE n° 118

MAI
2024

« De l'autre côté de la colline »
Atouts et fausses promesses de la transparence du champ de bataille

Guillaume GARNIER
Pierre NÉRON-BANCEL

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une fondation reconnue d'utilité publique par décret du 16 novembre 2022. Elle n'est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0872-6

Couverture : Char Stridsvagn 122 équipé du système de camouflage mobile (MCS) 'Barracuda' de SAAB AB © SAAB AB

Comment citer cette publication :

Guillaume Garnier et Pierre Néron-Bancel, « "De l'autre côté de la colline". Atouts et fausses promesses de la transparence du champ de bataille », *Focus stratégique*, n° 118, Ifri, mai 2024.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Comité de rédaction

Auteurs

Pierre Néron-Bancel est officier de l'armée de Terre inséré au sein du Laboratoire de recherche sur la défense (LRD) du Centre des études de sécurité de l'Ifri, où ses travaux portent sur les enjeux sécuritaires et stratégiques français et plus spécifiquement, sur l'étude des nouvelles conflictualités, l'évolution des formes de l'engagement aéroterrestre et les enjeux stratégiques de l'emploi des forces terrestres. Diplômé de l'École spéciale militaire de Saint-Cyr, il est breveté de l'École de guerre ainsi que de l'*Advanced Command and Staff Course* britannique.

Guillaume Garnier est chercheur associé au Centre des études de sécurité de l'Ifri. Il a été officier inséré au sein du Laboratoire de recherche sur la défense (LRD) de 2012 à 2014. Il est breveté de l'École de guerre et titulaire d'un Master 2 de géopolitique de l'Institut français de géopolitique (Paris 8). Il a occupé divers postes de coordination ou de conception en France et à l'étranger (Tchad, Turquie, Belgique) et contribué aux travaux relatifs à la *Revue Stratégique de Défense et de Sécurité Nationale 2017*, comme chef de bureau à la Direction générale des relations internationales et de la stratégie (DGRIS).

Résumé

Les conflits récents ont mis en lumière une caractéristique du champ de bataille contemporain, inédite par son ampleur et ses effets sur la conduite des opérations : la « transparence ». Celle-ci se définit comme la capacité à acquérir et exploiter une connaissance géolocalisée et en temps quasi réel d'un environnement opérationnel donné, garantie par une architecture de connectivité mettant en réseau des capteurs hétérogènes et redondants, des systèmes de traitement de données de masse et des effecteurs.

Cependant, la clarté visuelle acquise par la technologie ne garantit pas pour autant la clarté cognitive qui permettrait de comprendre les intentions de l'adversaire, voire de prédire ses actions. Ainsi, cette étude propose une approche raisonnée de la transparence, qui tient compte de la dialectique permanente entre transparence et opacité, entre connaissance et ignorance. À ce titre, la transparence doit être considérée comme le fruit d'une lutte pour la maîtrise de la supériorité informationnelle. Elle est avant tout une potentialité à conquérir, défendre ou interdire, au même titre que les supériorités de milieu.

La nécessité de savoir a toujours fait partie des besoins fondamentaux du chef militaire. Cette quête de la connaissance a bénéficié de l'évolution des techniques, garantissant progressivement au chef tactique une visibilité croissante de son environnement opérationnel. Au début du XXIe siècle, la révolution de la connectivité a ouvert un nouveau pan de l'histoire militaire, donnant corps à l'ambition de déchirer le brouillard de la guerre. Portant les promesses d'un nouvel art de la guerre qui reléguerait aux oubliettes les anciens principes et procédés, cette transparence inédite a pourtant généré ses propres illusions : la perfection de la connaissance, l'instantanéité décisive des effets, la fin de la friction… Remise à sa juste place, la transparence apparaît comme le résultat espéré d'un modèle capacitaire conçu autour de la donnée, articulé à partir d'un réseau de connectivité organisé pour capter, fusionner, stocker et diffuser cette donnée.

Décuplant la létalité du champ de bataille terrestre, mettant fin à la protection des zones arrières, interrogeant les principes mêmes de discrétion dans tous les milieux et champs, de dissimulation, de concentration des forces et de surprise tactique, la transparence remet en cause un certain nombre d'acquis du combat.

Elle influence radicalement la conflictualité à venir par les effets qu'elle produit sur les processus de commandement, tiraillés entre l'exigence de l'hyperconnectivité et la nécessité de disparaître du champ électromagnétique, et le nouveau rapport qu'elle induit vis-à-vis de

l'information et de la décision – rapport lui-même influencé par la tyrannie de l'immédiateté et l'accès partagé à l'information permanente en temps quasi réel.

La transparence du champ de bataille contemporain n'est cependant pas uniforme ni avérée selon le milieu. Étant donné leur disparité et leur résistance différenciée à la détection, il apparaît plus réaliste de parler de « transparences » en adaptant la réalité de ce concept aux caractéristiques propres à chaque espace de conflictualité.

Les progrès exponentiels des capacités techniques de recueil du renseignement, qui s'expriment dans des champs technologiques aussi variés que ceux des drones, des radars et des satellites, rendent possible une forme de « continuum de surveillance ». La précision, la permanence et la redondance des capteurs de tous types, couplés à des phénomènes nouveaux comme l'explosion du recours au renseignement de source ouverte (OSINT), donnent le sentiment que la transparence est devenue un phénomène indépassable. L'innovation technologique galopante touche également les outils d'exploitation de l'information, par essence cognitive, grâce l'intelligence artificielle (IA).

Le progrès technologique ne favorise cependant pas que la transparence mais fait évoluer également les moyens de favoriser l'opacité, à travers trois familles techno-capacitaires : la dissimulation, la métamorphose et la perturbation des capteurs. De même, de nouvelles possibilités techniques de manipulation de l'information peuvent dégrader les progrès du volet analyse. Dans cette dialectique techno-capacitaire, il existe une prime à la transparence dans le champ physique qui s'oppose à une opacité dans le champ cognitif.

À l'avenir, le rapport transparence-opacité devrait donc être fluctuant et dépendra fondamentalement de l'investissement que les principales puissances militaires seront prêtes à y consentir et des percées technologiques. Malgré les atouts qu'elle offre, la transparence restera limitée par les erreurs humaines d'interprétation, la dissimulation voire la déception adverse, et par son coût, qui pourrait handicaper un modèle de force en rendant son utilisateur simple spectateur du champ de bataille.

Trois approches principales se distinguent pour repenser la manœuvre en tenant compte de cette nouvelle réalité du champ de bataille. Le premier enjeu est d'abord de survivre avant même de manœuvrer et de combattre. Recréer une forme d'opacité suppose donc de retrouver les moyens d'échapper à la détection en se réappropriant les fondamentaux tactiques que sont la dissimulation, la discrétion et la dispersion en misant sur la protection, la mobilité et le brouillage.

La deuxième approche vise à conquérir la supériorité opérationnelle, ce qui implique pour les armées françaises de parvenir à maîtriser les exigences du combat multi-milieux/multi-champs (M2MC), d'adapter leurs processus

de renseignement à l'hyperconnectivité sans le réduire aux seules fins du ciblage cinétique, et enfin de rattraper le retard pris sur le segment drones.

En définitive, combattre dans un champ de bataille de plus en plus transparent rend nécessaire de repenser la surprise en inventant de nouvelles formes de manœuvre. Quelle que soit sa forme, la manœuvre pourrait reposer sur la réalisation de « couloirs d'opacité », cadre espace-temps d'optimisation des effets d'aveuglement de l'adversaire qui pourrait ensuite être exploité par une manœuvre privilégiant la saturation de l'adversaire et la vitesse d'exécution.

De cette nouvelle réalité tactique et opérative ressort de nombreuses implications stratégiques sur l'ensemble du spectre de la conflictualité.

Dans le champ de l'affrontement, l'accès facilité à l'information porte en lui le risque de la montée aux extrêmes en rendant davantage accessible la tentation de la frappe préemptive.

Dans le volet de la contestation, les modes d'agression dits hybrides, sous le seuil du conflit armé, conservent un bon rapport coût-efficacité pour les États souhaitant remettre en question le *statu quo* international, l'opacité l'emportant sur la transparence dans ce champ.

Enfin, il est possible pour les adversaires infra-étatiques de contourner les avantages comparatifs des armées étatiques en termes de transparence, notamment en exploitant les milieux opaques et en utilisant la démocratisation de la transparence à leur profit.

Executive summary

Recent conflicts have highlighted a key character of contemporary warfare, unprecedented in its scale and impact on the conduct of operations: the so-called 'battlefield transparency'. Transparency is defined as the ability to acquire and exploit geolocated, near-real-time awareness of a given operational environment, guaranteed through a connectivity architecture networking a heterogeneous and redundant array of sensors, big data computing capability and effectors.

However, the visual clarity guaranteed by technology does not lead automatically to the cognitive clarity that is required to understand an opponent's intentions, or even to predict his actions. This study espouses a balanced approach to transparency that reflects the irreducible dialectic between transparency and opacity, between knowledge and ignorance. In that regard, transparency must be seen as the fruit of the fight for information superiority. It is primarily a potentiality that needs to be won, protected or denied in the same way as superiority in any of the physical domains.

The search for knowledge has always been one of the fundamental needs of the military leader. This quest for awareness has benefited from the evolution of technology, gradually guaranteeing the tactical leader an increased visibility of his operational environment. At the beginning of the 21st century, the digital revolution opened a new chapter in military history, promising to fulfill a long-held ambition of tearing through the fog of war. While it held out the promise of a new way of war that would consign the old principles and procedures to oblivion, this unprecedented transparency also generated its own illusions: perfection of knowledge, instantaneous decisiveness of effects, end of friction... Put at its rightful place, transparency appears to be the expected result of a capability model designed for data based on a connectivity network organized to collect, fuse, store, and disseminate this very data.

As it drastically enhances lethality on the land battlefield, as it puts an end to the safety of the rear, as it questions the very principles of stealth in every domain, of concealment, of concentration of forces, then of tactical surprise, transparency challenges several established combat principles.

It drastically weighs on the character of future conflict by the way it affects command and control processes, torn between the demand for hyperconnectivity and the need to disappear from the electromagnetic field, but also by the new relationship it induces to information and decision-

making, affected by the tyranny of immediacy and the shared access to permanent, near real-time information.

However, transparency on the contemporary battlefield is neither homogeneous nor proven across all domains. Given their disparity and their own resistance to detection, referring to 'transparencies' would be more adapted as it would consider the specific characteristics of each warfighting domain.

The exponential progress in Intelligence, Surveillance and Reconnaissance (ISR) capabilities, expressed in technological fields as varied as drones, radar or satellites, allows for permanency of observation and surveillance. Performance, permanency and pervasiveness of sensors of all kinds, coupled with new trends such as the increasing recourse to open-source intelligence (OSINT), advocate for making battlefield transparency a permanent and inescapable feature of war. Rampant technological innovation is also affecting data analysis, which is essentially a cognitive process, thanks to the development of artificial intelligence (AI).

However, technological progress does not only enhance transparency but also affect to means that create opacity, through three techno-capability families: concealment, transformation, and sensor disruption. Similarly, new technical possibilities for information manipulation can undermine progress in data fusion. In such a technology-driven dialectic, transparency gets a premium in the physical field, but opacity comes first in the cognitive field.

In the future, the balance between transparency and opacity will remain inconsistent and will fundamentally depend on how much the main military powers are willing to invest as well as on technological breakthroughs. Despite its advantages, transparency will remain limited by human errors in interpretation, adversary concealment or deception. Above all, its cost will be a decisive factor that could hinder a whole force model, making its user a mere spectator of the battlefield.

Three main approaches stand out for rethinking manoeuvre considering the new battlefield reality. The first challenge is to survive even before maneuvering and fighting. Then, recreating a way for opacity means finding ways to evade detection by re-embracing tactical fundamentals: concealment, secret and dispersion, while focusing on protection, mobility and jamming.

The second approach aims to achieve information superiority, which requires the French armed forces to overcome the challenges of Multi-domain Operations (MDO), to adapt their intelligence processes to hyperconnectivity without restricting enhanced awareness to a kinetic approach, and eventually to catch up on the drone segment.

Last, fighting on an increasingly transparent battlefield requires to think back on surprise by imagining new forms of manoeuvre. Whatever form it would take, the maneuver could rely on creating 'corridors of opacity,' space-

time frames that would optimize the effects that contribute to blind an adversary, which could then be exploited by movement focusing on saturation and speed.

This new tactical and operational reality entails many strategic challenges across the full spectrum of conflict.

In the field of confrontation, easier access to information bears the risk of rising to extremes because of an enhanced temptation to recourse to preemptive strikes are more.

In the realm of contestation, the so-called hybrid warfare that rages below the threshold of conflict offers good value for money for states willing to challenge the international status quo, as opacity is prevailing over transparency in this field.

Last, non-state adversaries can bypass the comparative advantages of state armies that transparency offers, notably by exploiting opaque environments and by turning the democratization of transparency to their advantage.

Sommaire

Introduction

Au mois de mai 2022, un bataillon motorisé russe a été intégralement détruit alors qu'il était en train d'établir un site de franchissement sur la rivière Donets, perdant plus de 70 véhicules blindés et presque 500 hommes. Le site avait préalablement été repéré par un drone ukrainien, ce qui a permis de guider précisément les frappes d'artillerie sur les concentrations de troupe en amont et en aval des ponts flottants[1]. Au-delà des commentaires sur les fautes tactiques des forces armées russes, certains ont souligné que « la surveillance ubiquitaire du champ de bataille » ne laissait désormais « aucune possibilité aux unités relativement importantes pour se cacher[2] », concluant à la fin de la surprise tactique. En effet, l'impossibilité pour les belligérants de dissimuler leurs moyens sur le champ de bataille ukrainien à cause d'une profusion de capteurs en tout genre sur l'ensemble du front est l'une des leçons les plus communément admises par l'ensemble des analystes[3]. Toutefois, cette capacité inédite des deux camps à voir le dispositif adverse ne leur a épargné depuis deux ans ni erreurs de jugement, ni fautes tactiques lourdes, ni même défaillances de commandement.

La « friction », selon la définition qu'en donne Clausewitz, reste une réalité du champ de bataille au même titre que l'incertitude, maximisée par le hasard et la nature interactive de la guerre. Pour preuve, l'incapacité du renseignement israélien à anticiper et déceler l'attaque du Hamas le 7 octobre 2023 procède de ces mêmes défaillances et semble montrer au contraire que la surprise reste une option aussi bien stratégique que tactique. Malgré un système redondant de surveillance doté des moyens technologiques les plus avancés, le Hamas a su contourner les capteurs et les systèmes d'alerte israéliens pour tromper son adversaire sur ses capacités réelles et exploiter pleinement l'effet de sidération provoqué par son attaque surprise. L'échec israélien relève d'abord d'un défaut d'imagination, la quantité de données accumulées ne pouvant jamais valoir ni la qualité des données collectées ni la qualité de leur exploitation[4].

---

1. T. Fouillet, « Guerre en Ukraine : étude opérationnelle d'un conflit de haute intensité (premier volet) », *Recherches & Documents N°02/2023*, Fondation pour la recherche stratégique, 2023, p. 50.
2. D. Johnson, « Would We Do Better? Hubris and Validation in Ukraine », *War on the Rocks*, 31 mai 2022, disponible sur : https://warontherocks.com.
3. « Les 7 enseignements stratégiques de la guerre en Ukraine », Ministère des armées, 26 février 2024, disponible sur : www.defense.gouv.fr ; voir aussi M. Zabrodskyi, J. Watling, O. Danylyuk et N. Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*, Londres, RUSI, 2022.
4. Entretien avec un officiel israélien expert du renseignement, 19 novembre 2024.

Ces deux exemples contradictoires en apparence questionnent la réalité de ce qu'il est convenu de dénommer aujourd'hui la « transparence du champ de bataille ». Cette métaphore, dont l'usage remonte à la formalisation des doctrines américaines de la guerre en réseau des années 1990 (*Network Centric Warfare*), cherche à transcrire la visibilité inédite des éléments du champ de bataille obtenue grâce aux progrès sans précédent des technologies de l'information et de la communication :

> « En exploitant la technologie satellitaire et l'internet, les capteurs – du téléphone portable quotidien qui prolifère en Ukraine aux drones – en utilisant l'IA et l'apprentissage automatique pour exploiter les énormes volumes de données que nous collectons, nous avons vu le champ de bataille devenir transparent. »[5]

Cette transparence est le produit de la mise en réseau des données collectées dans un environnement opérationnel et de leur partage en temps utile à l'ensemble des acteurs du réseau. Elle repose sur un système de capteurs, des capacités de fusion et d'analyse de l'information et une architecture réseau, trois segments animés par une dynamique d'innovation technologique ininterrompue depuis les années 1980. Le choix du terme « transparence » s'explique par contraste avec le « brouillard de la guerre » qu'elle cherche à lever, métaphore dont use Clausewitz pour illustrer à la fois le manque de clarté et la distorsion due à l'incertitude inhérente à la guerre :

> « À la guerre, les trois quarts des facteurs sur lesquels repose l'action sont enveloppés dans un brouillard d'incertitude plus ou moins profonde [...] toute action prend place pour ainsi dire dans une certaine pénombre qui, comme le brouillard ou le clair de lune, tend souvent à donner aux choses une apparence grotesque ou à les faire apparaître plus large qu'elles ne sont. »[6]

L'augmentation significative de la visibilité, au sens météorologique du terme, permettrait ainsi de « percer le brouillard de la guerre, c'est-à-dire avoir une forme de transparence du champ de bataille[7] ». Elle s'oppose de fait à l'opacité naturelle de la guerre caractérisée par la lacunarité et l'imprécision de l'information dans l'environnement opérationnel. Le recours à une propriété physique pour décrire ce phénomène est cependant problématique à double titre : d'une part, il déforme le sens initial du mot « transparence », qui définit en sciences physiques la propriété d'un corps laissant passer la lumière et permettant de voir à travers lui les objets avec netteté[8]. Cette définition s'accommode bien des milieux sous-marin ou aérien par exemple, que l'on cherche à transpercer, mais n'a que peu de sens

5. P. Sanders, Discours du Chief of the General Staff à l'International Armed Vehicles Conference, janvier 2023.
6. C. von Clausewitz [trad. P. Paret et M. Howard], *On War*, Oxford, Oxford University Press, 2007, p. 46 et 88-89.
7. P. Samama, « Connecté et robotique : à quoi pourrait ressembler le char du futur de l'armée française », BFM TV, 24 octobre 2023, disponible sur : www.bfmtv.com.
8. « Transparent », *Larousse,* disponible sur : www.larousse.fr.

dans son application au milieu terrestre. D'autre part, il laisse penser que la transparence serait devenue une propriété intrinsèque du champ de bataille contemporain, alors qu'elle est le résultat d'un processus à renouveler en permanence, celui d'un système complexe de captation et de traitement de l'information. Cette fragilité de la transparence en fait un objectif plus qu'une caractéristique. Elle doit se conquérir et nécessite en retour de se protéger de la transparence acquise par l'adversaire.

La nature dialectique de la guerre s'applique en effet également à la transparence, au rebours du concept de *Network Centric Warfare* qui reposait sur le postulat informulé que la transparence ne serait l'apanage que des seules forces américaines. Non seulement les technologies de la transparence ne sont pas exclusives, mais encore les efforts pour dégrader la compréhension de l'adversaire sont réciproques. Plus fondamentalement, la transparence continue de véhiculer un certain nombre de mythes issus de l'époque de sa formalisation dans les années 1990, qui entretiennent les illusions sur sa capacité à révolutionner la décision. Ces illusions reposent sur la transcription injustifiée de la clarté visuelle acquise par la technologie en une clarté cognitive qui garantirait la compréhension des actions voire des intentions de l'adversaire. On atteint ici les limites du concept de transparence, qui est bien la négation de l'opacité et non pas de l'incertitude. Si la connaissance accumulée et partagée peut contribuer à réduire l'opacité, l'incertitude reste une donnée fondamentale de la guerre, intrinsèquement liée à la nature humaine de la conflictualité.,

En tenant compte de la réalité d'une visibilité inédite de l'environnement opérationnel, tout en restant dans les limites conceptuelles de l'incertitude, on peut définir la transparence comme la capacité à acquérir et exploiter une connaissance géolocalisée et en temps quasi réel d'un environnement opérationnel donné, garantie par une architecture de connectivité mettant en réseaux des capteurs hétérogènes et redondants, des systèmes de traitements de données de masse et des effecteurs. La dimension révolutionnaire de ce nouveau paradigme doit être interrogée, pour mesurer à quel point la supériorité informationnelle qu'elle induit est réellement décisive, et jusqu'où elle remet en cause les modes opératoires des armées contemporaines.

Cette étude défend une approche raisonnée de la transparence, comme le fruit d'une lutte pour la maîtrise de la supériorité informationnelle. La transparence doit être vue comme une potentialité à conquérir, défendre ou interdire, en considérant la supériorité informationnelle au même titre que les supériorités de milieu. Elle ne peut être absolue et est forcément contrainte dans l'espace et le temps. Elle reste le résultat d'un compromis dans la dialectique entre compréhension et ignorance, recherche du sens et privation des sens.

Comprendre les ambitions, la portée et les limites du concept de transparence nécessite au préalable d'effectuer un tour d'horizon historique et conceptuel de la quête de la visibilité et de la connaissance de l'environnement opérationnel. Cette première étape permet également d'analyser ce que l'avènement de la transparence modifie dans la manière de conduire la guerre, tout en s'attachant à différencier la réalité de cette transparence de l'environnement opérationnel selon les milieux physiques. Une analyse approfondie des capacités de renseignement et d'analyse, mais également en contrepoint des technologies de leurrage et d'intoxication permet ensuite de mettre en lumière la nature profondément dialectique de la lutte pour la transparence. Une troisième partie permet d'exploiter cette dialectique pour dégager des pistes et des recommandations visant à se prémunir de la transparence adverse, la conquérir ou en jouer dans une redéfinition de la supériorité informationnelle. Enfin, la dernière partie détaille comment la compréhension des enjeux de la transparence se décline nécessairement au niveau stratégique sur l'ensemble du spectre de conflictualité et comporte notamment une dimension escalatoire, du fait de l'association entre détection, vélocité et létalité.

Tout voir pour gagner à coup sûr : un rêve ancien, un concept récent

La quête de la connaissance a toujours fait partie des besoins fondamentaux du chef militaire engagé au combat. Cinq cents ans avant notre ère, Sun Tzu identifiait déjà la connaissance de soi-même, de ses troupes, de son environnement et de son adversaire comme l'atout maitre du général pour le conduire à la victoire[9]. Encore aujourd'hui, l'armée de Terre fait de la « compréhension » l'un des huit « facteurs de supériorité opérationnelle » nécessaire pour dominer un adversaire et vaincre au combat[10] Ce besoin de savoir consomme ainsi une grande partie des actions du combat, comme l'avait formulé le général anglais Wellington :

> « Toute l'affaire de la guerre, en fait toute l'affaire de la vie, consiste à s'efforcer de découvrir ce que l'on ne sait pas à partir de ce que l'on sait : c'est ce que j'ai appelé "deviner ce qu'il y a de l'autre côté de la colline". »[11]

Le besoin de voir pour comprendre a longtemps contenu la bataille dans un espace restreint, que le général en chef pouvait embrasser d'un regard. Entre les engagements en revanche, l'ignorance prévalait. Les progrès techniques conjugués ont progressivement d'abord, puis brutalement dilaté l'espace de bataille et ont d'autant augmenté le désir de voir plus loin, plus précisément, plus longtemps. Au début du XXIe siècle, la révolution de la connectivité a ouvert un nouveau pan de l'histoire militaire, donnant corps à l'ambition de déchirer le brouillard de la guerre qui avait si longtemps tenu en échec les plus grands chefs militaires. Portant les promesses d'un nouvel art de la guerre qui reléguerait aux oubliettes les anciens principes et procédés, cette transparence inédite a pourtant généré ses propres illusions. Replacer les évolutions techniques récentes dans le temps long de l'Histoire s'avère ainsi nécessaire pour distinguer en quoi et jusqu'où les nouvelles technologies transforment réellement l'engagement tactique.

9. Sun Tzu (éd. S.Griffith), *L'art de la guerre*, Flammarion,1ère ed. 1972, édition revue 2008, p. 213 à 222.
10. « Action terrestre future », État-major de l'armée de Terre, 2016, p. 25-27.
11. Duc de Wellington, cité dans J. Croker, L. J. Jennings (eds.), *The Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, Secretary of the Admiralty from 1809 to 1830*, Vol. III, Ulan Press, 2012 [1885], p. 276-277.

La transparence sur le temps long, un Graal insaisissable

Entre transparence tactique et opacité stratégique

Le brouillard de la guerre figure parmi les principes fondamentaux de Clausewitz, suggérant que le champ de bataille a toujours été nébuleux. Cependant, un rapide survol sur le temps long laisse plutôt penser le contraire. Le champ de bataille, pris au sens classique du terme comme un terrain de dimensions limitées[12] où s'affrontent plusieurs protagonistes, a généralement été un espace où l'essentiel du dispositif adverse était observable. Si le commandant en chef pouvait embrasser du regard – aidé de la « longue-vue » à partir du XVII[e] siècle – la majeure partie du champ de bataille, à condition de se positionner au bon endroit, il pouvait être induit en erreur par son adversaire ou interpréter à tort son intention. Ainsi, la capacité à localiser son adversaire et celle de prévoir sa conduite ne sont pas corrélées. Nombreux sont les exemples de ruses de guerre, fausses fuites pour attirer un adversaire trop bien positionné, feintes d'attaque, diversions, ayant permis une nette victoire alors même que l'essentiel du dispositif adverse était connu[13]. Une transparence quasi totale, comprise comme vision du dispositif ennemi, ne prédétermine donc pas l'issue d'un combat. L'interprétation de la séquence d'événements, la contingence (la « friction » de Clausewitz), la cohésion des troupes, la lucidité des chefs en présence sont autant de facteurs « immatériels » qui viennent altérer une équation « matérielle » (distances, puissance de feu, configuration du terrain, nombre d'hommes par rapport à la surface occupée…) en apparence simple à appréhender. Quel que soit le degré de transparence physique du champ de bataille, l'incertitude demeure donc et rend l'affrontement incertain. On « livre bataille », acceptant par là une part de hasard, même si les dispositions les plus minutieuses ont pu être arrêtées au préalable.

La guerre de siège est également relativement transparente. Le lieu de l'affrontement est par définition circonscrit. On connaît souvent, même approximativement, le volume de la garnison, on devine l'état des réserves alimentaires et d'eau potable, données matérielles qui ont pu être collectées par des informateurs. Il est plus difficile en revanche d'évaluer le moral de la garnison et plus encore celui des habitants : quel degré de privations sont-ils prêts à endurer et pendant combien de temps ?[14] Ici encore, la connaissance des données physiques ne présume pas de la victoire, dont l'issue dépend

12. Par exemple, un quadrilatère d'environ 2 km x 3,5 km pour Waterloo. Il est vrai que ce champ de bataille est plus réduit que la moyenne de l'époque. Voir J. Macdonald, *Les Grandes Batailles de l'histoire mondiale*, Paris, Albin Michel, 1985.
13. J. Latimer, *Deception in War*, New York, Overlook Press, 2001.
14. Voir V. Melegari, *Great Military Sieges*, Londres, Ferndale Editions, 1981.

souvent aussi de données psychologiques (la volonté, la cohésion, le *bluff*[15]). Les caprices du sort (météo, épidémies) renforcent l'incertitude.

Si la transparence physique prévaut au niveau tactique sur le temps long de l'histoire militaire, le rapport transparence-opacité est plus ambigu aux échelles opérative et stratégique. Le général Beaufre rappelle que, jusqu'à la fin du XVIIIe siècle, une armée se déplace d'un seul bloc, pour des raisons de sûreté et de logistique[16]. Cela facilite sa détection par un parti de cavaliers légers, rendant difficile la surprise opérative. L'invention du principe divisionnaire par le Comte de Guibert, perfectionné par le système napoléonien organisé en corps d'armée, permet de fluidifier les déplacements de corps autonomes à l'échelle du théâtre des opérations. Dès lors, l'opacité regagne l'avantage sur la transparence du fait de la difficulté à localiser chacun de ces grands mobiles. Quand bien même certains d'entre eux le seraient, cela n'en dit généralement pas assez de la manœuvre d'ensemble. *Quid* du lieu de concentration de la masse de manœuvre ? Y a-t-il une fraction des forces engagées dans un mouvement enveloppant ? Doit-on profiter du relatif isolement d'un corps ou s'agit-il d'un appât, les autres étant à bonne distance pour se concentrer « au son du canon » ? La présence d'unités légères de reconnaissance, en avant-garde ou flanc-garde, ne permet généralement pas de lever toutes ces indéterminations. Avec le système napoléonien, bientôt imité par toutes les puissances, le rapport transparence-opacité est ainsi altéré.

Jusqu'à cette époque donc, il n'y a pas de caractère intangible dans ce rapport, mais ses fluctuations rendent compte d'une transparence qui se manifeste plutôt à l'échelle tactique alors que l'opacité demeure importante à l'échelle stratégique, par manque de moyens de recueil (les espions demeurant le moyen essentiel).

Des progrès technologiques s'accélérant de la fin du XVIIIe siècle à la guerre froide

Les progrès techniques, d'abord timides, tendent quant à eux vers davantage de transparence. Le ballon à gaz[17] de la bataille de Fleurus (1794), réutilisé au siège de Mayence (1795) aide à observer les mouvements et affecte le moral des troupes adverses se sachant épiées. Le télégraphe Chappe par sémaphores (à partir de 1794) permet une accélération de la diffusion des informations, l'un des facteurs de la transparence, et ce sur de longues distances. Ce procédé se perfectionne tout au long du XIXe siècle, en particulier avec la guerre de Sécession voyant converger les progrès

15. Cas d'un assiégé qui feint (communication) d'être dans une situation confortable (vivres ou arrivée d'une pseudo-armée de secours) ; à l'inverse, menace d'exécutions de masse si l'assiégé ne se rend pas immédiatement, quasi systématiquement brandie par les Mongols notamment (lire T. May, « The Mongol Art of War », Barnsley, Pen and Sword Military, janvier 2007.
16. A. Beaufre, *Introduction à la stratégie*, Paris, Pluriel, 2012, p. 82-84.
17. « L'Entreprenant ».

techniques et opérationnels à la fois du télégraphe et des ballons. Les dirigeables sont encore largement utilisés lors de la Première Guerre mondiale.

Justement, à partir de la Grande Guerre, les progrès se démultiplient, essentiellement à l'échelle tactique. Dès la bataille de Marne, des aéroplanes jouent un rôle important côté allié en repérant l'inflexion de la marche de la première armée allemande[18]. L'appareil photographique complète et prolonge très vite l'œil humain. Les progrès en matière de transmission radio (postes TSF émetteurs embarqués) permettent ensuite de raccourcir la boucle détection-traitement du renseignement (réglage des tirs) – déclenchement des feux de l'artillerie. Ces gains en matière de détection concernent surtout l'échelle tactique, l'aviation étant peu capable d'opérer dans la profondeur[19]. Du reste, les progrès concernent aussi le camouflage, dans le domaine terrestre comme naval[20]. L'interception des communications adverses, transitant notamment par les câbles télégraphiques sous-marins, constitue un élément nouveau. D'une manière générale, la dialectique « du glaive et du bouclier » se manifeste pleinement dans le domaine de la cryptologie (codage des informations), puisque la volonté d'écouter l'adversaire, comme de se protéger de ses écoutes, conduit à des évolutions techniques constantes. Cette compétition sur le spectre électromagnétique se conjugue d'ailleurs à tous les niveaux, du tactique au stratégique. Là encore, la dialectique de cette « guerre du chiffre » ne permet pas à elle seule d'influer sur l'issue de ce conflit[21], mais une fenêtre de supériorité technique peut accorder un avantage important sur une phase donnée[22].

Il serait trop long de revenir sur l'ensemble des évolutions enregistrées au cours du Second conflit mondial. On peut citer l'amélioration technique des capacités de reconnaissance dans les trois milieux terre, air, mer, en particulier motivée dans le domaine aéronaval par l'immensité du théâtre Pacifique rendant difficile la détection des flottes. La rupture technologique que représente l'utilisation des radars mérite aussi d'être soulignée, ceux-ci jouant un rôle déterminant dès la bataille d'Angleterre de 1940[23]. Également, l'apparition de l'Asdic (*Anti-Submarine Detection Investigation Committee*), perfectionné en sonar (*Sound Navigation And Ranging*), change la nature de la lutte anti-sous-marine. Pour se soustraire à la détection adverse ou induire ce dernier en erreur, les opérations de

18. M. Goya, *S'adapter pour vaincre, comment les armées évoluent*, Paris, Perrin, 2019, p. 63-64.
19. À l'exception des bombardiers lourds.
20. Notamment, techniques de peinture zébrée (*dazzle*) des bâtiments navals pour en casser les formes.
21. Cette guerre du chiffre jouera un rôle plus significatif encore au cours du Second conflit mondial avec la machine Enigma permettant de décoder les communications allemandes.
22. Ainsi, le polytechnicien Georges Painvin parvenant à décoder un message allemand, le quartier général de Foch peut déjouer l'offensive déclenchée le 2 juin 1918 près de Compiègne. Également, l'interception du célèbre télégramme Zimmermann, fomentant un complot allemand utilisant le Mexique contre les intérêts américains, contribue à l'entrée en guerre des États-Unis.
23. M. Williamson, *Les Guerres aériennes, 1914-1945*, « Atlas des guerres », Paris, Autrement, 2000.

déception[24] atteignent un niveau de sophistication inédit par leur ampleur ou leur technicité, qu'il s'agisse de cacher de grandes masses d'unités (*maskirovka* soviétique[25]), ou de mettre au point une manœuvre d'ensemble de niveau stratégique combinant l'ensemble des processus de déception[26] (dissimulation, simulation, intoxication) : l'opération Fortitude[27] en est l'aboutissement ultime. Ainsi, même dans le cadre de concentrations gigantesques de moyens, la transparence du champ de bataille peut être altérée[28].

La guerre froide va ajouter peu à peu l'élément spatial à l'équation. Stimulé initialement par l'ardente nécessité de détecter le lancement de missiles nucléaires intercontinentaux, le développement des satellites militaires concerne ensuite d'autres applications opérationnelles : renseignement (écoutes, imagerie optique ou radar), météorologie, télécommunications sécurisées à longue distance, géolocalisation vers la fin de cette période (système GPS).

Il ressort de cet aperçu historique que la question de la transparence se décline différemment aux niveaux tactique, opératif et stratégique. Elle s'inscrit pleinement dans la dialectique du glaive et du bouclier (un progrès donné étant souvent contrecarré par un autre), traduisant une versatilité du rapport transparence-opacité. Enfin, « voir » (ou « écouter ») ne signifie pas « comprendre » la manœuvre adverse : l'erreur d'interprétation reste toujours possible, résultant d'une mauvaise appréciation personnelle ou des subterfuges adroitement échafaudés par l'ennemi. Ces erreurs d'appréciation sont en outre favorisées par la multiplicité facteurs à prendre en compte, matériels comme immatériels, auxquels s'ajoute l'incertitude inhérente au combat.

L'avènement de la connectivité : quand la transparence devient possible

Network Centric Warfare – la RMA et le tournant de la connectivité

L'idée de l'avènement d'une « transparence » du champ de bataille apparaît avec le développement spectaculaire des nouvelles technologies de l'information et de la communication (NTIC) ainsi que des technologies de positionnement (GPS). Arrivant à maturité à la fin de la guerre froide, leur mise en système est théorisée par les promoteurs de la « révolution dans les

24. R. Hémez, *Les Opérations de déception. Ruses et stratagèmes de guerre*, Paris, Perrin, 2022.
25. Par exemple, l'opération Bagration (été 1944) aboutissant à l'écrasement du groupe d'armées Centre allemand.
26. Voir schéma II-5, « Les trois modes de la déception », p. 51 de cette étude.
27. Opération supervisée par Churchill lui-même et visant à leurrer les Allemands en rendant crédible un débarquement dans le Pas-de-Calais au lieu de la Normandie.
28. Consulter B. Whaley, *Stratagem: Deception and Surprise in War*, Boston, Artech House, 2007.

affaires militaires[29] » (RMA), qui identifient les ingrédients d'un nouvel art de la guerre dans la convergence des capacités d'acquisition et de traitement de l'information et la précision des effecteurs de ciblage. Dès les années 1970, le chef d'état-major de l'*US Army*, le général William Westmoreland (*US Army Chief of Staff* de 1968 à 1972), annonçait avec un sens aigu de l'anticipation un champ de bataille « soumis à une surveillance en temps réel ou quasi réel de tout type 24 heures sur 24 » sur lequel « les forces adverses [seraient] localisées, suivies et ciblées de manière quasi instantanée grâce à l'emploi de réseaux de données et d'une évaluation du renseignement assistée par ordinateur » ; le chef militaire serait « en permanence au courant de l'ensemble du panorama du champ de bataille » et pourrait « détruire tout ce qu'il localiserait grâce à des transmissions instantanées[30] ». Dans le même contexte, le colonel américain John Boyd modélise la prise de décision en argumentant que la supériorité opérationnelle dépend fondamentalement de la capacité d'un système à compléter sa boucle de décision plus rapidement que son adversaire. C'est la fameuse boucle OODA : « Observation, Orientation, Décision, Action », dont l'enjeu est de raccourcir le délai d'exécution entre l'observation et l'action[31].

Cette convergence par le réseau trouve sa première réalisation dans la guerre du Golfe de 1990-1991, dans laquelle la maîtrise technologique de la coalition menée par les Américains impose la suprématie du modèle de la guerre en réseau (*Network Centric Warfare*, théorisée à partir de 1998[32]). Celui-ci repose sur la connectivité et la vitesse du cycle de décision[33]. Les technologies de l'information confèrent à la coalition la « qualité des premiers[34] » : « premiers à voir, premiers à comprendre, premiers à agir[35] », qui lui permettent d'imposer son cycle décisionnel sur l'adversaire. La victoire sans appel de l'appareil américain contre l'armée irakienne valide le modèle et ouvre la voie à une nouvelle manière de conduire la guerre. Celle-ci porte l'ambition de la maîtrise de l'information à travers la recherche d'une transparence « totale » du champ de bataille, conférant au décideur une visibilité parfaite, permanente et en temps réel de son environnement opérationnel. La transparence, entendue donc comme la capacité à « tout

29. B. Tertrais, « Faut-il croire à la "révolution dans les affaires militaires ?" », *Politique étrangère*, vol. 63, n° 3, Ifri, septembre 1998, p. 611-629.
30. W. Westmoreland, « Battlefield of the Future », *US Army Aviation Digest* 16-2, Department of the Army, 1970.
31. Voir D. Fadok, *La Paralysie stratégique par la puissance aérienne,* Paris, Economica, 1998.
32. A. Cebrowski et J. Garstka, « Network-Centric Warfare: Its Origin and Future », *Proceedings*, vol. 124/1, janvier 1998 ; voir aussi M. Shurkin, R. Cohen et A. Chan, *French Army Approaches to Networked Warfare*, Santa Monica, RAND Corporation, 2022.
33. T. Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs*, Londres, Brassey's, 2004.
34. H. McNaster, « Continuity and Change: The Army Operating Concept and Clear Thinking About Future War », *Military Review*, 2015, p. 12.
35. TRADOC, TP 525-7-1, *The United States Army Concept Capability Plan for Unit Protection for the Future Modular Force, 2012-2024*, Version 1.0, US Department of the Army, 2007, p. 4.

voir dans une zone donnée[36] », devient une finalité opérationnelle, l'efficacité militaire se mesurant à la capacité de destruction immédiate d'un objectif repéré sous un rapport « équationnel[37] ».

À partir des années 2000, la RMA laisse la place à la *transformation*, dont les concepts consacrent la *total battlespace awareness* comme la clé de la domination de l'adversaire. C'est le cas par exemple du concept de « connaissance dominante du champ de bataille » (*Dominant Battlespace Knowledge*[38]) qui développe l'idée selon laquelle « le traitement automatisé de données, les technologies de captation de l'information et de télécommunication » s'intégreraient dans un système de systèmes qui conférerait à l'*US Army* la capacité d'obtenir « une connaissance dominante de l'espace de combat » à compter de 2005. De même, le concept de « *Rapid Dominance* » (domination rapide) de la doctrine « *Shock and Awe* » (choc et effroi) mise en œuvre en Irak en 2003, repose sur une « connaissance et une compréhension presque totales voire absolues de ses forces, de son adversaire et de l'environnement[39] ».

Les interventions de contre-insurrection vont pourtant mettre à mal la réalité de cette transparence. L'opacité demeure une caractéristique majeure des environnements de contre-insurrection dans lesquels les forces armées occidentales vont évoluer des années 2000 aux années 2020[40]. L'asymétrie annule le caractère décisif de la domination par l'information et pose les limites de l'approche hyper-technologique qui cherche à maîtriser la guerre par la connaissance parfaite des paramètres de l'environnement opérationnel[41]. À ce titre, la guerre du Golfe, occurrence exceptionnelle d'une « asymétrie informationnelle[42] », a contribué à fausser les perceptions sur l'aspect décisif de la supériorité informationnelle et technologique de la guerre en réseau.

La visibilité parfaite du champ de bataille : des espoirs aux illusions

Avec l'ambition de la domination de l'adversaire par l'information, le réseau devient le moyen pour faire de la donnée elle-même à la fois une arme, un levier et une cible[43], dans un nouveau modèle dit *data-centric warfare*. Cette ambition de la maîtrise de l'information porte quatre grands espoirs à travers

36. É. de Durand, « "Révolution dans les affaires militaires", "Révolution" ou "transformation" ? », *Hérodote 2003/2 N° 109*, 2003, p. 57-70.
37. J. Henrotin, « Les mutations du renseignement militaire, dissiper le brouillard de la guerre ? », *Focus stratégique,* n° 71, Ifri, janvier 2017.
38. S. Johnson, « DBK: Opportunity and Challenges », *in* S. Johnson et M. Libicki (dir.), *Dominant Battlespace Knowledge*, Washington D.C., National Defense University, 1996, p. 17-20.
39. H. Ullman, J. Wade *et al.*, *Shock and Awe, Achieving Rapid Dominance*, Washington D.C., National Defense University, 1996.
40. J. Henrotin, « Les mutations du renseignement militaire », *op. cit.*
41. P.-M. Léoutre, *Comment l'Occident pourrait gagner ses guerres*, Nancy, Le Polémarque, 2013.
42. T. Benbow, *The Magic Bullet?, op. cit.*, p. 118.
43. DCDC, JCN 2/18, *Information Advantage*, Ministère de la Défense britannique, 2018.

la transparence : l'amélioration de la fonction commandement et contrôle (C2), la maîtrise du milieu, le renforcement du potentiel ami et l'optimisation de l'attrition adverse.

L'illusion la plus profonde et la plus étroitement associée à la métaphore de transparence est celle de l'omniscience et de la certitude, qui résulte d'une confusion entre le fait de voir précisément le champ de bataille et celui d'en maîtriser l'ensemble des paramètres, d'en comprendre ses dynamiques, voire de prédire les intentions de l'adversaire. Ce glissement intellectuel de la connaissance vers la compréhension et la prédiction est aujourd'hui renouvelé par les perspectives d'applications de l'IA. Ce mirage de la connaissance parfaite a été fortement influencé par la pensée de l'amiral américain Bill Owens, notamment par son ouvrage *Lifting the Fog of War* dans lequel il fait la capacité de « vue omnisciente en temps réel[44] » la clé de la victoire militaire[45]. La compréhension repose *in fine* sur la capacité de jugement du commandement, qui ne se nourrit pas seulement d'information et de contexte, mais également sur une appréciation, un sens de la perspicacité et de la clairvoyance, facultés humaines nécessairement faillibles et imparfaites[46].

Cette illusion de la perfection technologique continue régulièrement d'influencer la culture stratégique américaine[47]. Plus raisonnablement, la transparence est analysée comme le levier d'une accélération du cycle décisionnel. La capacité à disposer en permanence d'un « avantage informationnel[48] », résultant à la fois d'une connaissance quasi parfaite de la situation et d'une interdiction continue de cette connaissance à l'adversaire est considérée comme un facteur clé de supériorité opérationnelle qui permettrait d'accélérer le *tempo* opérationnel en décidant « à la vitesse de l'information », forçant ainsi le cycle de décision de l'adversaire jusqu'à son implosion. Robert Leonhard fait ainsi de la vitesse l'avantage le plus important que la transparence doit permettre d'acquérir[49].

L'ambition de la maîtrise du milieu découle de l'expansion permanente des champs de confrontation sur des espaces de plus en plus grands et ouverts. À l'instar du combat naval, dont l'immensité du milieu fait de la connaissance de la position adverse le prérequis indispensable pour disposer de l'avantage tactique, la quête de la maîtrise de l'espace opérationnel conduit à mener « un effort permanent pour balayer toujours plus vite un

44. B. Owens, *Lifting the Fog of War*, New York, Farrar, Strauss and Giroux, 2000.
45. O. Mackubin, « Reflections on Future War », *Naval War College Review*, vol. 61, n° 3, U.S. Naval War College Press, 2008, p. 61-76.
46. « Action terrestre future », *op. cit.*, p. 25.
47. I. Reynolds, « Seeing, Knowing, and Deciding: the Technological Command Dream That Never Dies? », *War on the Rocks,* 13 juillet 2022, disponible sur : https://warontherocks.com. Voir aussi A. Cattaruzza et S. Taillat, « Les enjeux de la numérisation du champ de bataille », *Dynamiques internationales*, n° 13, 2018, p. 2.
48. *Summary of the Joint All-Domain Command and Control (JADC2) Strategy*, Département de la Défense américain, 2022.
49. R. Leonhard, *The Principles of War for the Information Age*, Novato, Presidio Press, 1998.

espace toujours plus vaste[50] ». Le double enjeu de l'espace et du temps incite à appréhender la situation opérationnelle sous la forme d'une « image » opérationnelle commune (*common operational picture* – COP) partagée, géolocalisée et actualisée. Cette modélisation de la représentation de l'environnement opérationnel vise à maîtriser les paramètres du combat, mais se confronte à la dilatation du besoin tactique de savoir toujours plus loin, toujours plus vite et plus précisément[51].

La connaissance en temps quasi réel et partagée de la situation amie est en soi un fait unique dans l'histoire militaire dont il reste encore à percevoir toutes les implications[52]. Le chef militaire dispose désormais d'une vue complète et ajustée de son propre dispositif tactique et de l'état de ses forces. Le *Blue Force Tracking* (BFT), qui permet la géolocalisation des unités amies avec des taux de rafraîchissement[53] de plus en plus élevés, contribue à diminuer les risques de tirs fratricides, à mieux répartir les forces sur le terrain, et à mieux appréhender ses capacités de manœuvre. Sur le plan logistique, les capteurs intégrés et les progrès de l'IA vont également contribuer au renforcement du potentiel ami, en permettant le suivi permanent des paramètres logistiques de chaque unité déployée, le juste dimensionnement du soutien aux besoins opérationnels réels et une amélioration de la disponibilité opérationnelle des matériels grâce au développement de la maintenance prédictive et à l'optimisation des diagnostics de réparabilité. Cette transparence vise moins la levée du brouillard de la guerre que la disparition des causes de la « friction » chère à Clausewitz. Tirant des conclusions très optimistes des progrès cumulés de la connaissance amie et ennemie associées à la précision des feux, Guy Hubin en concluait même, de manière sans doute prématurée, que la fin du recours aux feux de saturation entraînerait *de facto* une réduction drastique des flux logistiques[54] et une libération des contraintes de ravitaillement.

L'espoir d'atteindre une visibilité parfaite du champ de bataille s'est enfin accompagné très tôt de celui de la destruction instantanée de toute cible se dévoilant. Le développement sans précédent des capteurs en termes de performance, de redondance et de permanence, couplé aux progrès de la connectivité et à l'allongement de la portée des effecteurs terrestres et aériens (*cf.* partie 2), a conduit à raisonner la transparence quasiment exclusivement en termes d'attrition, limitant le nouvel art de la guerre à deux actions techniques : « trouver des cibles et les frapper[55] », par le biais d'une « boucle reconnaissance-feu[56] » ou *kill chain* optimisée. De cette conception

50. T. Lavernhe et F.-O. Corman, *Vaincre en mer au 21e siècle : la tactique au cinquième âge du combat naval*, Paris, Équateurs, 2023, p. 259.
51. *Ibid.*, p. 260.
52. B. Durieux, « La manœuvre future », *in* C. Malis, *Guerre et Manœuvre,* Paris, Economica, 2009.
53. Actualisation des données tactiques (dont positionnement).
54. G. Hubin, *Perspectives tactiques*, Paris, Economica, 2009.
55. M. Libicki, « The Small and the Many », *in* J. Arquilla, D. Ronfeldt *et al.*, *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND Corporation, 1997, p. 191-216.
56. Entretien avec un officier supérieur de l'armée de Terre, 4 décembre 2023.

découle un modèle de bataille conduite par et pour les feux et orientée prioritairement vers l'attrition de l'adversaire. La précision croissante des feux indirects observée sur le front ukrainien[57] et la létalité d'un espace de bataille saturé de moyens d'observation renforce cette tendance d'une transparence pensée exclusivement dans une perspective de ciblage. L'ambition ultime de cette optimisation serait d'aboutir à une quasi-immédiateté de la frappe en réduisant la boucle décisionnelle à quelques secondes[58]. L'instantanéité de la visibilité équivaudrait à une instantanéité des effets, dans un environnement de combat où se dévoiler reviendrait à être détruit.

La connectivité, fragile système nerveux de la transparence

Au-delà des concepts doctrinaux, la transparence est fondamentalement le résultat d'un système de mise en réseau de données dans le temps et dans l'espace, qui repose sur :

- des capteurs, qui collectent des données variées et en grand volume, en permanence et sur toute la surface de l'environnement opérationnel ;
- des outils de fusion et d'analyse de ces données, qui donnent sens à ces données dans le temps et dans l'espace (géolocalisation, mise en cohérence et vue d'ensemble actualisée) ;
- un réseau qui assure la transmission instantanée des données collectées et traitées et garantit par là leur validité, c'est-à-dire leur valeur opérationnelle.

Cette mise en synergie des données dans le temps et dans l'espace confère au décideur une forme de vue « panoptique », entendue comme la capacité à embrasser d'un coup d'œil l'ensemble de l'espace de bataille[59].

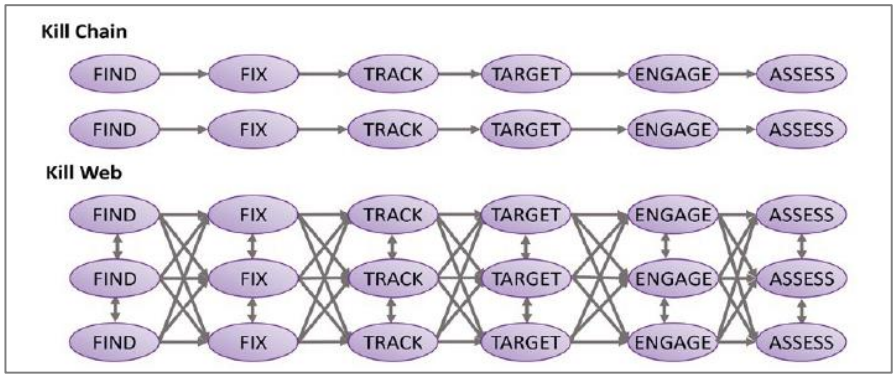
La connectivité est la clé du fonctionnement de ce système, véritable « colonne vertébrale numérique » (*digital backbone*) des modèles capacitaires contemporains, sur laquelle sont « branchés l'ensemble des capteurs, effecteurs et décideurs[60] », sans laquelle ils perdent leur supériorité intrinsèque. Elle doit s'incarner dans un réseau suffisamment stable et puissant pour faire circuler les gigantesques volumes de données que génèrent les capteurs contemporains, à une vitesse toujours accélérée. Ainsi, la dimension des réseaux de connectivité est en train de se dilater dans un changement d'échelle écrasant, ouvrant la voie à l'ère de

57. J. Watling et A. Reynolds, « Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive », *Special Report*, RUSI, 2023.
58. Entretien avec un officier supérieur de l'armée de Terre, le 6 février 2024.
59. Concept tiré du dispositif pénitentiaire dit « panoptique » de Jeremy Bentham qui, est supposé permettre au sujet qui regarde de tout voir, et repris par Michel Foucault dans *Surveiller et punir*, voir : C. Laval, « Surveiller et prévenir, la nouvelle société panoptique », *Revue du Mauss*, n° 40, 2012, p. 47 à 72.
60. N. Carter, Discours à *Policy Exchange*, 30 septembre 2020, disponible sur : www.gov.uk.

« l'hyperconnectivité[61] ». Le réseau 4G comprend aujourd'hui environ 20,4 milliards d'appareils connectés dans le monde, soit environ 60 000 appareils par kilomètre (km) carré. Le réseau 5G permettra de prendre en charge plus d'un million d'appareils sur la même surface[62]. À titre d'illustration dans le domaine militaire, le volume d'échange de données entre les FREMM (frégates multimissions) actuelles et les futures FDI (frégates de défense et d'intervention) sera multiplié par un million[63]. De même, les flux vidéo des drones qui sillonnent l'espace aérien ukrainien ne pourraient pas être exploités sans les 100 mégabits (Mbits) par seconde que garantit le réseau *StarLink* aux postes de commandements équipé de ces terminaux[64].

La complexité technologique de la connectivité contemporaine se double de la complexification des fonctions qu'elle sert. À ce titre, la boucle « renseignement/feu » offre un bon aperçu de la densité du maillage de connectivité nécessaire à la mise en réseau des fonctions garantissant son efficacité. En réalité, « voir » est loin d'être suffisant, et recouvre une réalité beaucoup plus complexe. La fonction de captation de la donnée se décline en fait en plusieurs étapes successives ou simultanées : « trouver, acquérir, suivre, engager, évaluer[65] ». L'enjeu est prioritairement de compléter cette boucle dans les délais les plus brefs possible, mais également de pouvoir faire tourner plusieurs boucles identiques en simultané, ce qui accroît d'autant les exigences de connectivité. La vulnérabilité face aux actions cyber-électroniques adverses impose en plus une redondance des moyens pour garantir la permanence du réseau, transformant la « chaîne » en « réseau »[66].

Schéma I-1 : Évolution de la connectivité, de la « chaîne » au « réseau »

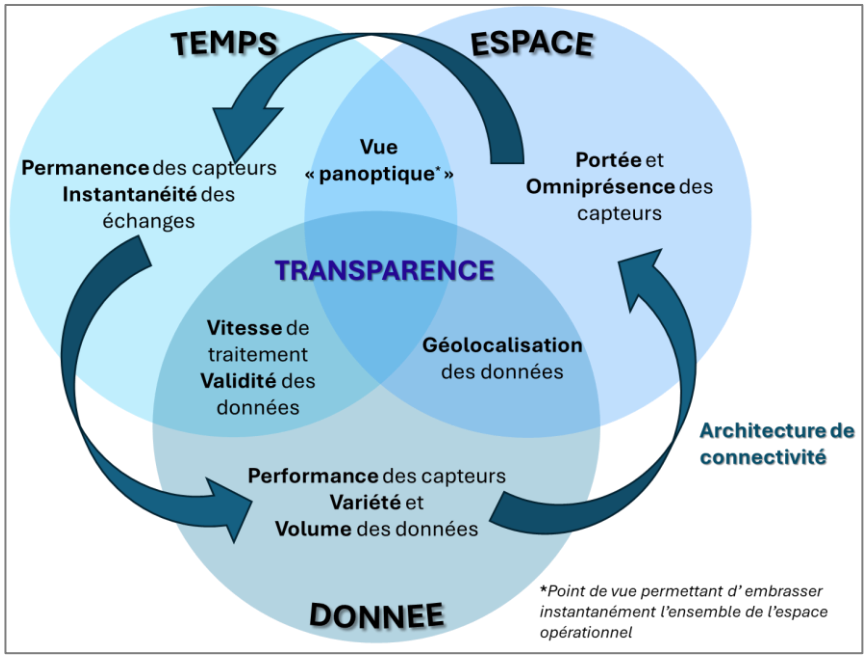


Source : H. Penney, « Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition », Policy Paper, Mitchell Institute, 2023.

61. L. Meny, « L'art de la guerre dans un monde hyperconnecté », *Revue Défense Nationale*, HS n° 4, 2021, p. 155-168.
62. N. Monaco, S. Minneman et K. Joseff, *The Hyperconnected World of 2030–2040*, IFTF, 2020.
63. Entretien avec un cadre de l'industrie de défense, le 6 décembre 2023.
64. S. Skove, « What the US Military Can Learn from Ukrainian Command Posts », *Defense One*, 12 janvier 2024, disponible sur : www.defenseone.com.
65. H. Penney, « Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition », *Policy Paper*, Mitchell Institute, 2023.
66. Dans la doctrine française, on parle de « réseau multi-senseurs/multi-effecteurs », RM2SE.

La transparence est donc le résultat espéré d'un modèle capacitaire conçu autour de la donnée, articulé à partir d'un réseau de connectivité organisé pour capter, fusionner, stocker et diffuser cette donnée. Elle suppose pour se manifester une optimisation technique (nature des réseaux, gestion de la bande passante et de la saturation des gammes de fréquence), mais aussi procédurale et organisationnelle visant à organiser et gérer la masse de données produites afin de disposer d'une boucle de décision fluide, rapide et permanente. *A contrario*, il suffit de cibler un maillon de cette chaîne de connectivité pour dégrader significativement la transparence délivrée en bout de chaîne.

Schéma I-2 : Modélisation de la transparence



© Pierre Néron-Bancel/Ifri, 2024.

La fin de l'incertitude ?

« There is no sanctuary on the battlefield[67] »

Au rebours de la vision positive de la transparence comme facteur de supériorité opérationnelle, la reconnaissance de sa réciprocité[68] conduit à relativiser son caractère absolu. Le postulat de sa maîtrise par le camp adverse conduit à analyser actuellement la transparence davantage sous l'angle des contraintes qu'elle fait peser sur le champ de bataille et des principes, procédés et capacités qu'elle vient remettre en cause et invalider.

67. M. Zabrodskyi *et al.*, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine*, *op. cit.*, p. 53.
68. Entretien avec un chercheur, le 13 décembre 2023.

La contrainte la plus drastique que fait peser la transparence, surtout dans le milieu terrestre, est l'augmentation de la létalité. La permanence et la qualité des moyens de surveillance contemporains dégradent singulièrement les facteurs qui garantissent la survivabilité, comparable à un oignon formé de « couches successives qui séquencent un engagement au combat » : « détecter sans être détecté ; si l'on est détecté, ne pas être identifié ; si l'on est identifié ne pas être acquis ; si l'on est acquis, ne pas être touché…[69] ». L'impossibilité pour un véhicule blindé de se déplacer sur la ligne de front ukrainienne de jour témoigne de l'impact significatif de la saturation des capteurs sur la survivabilité. Même la protection du fantassin enterré ou protégé par son blindage est remise en cause par le développement de drones suicides dits « FPV[70] » capables de repérer et d'atteindre leur cible jusqu'à l'intérieur des tranchées.

La zone arrière, jusqu'ici considérée comme un sanctuaire hors de portée des vues et des feux tactiques adverses, ne peut plus elle-même être considérée comme sûre, ce qui confirme l'obsolescence des modèles de déploiement des bases logistiques et des postes de commandement actuels, déjà mis à mal par l'extension de la portée des effecteurs. La frappe ukrainienne contre les aéroports de Berdyansk et Luhansk le 17 octobre 2023 ayant permis la destruction de neuf hélicoptères russes[71] illustre cette vulnérabilité accrue des zones arrière et la difficulté intellectuelle à s'adapter à cette nouvelle réalité. Il faut cependant porter un regard mesuré sur le réel degré de transparence dans la profondeur. Plus l'on s'éloigne de la ligne de front et plus la difficulté à identifier des objectifs valides est élevée[72].

Plus largement toutefois, ce sont les concepts même de discrétion et de secret qui semblent mis à mal par l'avènement de la transparence adverse, ce qui pose la question des nouvelles conditions de réalisation de la surprise tactique[73]. Alors que les deux facteurs fondamentaux de la surprise sont la vitesse et le secret, la lisibilité inédite des dispositifs tactiques contraint fortement la discrétion et rend singulièrement difficile la réalisation de la surprise tactique. Cependant, la capacité des forces armées ukrainiennes à masquer la préparation de la contre-offensive de Kharkov en concentrant cinq brigades blindées-mécanisées à l'insu du renseignement russe en août 2022 laisse penser que dans certaines conditions la discrétion reste un procédé viable[74].

69. R. Hémez, « La survivabilité sur le champ de bataille. Entre technologie et manœuvre », *Focus stratégique*, n° 72, Ifri, mars 2017.
70. *First-person view*. Lire « Killer Drones Pioneered in Ukraine Are the Weapons of the Future », *The Economist*, 8 février 2024, disponible sur : www.economist.com.
71. « Guerre en Ukraine : des frappes destructrices sur des aérodromes de l'armée russe revendiquées par l'Ukraine », *Le Figaro,* 18 octobre 2023, disponible sur : www.lefigaro.fr.
72. Entretien avec un officier supérieur du CPCO, 16 janvier 2024.
73. R. Hémez, « L'avenir de la surprise tactique à l'heure de la numérisation, *Focus stratégique*, n° 69, Ifri, juillet 2016, p. 19-22.
74. M. Goya, « 1918 en Ukraine », *La voie de l'épée,* 29 octobre 2022, disponible sur : https://lavoiedelepee.blogspot.com.

Cette même problématique de discrétion pourrait se poser à l'horizon 2050 dans le milieu sous-marin, dans lequel les dynamiques convergentes de l'intelligence artificielle, des progrès de la détection maritime et des communications sous-marines viendraient remettre en cause de manière radicale l'opacité naturelle du milieu et les efforts de contre-détection des sous-marins[75]. Une bascule de l'équilibre opacité-transparence en faveur de la seconde aurait bien entendu de lourdes implications sur la sûreté des dispositifs maritimes et en particulier ceux liés à la dissuasion nucléaire[76]. Une remise en cause de la discrétion du sous-marin compromettrait en tout cas sa capacité à se « diluer » dans son milieu, alors que c'est sur cette aptitude que repose l'incertitude propre au combat sous-marin. Cette perspective est âprement discutée au sein des marines les plus avancées qui suivent de près toutes les avancées scientifiques en la matière et veillent à conserver plusieurs longueurs d'avance sur de tels progrès à travers l'optimisation de la furtivité de leurs porteurs.

La lisibilité accrue des dispositifs tactiques pose également la question de la validité du principe de concentration des forces[77]. Le regroupement de forces n'est plus ni souhaitable, car immédiatement détecté, ni même possible car immédiatement ciblé. Faut-il pour autant en déduire la fin du principe de concentration[78] ? L'enjeu devient celui de la rapidité du regroupement des moyens et de la fluidité du mouvement tactique pour devancer le temps de la détection adverse. C'est l'avenir de la manœuvre elle-même qui se pose, alors qu'elle est soumise aujourd'hui dans le milieu terrestre à un double phénomène qui la neutralise. D'un côté, les progrès de la transparence figent la manœuvre en un front fixe, de l'autre la linéarité qu'elle crée décuple les effets de la transparence, notamment l'attrition[79]. Dans le débat doctrinal américain classique entre la manœuvre et l'attrition[80], les tenants de l'attrition considèrent que l'omniprésence de la surveillance du champ de bataille a « tué la manœuvre » en amplifiant la prépondérance des feux sur la mobilité, limitant la bataille terrestre future à un duel d'artillerie au-dessus d'un « *no man's land* dangereux[81] ». Alors que les théoriciens de la RMA faisaient de la domination par l'information le

75. R. Bradbury *et al.*, « Transparent Oceans? The Coming SSBN Counter-Detection Task May Be Insuperable », *ANU National Security College*, 2020.
76. A. Gilli, M. Gilli *et al.*, « Climate Change and Military Power: Hunting for Submarines in the Warming Ocean », *Texas National Security Review*, vol. 7/2, 2024, disponible sur : https://tnsr.org.
77. A. Faurichon de la Bardonnie, « Le paradoxe de la surprise et de la transparence », *Revue Défense Nationale*, HS n° 13, 2023, p. 46-62.
78. G. Hubin, *Perspectives tactiques, op. cit.*
79. Entretien du 13 décembre 2023.
80. Voir P. Garrett, U. et F. Hoffman, « Maneuver Warfare Is Not Dead, But It Must Evolve », *Proceedings*, n° 149/11, novembre 2023 ; F. S. Gady, « Manoeuvre Versus Attrition in U.S. Military Operations », *Survival*, n° 63/2, août-septembre 2021, p. 131-148.
81. A. Fox, « Manoeuvre Is Dead? Understanding the Conditions and Components of Warfighting », *The RUSI Journal*, n° 166, avril 2022, p. 10-18.

moyen de la « foudroyance[82] » décisive, il semble que le caractère décisif de la transparence soit annulé par sa réciprocité.

Les effets de l'hyperconnectivité sur le C2

L'accès partagé à l'information permanente et en temps réel induit également des changements profonds sur les processus de commandement, amenant à s'interroger sur ce que la transparence pourrait changer dans le rapport à l'information et dans les processus décisionnels. Les NTIC contemporaines facilitent les échanges entre les utilisateurs d'un même réseau en accélérant l'expression et la satisfaction du besoin, mais également en élargissant considérablement l'offre disponible grâce à la mise en réseau d'un nombre croissant de capteurs et d'effecteurs.

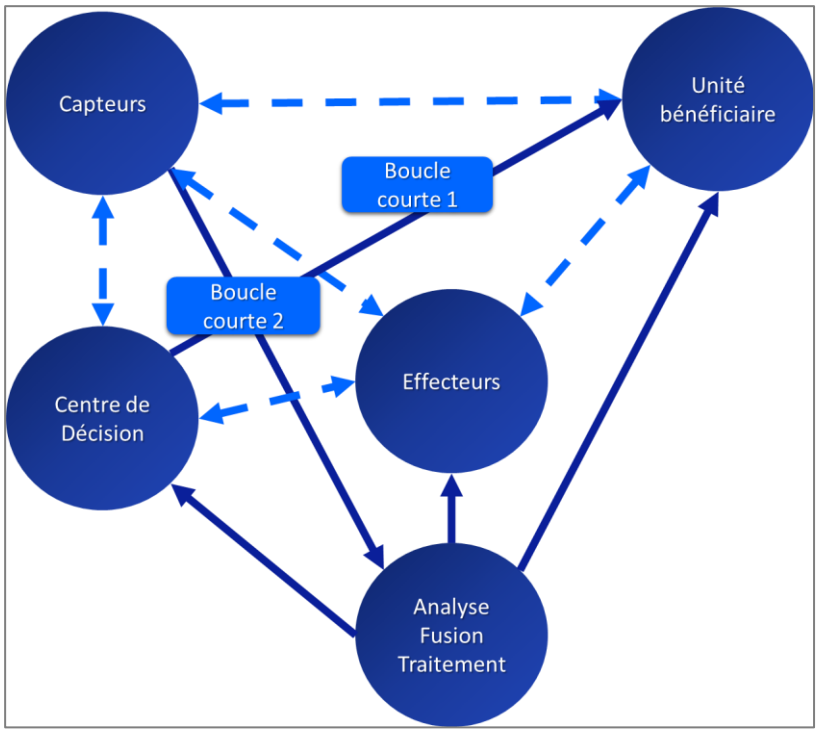
En ce sens, l'hyperconnectivité induit un effet d'« ubérisation[83] » de la donnée, qui laisse entrevoir un nouveau rapport à l'organisation des réseaux de commandement, guidée par l'optimisation permanente du cycle informationnel. La recherche d'efficacité et de rentabilité du système de surveillance par une accélération de la boucle de décision se traduit par un raccourcissement physique de la boucle, qui permet au demandeur de relier directement le capteur à l'effecteur, sans nécessairement passer par l'analyse préalable de la donnée ou la validation du décideur. Le choix d'une boucle courte amène nécessairement à développer les organisations horizontales et à limiter les interactions verticales. Elle peut également renforcer une tendance à privilégier « l'information » du capteur sur le « renseignement » de l'analyste.

La relation directe capteur/effecteur dans une boucle raccourcie peut avoir cependant l'effet opposé, si le capteur est géré directement par le niveau supérieur décisionnaire, de sortir l'unité bénéficiaire de la boucle. Le besoin opérationnel risque alors d'être écrasé par la logique d'efficacité de la boucle de transparence. Ce biais s'illustre dans des cas répétés de demandes d'appuis fumigènes par des unités ukrainiennes au contact refusées par les échelons supérieurs qui souhaitent privilégier leur couverture drone[84]. De la même manière, les PC ukrainiens disposant d'une recopie vidéo de leurs drones ont tendance à cibler en priorité les objectifs dans la profondeur couverts par les drones au détriment d'objectifs au contact d'unités qui

82. « Aptitude à frapper avec puissance, rapidité et soudaineté pour surprendre et sidérer », CIA 01, *Concept d'emploi des forces*, État-Major des Armées, 2021.
83. À comprendre ici non pas dans son sens de remise en cause d'un modèle économique traditionnel, mais dans celui du développement d'un modèle de mise en relation directe du besoin client géolocalisé à l'offre de service disponible en temps réel. Voir C. Parker, « Uber-style Technology Helped Ukraine to Destroy Russian Battalion », *The Times*, 14 mai 2022, disponible sur : www.thetimes.co.uk.
84. J. Watling et A. Reynolds, « Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive », *op. cit.*, p. 22.

expriment des demandes de tir[85], illustrant également cette « fascination pour le capteur[86] ».

Schéma I-3 : Le raccourcissement de la boucle de connectivité



© Pierre Néron Bancel/Ifri, 2024.

Les effets de la transparence sur les postes de commandement

La question de la vulnérabilité des postes de commandement tactiques terrestres est au cœur des débats actuels sur la transparence du champ de bataille et peut se résumer en deux dynamiques qui se renforcent l'une l'autre :

- d'une part les capteurs contemporains sont de plus en plus performants pour détecter la signature multi-spectre des PC de grandes unités et rendent leur dissimulation beaucoup plus complexe ;
- d'autre part la centralité de la donnée dans les systèmes de commandement limite la discrétion des PC et contribue à renforcer significativement leur empreinte dans tous les champs (volume et composition, poids et traînée logistique, signature thermique, signature digitale et rayonnement électromagnétique), tout en en faisant un nœud vital du système de connectivité dont la destruction dégrade significativement la capacité de combat d'une force.

85. Entretien du 6 février 2024.
86. J. Henrotin, « Les mutations du renseignement », *op. cit.*, p. 17.

Les systèmes de commandement ont subi depuis 1945 une « dérive inflationniste[87] » qui résulte à la fois d'un élargissement des fonctions qu'ils animent, des exigences croissantes de précision et d'exhaustivité encouragées par la situation de « confort opératif » post-guerre froide, et de la complexité croissante des procédures et des doctrines[88]. Cet accroissement des PC a été nourri par les exigences en termes de qualité et de volume de l'information, la recherche d'une maîtrise toujours plus grande de l'environnement opérationnel requérant toujours plus de spécialistes, de serveurs et de systèmes de contrôle et de liaisons de données[89], sans même évoquer la multiplication des processus d'état-major qui en découle.

Les systèmes de PC modernes doivent répondre à deux injonctions contradictoires : accélérer leurs processus et être davantage connectés pour acquérir une meilleure compréhension de l'environnement opérationnel tout en diminuant drastiquement leur surface électromagnétique pour gagner en discrétion et limiter leur vulnérabilité. Leur dépendance accrue aux systèmes d'information opérationnels et des communications (SIOC) les rend incapables de réduire leur empreinte numérique et électromagnétique sans affecter du même coup leur efficacité. Cette logique s'applique également aux navires de combat dont la signature électromagnétique contribue à alimenter l'indiscrétion de tout déploiement naval dès son départ à la mer[90].

« Des » transparences aux réalités bien différentes

Définir le degré de transparence du champ de bataille contemporain implique de tenir compte de la disparité des milieux et de leur résistance différenciée à la détection. Il serait donc plus juste de parler de « transparences » en adaptant la réalité de ce concept aux caractéristiques propres à chaque espace de conflictualité, en se concentrant ici sur les milieux physiques qui induisent une présence humaine.

Depuis le perfectionnement du radar, l'espace aérien est devenu le milieu le plus transparent. Espace *a priori* vide d'activité humaine, l'activité aérienne y est forcément temporaire et donc discontinue, ce qui en fait une anomalie plus facilement détectable[91]. En dehors de la furtivité ou de certaines formes de brouillages de déception, l'arme aérienne a appris à s'accommoder de la transparence de son milieu pour préserver l'ambiguïté sur ses intentions, en jouant sur la vitesse et la mobilité pour retarder au plus

87. Général Alabergère, cité dans S. Caplain et R. Hémez, « Haute intensité : la survie des postes de commandement », *DSI*, n° 153, Areion Group, mai-juin 2021, disponible sur : www.areion24.news.
88. S. Caplain, « La fourmilière du général, le commandement opérationnel face aux enjeux de la haute intensité », *Focus stratégique*, n° 89, Ifri, juin 2019.
89. M. Beagle, J. Slider et M. Arrol, « The Graveyard of Command Posts: What Chornobaivka Should Teach Us About Command and Control in Large-Scale Combat Operations », *Military Review Online Exclusive*, mars 2023, disponible sur : www.armyupress.army.mil.
90. E. Lanquetot, « Le silence relatif », *DSI*, n° 163, Areion Group, janvier-février 2023, p. 70-75.
91. Entretien avec un officier supérieur de l'armée de l'Air et de l'Espace, le 29 novembre 2023.

tard la détection et limiter la fenêtre d'opportunité de la réaction adverse. En ce sens, la manœuvre aérienne recherche la surprise dans le sens que lui donne Leonhard du résultat « de l'interaction entre deux composantes : un état d'impréparation permanent et le temps[92] ». Les technologies de la furtivité semblent pourtant redonner à ceux qui en maîtrisent la complexité une forme d'opacité inégalée depuis 1940.

Interface entre les espaces terrestres, aériens et sous-marins, la mer apparaît comme le milieu le plus paradoxal sur le plan de la transparence, à la fois très lisible mais immense en surface, et extrêmement opaque et complexe sous l'eau. Quant aux espaces littoraux, ils sont particulièrement hermétiques à la surveillance depuis la mer alors qu'ils favorisent la transparence des approches maritimes vu de la terre. La manœuvre navale cherche à exploiter à son avantage l'incertitude résultant de la capacité à se diluer dans l'immensité du milieu tout en visant une certaine maîtrise de cette incertitude pour assurer sa sûreté, consacrant à cette tâche une ressource importante qui entretient le dilemme de la dispersion des moyens[93].

L'opacité élevée du milieu terrestre[94] est due en premier lieu à son caractère très hétérogène et discontinu, ensuite à l'absence de profondeur de vue dans la plupart des espaces qui le constituent (végétation, relief, urbanisme…), enfin à l'extrême diversité des activités humaines qui s'y déroulent en permanence et qui le soumettent à une mutation constante[95]. Celles-ci génèrent une masse continue d'informations, véritable « chaos informationnel[96] » qui complique la lecture de l'environnement opérationnel. La manœuvre terrestre repose sur une exploitation optimale du terrain pour en tirer un avantage, mais doit tenir compte en permanence de l'environnement humain dans lequel elle agit, qui peut être son objectif, sa protection ou une contrainte. Sa sûreté dépend à la fois de sa dissimulation et de sa mobilité, facteurs rendus complexes par la « viscosité » du milieu et son ouverture aux espaces aériens et exo-atmosphériques, qui facilitent la détection des variables dans un environnement essentiellement fixe.

92. R. Leonhard, *Principles of War, op. cit.*, p. 183.
93. T. Lavernhe et F.-O. Corman, *Vaincre en mer au XXIe siècle. La tactique au cinquième âge du combat naval*, Paris, Équateurs, 2023, p. 260.
94. É. Tenenbaum, « Le rôle stratégique des forces terrestres », *Focus stratégique*, n° 78, Ifri, février 2018.
95. « RFT 3.2.0 - Concept d'emploi des Forces terrestres », CDEC, 2021.
96. « Action terrestre future », *op. cit.*

L'espace exo-atmosphérique a jusqu'à présent été considéré comme un amplificateur de la transparence des autres milieux grâce à ses capacités d'observation, de communication et de positionnement. Son évolution vers un milieu opérationnel à part entière rend nécessaire le développement d'une surveillance militaire de l'espace aujourd'hui réservée à quelques puissances, étant donné la complexité technique des moyens de surveillance. Si la détection est accessible, la caractérisation reste très ardue, ce qui favorise l'ambiguïté et l'incertitude[97], surtout dans les orbites éloignées.

Les progrès des technologies de la transparence semblent ainsi remettre en cause la capacité à se dissimuler dans les milieux les plus opaques et incitent à repenser la manœuvre dans ces milieux pour y maintenir ou recréer les conditions de l'incertitude.

Tableau I-4 : Caractérisation des espaces naturels

	Espace aérien	Espace maritime (de surface)	Espace sous-marin	Espace terrestre	Espace exoatmosphérique
Caractéristiques naturelles du milieu	Espace "lisse" homogène	Espace "lisse", relativement homogène (hors littoral), fluide, hostile	Espace"lisse", homogène et fluide	Espace "solide" hétérogène rugueux et visqueux	Espace "lisse" homogène et déterministe
Densité	Très faible à nulle	Faible, sauf littoral	Moyenne à faible	Elevée	Faible à moyenne,
Profondeur / extension	Milieu tendant vers l'infini	Milieu fini mais immense Milieu d'interface tridimensionnel	Milieu fini mais immense et multidimensionnel	Milieu fini et très cloisonné	Milieu infini
Pénétration des phénomènes physiques détectables	Très bonne dans tous les spectres selon la météo	EM: bonnes Optique / sonore: très faible	Optique / EM: très faible Sonore: très bonne mais complexe	Moyennes à faible dans tous les spectres, très contraintes Très élevées dans un cercle proche de détection	Optique / EM : Excellente
Obstacles	Météorologie Relief terrestre	Météorologie Zones littorales Activité maritime	Fonds marins Bathythermie Bathymétrie	Relief Végétation Urbanisation Activités humaines	Distance de détection
Densité de l'activité humaine	Très faible (activité discontinue) Discrimination aisée	Très faible à très élevée (littoral, couloirs, points de passage obligés) Discrimination difficile	Quasi-nulle Discrimination aisée (si détecté)	Elevée à très élevée Occupation permanente et vitale de l'espace Discrimination complexe	Nulle à élevée Discrimination complexe (nature et mission)

Source : C. Paulin, M. Asencio et al.*, « Vers une vision réaliste des opérations en réseau », Recherche et Documents, n° 2/2009, Fondation pour la recherche stratégique, 2009.*

97. M. Friedling, « L'Espace : un enjeu stratégique et un nouveau champ de confrontation militaire », *Revue Défense Nationale*, 2019, p. 67 -73.

Tableau I-5 : Caractérisation des milieux de confrontation

	Milieu aérien	Milieu maritime (de surface)	Milieu sous-marin	Milieu terrestre	Milieu spatial
Mobilité militaire / vitesse dans le milieu	Très élevée Foudroyance	Elevée Manœuvrabilité	Très élevée Ubiquité	Faible et très contrainte Stabilité	Elevée mais contrainte
Caractéristiques des dispositifs militaires	Densité faible Dispersion élevée Présence limitée et discontinue	Densité faible Dispersion élevée Présence prolongée mais limitée	Densité très faible, Dispersion maximale Présence prolongée	Densité élevée Dispersion très faible Présence permanente	Densité faible Présence quasi-permanente
Intégration dans le milieu	Transit	Maitrise	Dilution	Occupation	Transit
Capacité de représentation de l'environnement opérationnel (situation awareness)	Vision globale, acquisition rapide Représentation dynamique	Vision d'ensemble 360° dans la surface d'action Représentation dynamique	Vision restreinte	Vision fragmentée et parcellaire Déformation de la vision selon le niveau Représentation statique	Vision globale dépendante des moyens d'observation Représentation par catalogue
"Transparence" théorique du milieu	Transparent	Plutôt transparent	Opaque	Opaque	Transparent

Source : C. Paulin, M. Asencio et al.*, « Vers une vision réaliste des opérations en réseau »,* op. cit.

La dialectique de la transparence et de l'opacité sur le plan techno-capacitaire

La transparence est souvent considérée comme une donnée d'entrée de l'art opératif du XXIe siècle, phénomène indépassable du fait des progrès techniques concernant les capteurs, les plus médiatisés étant les drones. Ceci est en grande partie fondé mais mérite d'être nuancé. Un examen clinique du rapport transparence-opacité sur le plan techno-capacitaire est donc requis pour en évaluer précisément la dynamique et les éventuelles limites, sous ses deux grands volets : le recueil des données (champ physique) et leur traitement (champ cognitif).

Perfectionnement spectaculaire des capteurs, progrès sensibles des capacités d'analyse

Le développement tous azimuts des drones

Ces vingt dernières années ont connu des progrès exponentiels dans les capacités techniques de recueil du renseignement, les drones en particulier. Ce terme devenu très générique oblige à se pencher sur la variété d'aptitudes qu'il recouvre. Le champ de bataille moderne comprend des drones de surveillance de l'échelle tactique (des nano- ou mini-drones au *Patroller* de Safran) à l'échelle opérative ou stratégique avec les drones MALE (*Medium Altitude Long Endurance*) comme le MQ-9 Reaper ou HALE (*High Altitude Long Endurance*) comme le RQ-4 Global Hawk.

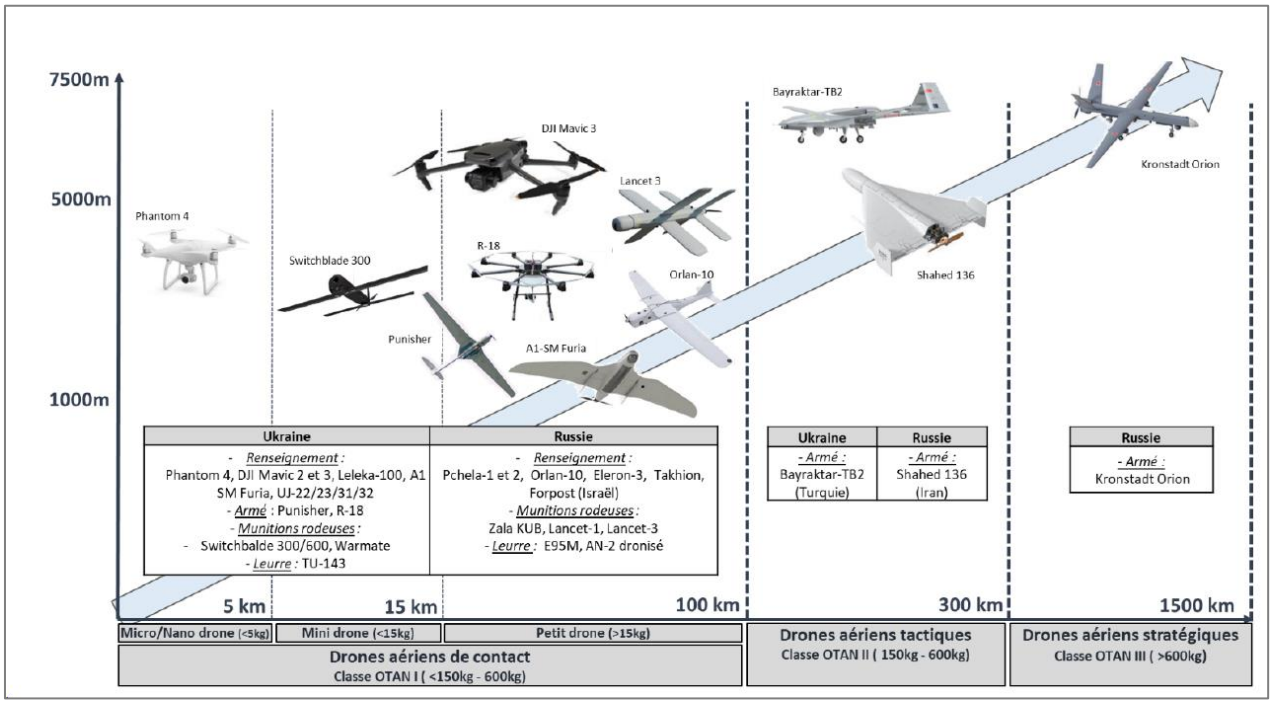
Sur l'ensemble de ce large spectre, les drones ont connu des progrès fulgurants, tant en termes de rayon d'action, d'endurance, de connectivité, que d'emport en charge utile. Sur ce dernier point, les charges embarquées bénéficient de capacités de discrimination sans cesse améliorées, notamment en termes de résolution. Plusieurs charges peuvent équiper un même drone « multicapteurs » (capteurs optroniques, électromagnétiques, etc.). En quelque sorte, un drone perfectionné fournit à lui seul un renseignement multi-sourcé. Ainsi, le RQ-4 possède une endurance de 24 à 36 heures, un rayon d'action de plus de 22 000 km et peut emporter une charge utile totale de 1 360 kg, déclinable en capteurs variés (électro-optiques de haute résolution, infrarouges, SAR/MTI-*Synthetic Aperture Radar/Moving*

Target Indicator). À eux seuls, les drones créent un effet « d'occupation aérienne[98] » : leur multiplicité garantissant une surveillance quasi continue.

Aux drones de surveillance s'ajoutent les munitions télé-opérées, ou drones maraudeurs. Ceux-ci peuvent désormais combiner une fonction de détection et de frappes, comme l'ont montré la dernière guerre du Haut-Karabakh et le conflit russo-ukrainien. Des drones maraudeurs[99] consommables attaquent leur proie dès que celle-ci est détectée. Ceux-ci sont à distinguer des drones armés, larguant quant à eux des munitions et conçus pour être réutilisés. La guerre en Ukraine voit la multiplication des micro-drones de tous niveaux techniques, consommables ou non, disponibles aux plus petits niveaux tactiques (sections de combat). Ils ont deux fonctions principales : améliorer la connaissance de la situation tactique des unités ; raccourcir et parfaire la boucle détection-frappes s'agissant des feux de l'artillerie. En situation de conflit, quantité de drones civils, de moindre qualité que les drones militaires en dotation, viennent ainsi compléter l'inventaire existant et œuvrent, à leur manière, à la transparence. Leur taux d'attrition a beau être élevé, ils sont facilement remplaçables et peuvent bénéficier d'un écosystème agile (adaptations réactives sur le terrain, start-ups et petites et moyennes entreprises [PME] industrielles innovantes[100]). Aussi, pour répondre à la vulnérabilité des drones en contexte de haute intensité, des programmes de longue haleine s'efforcent de mettre au point un drone hypervéloce (SR-72 de Lockheed-Martin)[101] ou furtif (RQ180 de Northrop Grumman)[102].

98. J.-C. Noël, « Occuper sans envahir, drones aériens et stratégie », *Politique étrangère*, vol. 78, n° 3, Ifri, septembre 2013, p. 105-117.
99. Aussi nommés munitions vagabondes ou munitions téléopérées (MTO).
100. Par exemple en France : Parrot, Delair, Drone XTR, Drone Volt, Elistair, Novadem, etc.
101. Vitesse de Mach 6.
102. On pourrait ajouter le MQ28 Ghost-Bat de Boeing Australia, même s'il s'agit surtout d'un drone multirôles. Voir T. Fouillet, *La Guerre au XXIe siècle. Le retour de la bataille*, Paris, Éditions du Rocher, 2023, p. 277.

Schéma II-1 : Classification des systèmes de drones et application au conflit ukrainien



Source : A. Cervera et O. Entraygues, Russie – Ukraine : Dix-huit mois de guerre totale*, CDEC, 18 septembre 2023.*

Outre le milieu aéroterrestre, le développement des drones concerne le domaine maritime[103]. Ainsi, le RQ-4 est décliné dans une version maritime, le MQ-4 Triton. Le drone aérien de reconnaissance Camcopter S-100 peut être mis en œuvre depuis une plateforme navale[104]. Certains pays, comme la Turquie, réfléchissent à un concept de porte-drones en lieu et place des porte-aéronefs[105]. Le Blackwing, projet américain, est un drone à changement de milieu pouvant être mis en œuvre à partir d'un sous-marin puis conduire sa mission de surveillance dans l'espace aérien. Les drones sous-marins (UUV)[106] connaissent aussi des progrès rapides, tout comme les *gliders*, « planeurs sous-marins » d'une grande autonomie et très discrets.

En conclusion, le développement capacitaire protéiforme des drones, qu'ils soient aériens ou navals, a pour effet de créer une forme de « *continuum* de surveillance », favorisant la détection, dans tous les milieux, à tous les niveaux.

103. Lire à ce sujet L. Péria-Peigné, « La dronisation navale, une opportunité pour la Marine nationale de 2030 ? », *Briefings de l'Ifri*, Ifri, 25 août 2022.
104. Testé sur les porte-hélicoptères de la classe *Mistral*. Le Camcopter doit être remplacé par le SDAM (Système de drone aérien pour la Marine).
105. Y. Smaldore, « Drones, VTOL, convertibles : quel avenir pour les aéronavales embarquées ? », *Deftech*, août 2023.
106. *Unmanned-Undersea-Vehicles*.

Les autres moyens de surveillance : redondance et permanence

Les progrès techniques ne laissent pas en reste les autres moyens de surveillance ou détection, à commencer par les radars. Les plateformes de guet aérien AEW (*Airborne Early Warning*) voient également leurs capteurs se perfectionner sans cesse (portée du recueil, degré de résolution ou de discrimination, capacité simultanée de traitement, résilience…), de même pour les pods de reconnaissance (à l'instar du pod-TR pour le *Rafale* F5, fusionnant les actuels pods reco-NG et les pods de désignation Talios)[107]. Outre les radars embarqués sur plateformes aériennes ou navales, les radars au sol connaissent aussi des perfectionnements continus, progrès laissant présager de possibles ruptures s'agissant notamment des radars passifs, transhorizon, basse fréquence[108] ou de futurs radars incorporant la technologie quantique. Cette dernière autorise une puissance de calcul inégalée et pourrait remettre en question la furtivité des vecteurs, entre autres cas d'usage envisageables[109]. Les performances des radars seront en outre maximisées par l'IA.

Bien au-dessus du champ de bataille aérien classique, les pseudolites ou HAPS (*High Altitude Pseudo-Satellites*) agissent aux abords de la stratosphère[110]. On ne parle plus ici en heures de surveillance mais en mois. Très économes en énergie, ces engins de grande taille, à l'instar du projet d'aérostat *Stratobus* de Thalès Alenia Space (250 kilogrammes de charge utile)[111] ou du plus récent ballon manœuvrant BalMan d'Heremia, pourraient se voir attribuer des missions d'observation, d'écoute (COMINT) ou de renseignement d'origine électromagnétique (ROEM), à des fins militaires mais aussi environnementales et scientifiques. Par rapport aux satellites, le degré de résolution de leurs images serait accru par leur plus grande proximité avec la surface terrestre ou maritime.

À l'avenir, ces vecteurs, drones, avions ou HAPS pourraient être dotés de capteurs utilisant de l'imagerie hyperspectrale. Cette technologie en développement est capable d'acquérir une multitude de bandes spectrales[112] très étroites (plusieurs centaines), démultipliant le champ d'analyse envisageable. La détection précise de tunnels souterrains deviendrait

107. L. Lagneau, « Le *Rafale* F5 sera équipé du POD TR, qui fusionnera les capacités des nacelles TALIOS et RECO NG », *OPEX360*, juin 2023.
108. M.-A. Eva, « Vitesse, furtivité, la quête de survivabilité », *Revue Défense Nationale*, n° 809, avril 2018, p. 78-82.
109. E. Hardy, « La stratégie militaire et le champ opérationnel des compétitions technologiques », *Revue Défense Nationale*, HS n° 4-2021, p. 214-226.
110. Rappelons qu'en matière de souveraineté, on est situé juridiquement dans un « espace commun » à partir de la stratosphère.
111. M. Cabirol, « Thales Alenia Space : si, si le projet de dirigeable stratosphérique Stratobus respire encore », *La Tribune*, septembre 2022.
112. L'imagerie conventionnelle en perçoit 3 (rouge, vert, bleu, c'est-à-dire ce que voit l'œil humain), l'imagerie multispectrale en analyse autour d'une demi-douzaine supplémentaire.

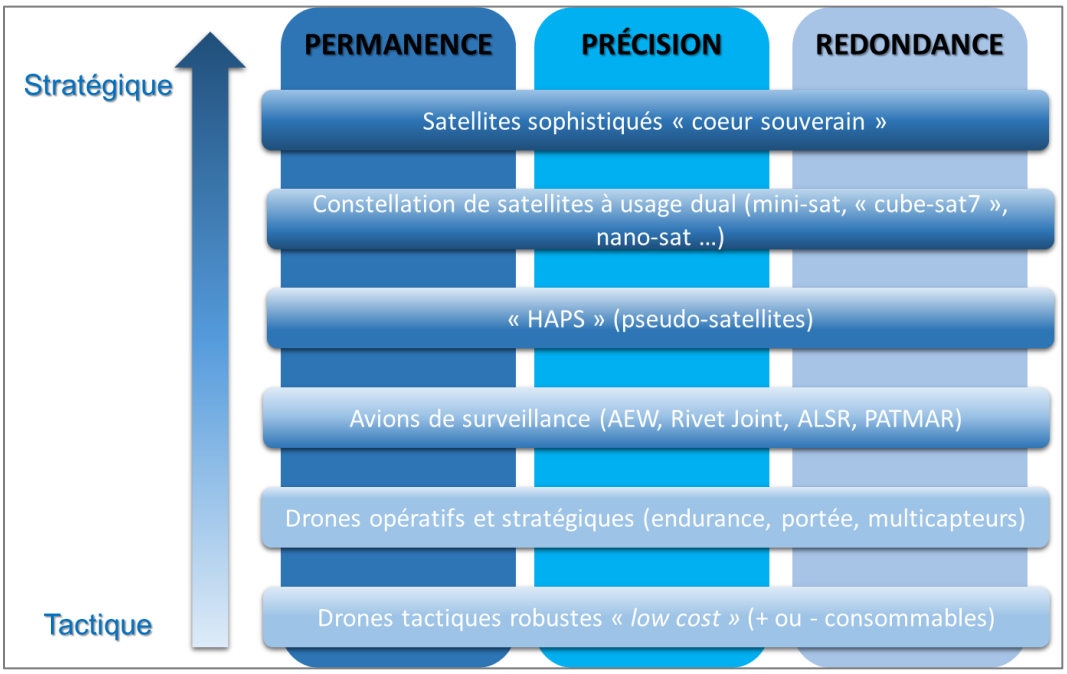
possible, entre autres, bien que les techniques d'interprétation demeurent complexes[113].

Instruments par essence stratégique, les satellites ont eux aussi connu un développement effréné, plus précoce que celui des drones, et encore accentué ces dernières années par les progrès civils, notamment autour du *New Space*. S'agissant des satellites du « cœur souverain[114] », les plus sophistiqués, ces progrès renforcent incontestablement l'effet de transparence, tant dans le domaine de l'observation (imagerie optique ou radar), que de celui des écoutes, des télécommunications (portée et flux de bandes passantes) ou de la géolocalisation avec sa résultante, le guidage d'armements par GPS. Les perfectionnements techniques sont constants : résolution panchromatique, amélioration du taux de revisite (fréquence d'actualisation des images) ou résilience (durcissement avec de nouvelles contre-mesures), pour ne citer que les principaux paramètres[115].

En parallèle, on assiste ces cinq à dix dernières années aux progrès fulgurants du secteur spatial civil, dont la plupart des applications sont duales. Des constellations de mini ou nanosatellites, de plusieurs dizaines à plusieurs centaines d'objets de la taille d'une boîte à chaussures, sont ainsi présents dans l'espace. L'utilisation du réseau *Starlink* de SpaceX (jusqu'à 42 000 satellites prévus[116]) par l'armée ukrainienne a été amplement relatée et rappelle qu'en cas de conflit, ces constellations, résilientes par leur redondance, peuvent largement compléter le « cœur souverain », voire y suppléer en cas d'attrition. Ceci est vrai dans tous les segments mentionnés (observation, communications, liaison de données). Autre exemple, la start-up française Unseenlabs permet de géolocaliser des navires grâce à sa constellation de nanosatellites et ce en détectant leurs émissions électromagnétiques passives, contribuant ainsi à la transparence du domaine maritime[117].

113. Mais l'IA pourrait justement faciliter ce travail.
114. Les 13 satellites militaires patrimoniaux, voir X. Pasco et P. Wohrer, « La mise en œuvre de la stratégie spatiale de défense française : vers la maîtrise de l'espace », Note n° 12, Fondation pour la recherche stratégique, avril 2023.
115. Voir « Rapport d'information n° 506 (2019-2020) », Délégation parlementaire au renseignement, juin 2020, p. 199-212.
116. M. Borowitz, « The Military Use of Small Satellites in Orbit », *Briefings de l'Ifri*, Ifri, 4mars 2022.
117. J. Bachelier et P. Boulanger, « La fusion de l'information : levier de la puissance maritime française ? », *Briefings de l'Ifri*, Ifri, 7 décembre 2023.

Schéma II-2 : La permanence et l'ubiquité de la surveillance aérienne et spatiale



La démocratisation de l'accès à la transparence

La transparence peut donc s'appuyer, en sus des moyens militaires souverains, sur une pléthore de moyens civils, satellites comme drones[118] (*cf. supra*), antennes de réseaux 4G/5G, objets connectés, etc., donnant l'impression d'un phénomène indépassable. En effet, si ces objets sont bien moins protégés ou sophistiqués que leurs homologues militaires, leur simple masse semble leur donner un caractère inépuisable et le réseau afférent de start-ups imprime un rythme d'évolutions tel qu'il semble que l'on puisse toujours y puiser une solution idoine pour fournir des services ayant trait à la transparence, si celle-ci se trouvait en partie empêchée.

Cette démocratisation de l'accès à la transparence se conjugue aussi dans le recueil d'informations en source ouverte (OSINT). Le phénomène n'est pas nouveau[119], l'OSINT étant considéré comme un grand pourvoyeur de renseignement[120]. Là encore, le conflit russo-ukrainien a joué le rôle de révélateur et d'accélérateur. Des analystes civils, souvent organisés en

118. P. Cheminade, « Quand les militaires draguent les drones civils », *La Tribune*, octobre 2023.
119. J. Henrotin, « Les mutations du renseignement militaire, dissiper le brouillard de la guerre ? », *op. cit.*
120. Voir à ce sujet le n° 186 d'*Hérodote* « OSINT : Enquêtes et terrains numériques », 3e trimestre 2022.

communautés « d'osinteurs[121] », sont capables de suivre les actions tactiques selon un degré de granularité inaccessible auparavant. Les réseaux sociaux donnent une caisse de résonance à leurs productions. Un site comme *oryxspioenkop.com* peut documenter de façon étayée les pertes de matériels russes. Un autre, *understandingwar.org*, diffuse des cartes de situation et des appréciations opérationnelles qui rappellent un travail d'état-major.

Sur le terrain, les combattants utilisent des applications issues du monde civil. Les Ukrainiens par exemple exploitent l'application mobile « DIIA », elle-même hébergeant l'application « Delta » permettant d'échanger en temps réel des données tactiques[122]. Une douzaine d'autres logiciels leur sont disponibles comme MilChat (messagerie sécurisée) ou MyGun (calculateur balistique). Les données peuvent être géoréférencées et horodatées ; elles concourent au raccourcissement de la boucle du ciblage, facilitant la destruction d'unités. Le smartphone devient un outil essentiel du champ de bataille, à la fois arme et cible parfaite. Cette démocratisation de l'accès à la transparence peut évidemment bénéficier à des acteurs non étatiques, les autorisant à mener des actions de combat sans être soutenus par les moyens militaires conventionnels *ad hoc*[123] : la transparence joue aussi en faveur d'adversaires infra-étatiques capables d'adaptation réactive[124].

Pour conclure sur le recueil d'informations, on peut noter que chacun des phénomènes décrits (drones, satellites, OSINT…) semble s'auto-soutenir et s'auto-entretenir. Les satellites apparaissent au cœur de ce « système de systèmes de recueil », ne serait-ce que par la connectivité qu'ils assurent à la fois aux capteurs et aux effecteurs. Toutefois, la qualité du recueil n'est décisive qu'à la condition où les informations transmises sont exploitées correctement.

De la transparence physique à la transparence cognitive

Des quatre phases qui constituent le cycle du renseignement[125], la phase d'exploitation, par essence cognitive, est centrale si l'on veut un appui renseignement efficace. Là aussi, les progrès techniques sont impressionnants, notamment du fait de l'intelligence artificielle.

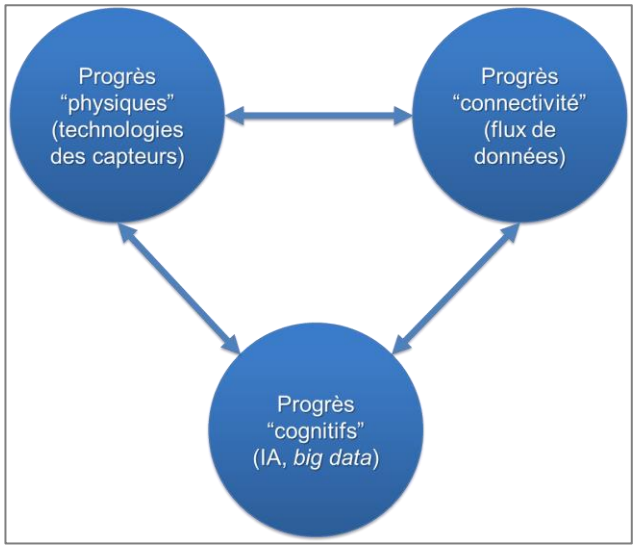
Si la capacité d'exploitation d'une trop grande masse d'informations peut s'avérer hors de portée d'un analyste humain, celui-ci bénéficie

121. Voir auditions de la Commission de la défense nationale et des forces armées : « Enjeux, à travers l'exemple ukrainien, du renseignement d'origine sources ouvertes (OSINT) », 23 novembre 2022.
122. Général J. M. Wasielewski, « L'emploi de la cyber-électronique en Ukraine », *Revue Défense Nationale*, n° 859, avril 2023.
123. Voir J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, Nuvis, 2014.
124. K. Crombe et J. A. Nagl, « A Call to Action: Lessons from Ukraine for the Future Force », *Parameters*, n° 3/53, automne 2023.
125. Orientation, Recherche, Exploitation, Diffusion.

désormais d'aides logicielles diverses. L'IA peut ainsi aider à extraire du *big data* les éléments les plus pertinents, répertoriant et sélectionnant au mieux les données (*data mining*). Elle laisse l'analyste se concentrer sur les dimensions les plus complexes à démêler, requérant jugement, culture générale ou nécessitant de croiser des compétences pointues, pluridisciplinaires. Par exemple, des dossiers d'objectifs où il s'agit de modéliser les *patterns of life*[126] de groupes terroristes sur foi de différentes statistiques peuvent être en partie réalisés par un soutien de l'IA : l'algorithme se chargera plutôt du spectre bas à moyen de l'échelle cognitive, l'opérateur humain se concentrant sur les aspects les plus complexes de l'analyse. Les cas d'usage montrent que l'IA est particulièrement efficace dans l'analyse (ou préanalyse) des données imagerie ou des données/signaux acoustiques. L'analyste est ainsi amené, lui et son organisation, à faire plus vite et mieux, se concentrant sur la réflexion à haute valeur ajoutée.

Des processus d'état-major peuvent être mis au point pour tirer tout le parti de ces progrès. À la fois capacité et technique de travail collaboratif, le GEOINT[127] agrège des données pluridisciplinaires (multicouches et multicapteurs) et géoréférencées. La fusion de ces données issues de différentes couches d'analyse superposées permettent une exploitation très élaborée.

Schéma II-3 : Les progrès cumulatifs de la transparence



126. Étude des habitudes, voire de l'organisation sociale d'un groupe donné, généralement à des fins de ciblage.
127. J. Bachelier et P. Boulanger, « La "fusion de l'information" : levier de la puissance maritime française ? », *Briefings de l'Ifri*, Ifri, 7 décembre 2023.

Tromper la transparence : tout un éventail de duperies

Si les technologies et équipements favorisant la transparence ont connu des développements sans précédent, donnant une impression d'ubiquité et de permanence du recueil de renseignement, il ne faut pas pour autant mésestimer les progrès, certes pour l'heure moins rapides, intervenant pour s'en protéger. Trois familles techno-capacitaires existent pour contourner la transparence : la dissimulation, la métamorphose, la perturbation. *In fine*, il reste l'option de l'élimination des moyens l'autorisant.

Un recueil altéré

Pouvoir mieux se dissimuler

Se dissimuler relève autant de savoir-faire collectifs que de progrès technologiques permettant de se rendre, au moins en partie, invisible. On augmente ainsi sa probabilité de survie.

Sur le plan technologique, de nouvelles formes de camouflage apparaissent, à divers degrés de maturité technique. Plusieurs initiatives vont en ce sens en France. Parmi elles, dans le domaine terrestre, le combattant pourra bénéficier du « bariolage multi-environnement » (BME), tenue de camouflage adaptable à plusieurs types de milieux. Le BME est conçu comme un trompe-l'œil dont on attend qu'il génère un temps de détection accru de 25 %[128]. Encore n'est-il considéré que comme le précurseur d'un futur treillis composé de textiles intelligents, auto-adaptables à l'environnement direct, à la manière d'un caméléon. Le système CAMTAC (camouflage tactique) est quant à lui constitué d'un kit de stickers à installer sur un véhicule pour en casser les formes et en retarder la détection[129]. Un camouflage plus efficace encore cherchera à compliquer la détection dans plusieurs champs de signatures, signature visuelle certes, mais aussi thermique (dans la bande de fréquence infrarouge), voire radar, et ce afin de leurrer plusieurs types de capteurs. C'est l'ambition du système de camouflage multispectral Barracuda MCS de Saab sous la forme de filet. Sur un autre plan, le pouvoir obscurcissant des obus fumigènes peut être largement amélioré[130] et peut même absorber ou dévier les lasers[131]. Enfin, la signature acoustique des véhicules peut tirer parti de moteurs plus discrets (hybrides ou électriques).

128. N. Gain, « Vers un bariolage multi-environnement unique pour les armées françaises », *FOB*, mai 2022.
129. N. Gain, « Eurosatory 2022 : l'armée de Terre veut passer à l'échelle sur le futur camouflage de ses véhicules », *FOB*, juin 2022.
130. R. Hémez, « Derrière un écran de fumée. Perspectives sur l'emploi des fumigènes dans la manœuvre terrestre », *DSI*, n° 168, décembre 2023.
131. R. Hémez, « Opérations de déception. Repenser la ruse au 21e siècle », *Focus stratégique*, n° 81, Ifri, juin 2018, p. 46.

Dans les domaines plus fluides, aérien ou maritime, les progrès de la dissimulation s'appuient essentiellement sur la furtivité, grâce aux technologies liées au *RAM* (*Radar-Absorbent Materials*) qui réduisent l'écho radar renvoyé par les plateformes et modifient la forme perçue de l'objet observé. La classe de frégate La Fayette avait été précurseur de cette technologie dans le domaine naval, il y a plus de trente ans (principe de diminution de la surface-équivalente-radar ou SER). Le F-35 en est aujourd'hui l'illustration la plus emblématique dans le domaine aérien. Là encore, il s'agit davantage de compliquer ou retarder la détection plutôt que de produire une parfaite « cape d'invisibilité ». Dans le milieu sous-marin, les revêtements anéchoïques réduisent ou déforment les ondes sonar réfléchies et atténuent les propres sons du submersible.

Se transformer pour leurrer

Plus subtile que la stricte dissimulation, la modification de sa propre apparence peut permettre non plus seulement de se cacher mais de duper l'adversaire. Dans le milieu terrestre, la Direction générale de l'Armement (DGA) coordonne depuis plusieurs années le projet Caméléon-Salamandre pour offrir aux véhicules un camouflage cryptique[132]. Au-delà, ce projet ambitionne de leur donner une autre apparence, grâce à un système intelligent d'écrans pixelisés, piloté par un algorithme d'IA capable de leur générer une signature différente. Le système *Adaptiv* de BAE met déjà en œuvre ce type de principe, mais dans une gamme limitée de signatures infrarouges. Il utilise un revêtement de briques thermo-réactives modifiables par l'ordinateur de bord : un char observé en caméra thermique se transforme alors en simple voiture. Plus simple et plus économique, les leurres peuvent simuler la présence fictive de matériels. Le CAESAR possède désormais une version gonflable produite par la société tchèque Inflatech[133] qui est en outre capable d'en reproduire la signature thermique tout en imitant sa surface équivalente radar, cette combinaison d'artifices rendant le leurre beaucoup plus crédible.

Les capacités de leurrage dans le combat aérien font l'objet de récents efforts. Il existe déjà des « appâts » non pilotés, comme l'ADM-160 MALD (*Miniature Air-Launched Decoy*) de Raytheon. Ce leurre duplique la signature et le profil de vol d'un aéronef de combat. Il incite ainsi les systèmes de défense aérienne à se dévoiler, facilitant en retour leur destruction par les « vrais » chasseurs, placés à plus grande distance dans le cadre d'une mission SEAD (*Suppression of Enemy Air Defences*) ; le MALD en version brouillage peut compléter l'action. Le perfectionnement de ce schéma sous-tend les réflexions entourant le développement des futurs standards de l'aviation de

132. Cryptique : dans le monde animal ou végétal, un camouflage est dit cryptique dès lors qu'il permet de se fondre dans son milieu naturel.
Pour une application militaire, voir L. Lagneau, « Révolutionnaire, le camouflage adaptatif en milieu terrestre pourrait être prêt en 2025 », *OPEX360*, novembre 2021.
133. N. Gain, « Faux CAESAR et autres idées pour doter l'épée d'un bouclier », *FOB*, décembre 2023.

combat, avec un partage de tâches plus intégré entre l'aéronef et ses *loyal wingmen* (ailiers), grâce à une architecture numérique commune. Ainsi, ces ailiers peuvent venir tester le réseau de défense sol-air (leurres), le saturer (vol en essaim coordonné par une IA)[134], le perturber (brouillage) et entamer l'attrition (feux air-sol). La transparence du système défensif serait alors au moins altérée, au mieux rendue inopérante. Les aéronefs habités pourraient alors porter l'estocade finale.

Perturber, dégrader ou éliminer les capteurs

Les capteurs ont pour point commun de dépendre, à divers titres, du spectre électromagnétique. En le perturbant, la guerre électronique (GE) peut altérer, voire interdire le recueil d'informations. Le brouillage des moyens adverses est un procédé efficace, à condition, comme l'enseigne le théâtre ukrainien, de l'utiliser sans brouiller ses propres systèmes. Il est d'autant plus aisé que le capteur est rudimentaire, comme un drone bon marché[135]. Des techniques de déception électronique telles que le *spoofing* (leurrage du signal qui indique alors une vitesse relative ou un positionnement erroné du vecteur) peuvent être employées[136]. Outre les moyens de recueil, c'est bien l'ensemble du système de systèmes permettant la transparence qui peut être perturbé[137] : capteurs, PC où les informations sont reçues et fusionnées, effecteurs. La sauvegarde de la liaison de données, essentielle, met en lumière la nécessité de dominer le spectre électromagnétique pour garantir le fonctionnement de la chaîne C4ISR (*Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance*), certes des trois milieux classiques (terre, air, mer) mais plus encore l'intégrité de la liaison entre eux et le milieu spatial. Les perturbations électromagnétiques peuvent être complétées par des agressions cyber. Étroitement coordonnés, les effets GE et cyber produisent des actions « cyber-électroniques[138] », un champ en développement mais prometteur.

D'autres moyens non cinétiques peuvent dégrader les capteurs, en particulier les optiques ou les antennes : les armes à énergie dirigée (AED). Lasers ou armes à micro-ondes connaissent des perfectionnements, mus par le souci de détruire les drones dont l'impact tactique et psychologique (sentiment d'être nulle part à l'abri) a été révélé par les conflits du Haut-Karabakh et d'Ukraine.

134. De tels vols ont déjà été expérimentés, à l'exemple des essaims de Gremlins - X61.
135. « Les systèmes de lutte anti-drones [russe] comme le Shipovnik-Aero permettent d'abattre plus de 50 % des 10 000 drones ukrainiens détruits par mois », *in* J. Henrotin, « La loi de programmation, militaire face aux leçons de la guerre en Ukraine », *DSI*, HS n° 191, août-septembre 2023.
136. P. Gros, « Les opérations en environnement électromagnétique dégradé », Note n° 357, Fondation pour la recherche stratégique, mai 2018, p. 10-11 ; P. Gros « Navigation Warfare et positionnement, navigation, synchronisation (PNT) », Note n° 3, Rapport n° 193, Observatoire des conflits futurs, mai 2022.
137. Et notamment les nœuds C4ISR, garants du fonctionnement de l'ensemble.
138. O. Letertre, P. Justel, R. Lechâble et S. Dossé, « Regards croisés sur la guerre électronique », *Focus stratégique*, n° 90, Ifri, juillet 2019.

S'agissant de la mise en œuvre cohérente de ces différents moyens, de nombreuses réflexions sont actuellement menées dans le cadre de la lutte anti-drones (LAD), afin de déterminer le meilleur rapport coût-efficacité. Le cadre en est encore ouvert, plusieurs combinaisons étant envisageables, mixant armes à impulsion électromagnétique (canons micro-ondes)[139], systèmes laser à haute énergie[140], canons antiaériens à grande cadence de tir, dont systèmes CIWS[141], drones tueurs de drones[142], sans être exhaustif. À une autre échelle, lasers et AED peuvent être employés contre les satellites (éblouissement, surchauffe des composants…)[143].

Les capacités et technologies actuelles, en développement ou envisageables à court et moyen termes laissent donc entrevoir une grande variété de procédés pour tromper ou tout au moins réduire l'acuité de la transparence en s'attachant à altérer le recueil de renseignement. Les effets obtenus se déclinent sous des aspects plus ou moins complexes allant de la dissimulation au leurrage, de la perturbation à l'élimination des capteurs.

Une analyse tronquée

Si le recueil peut être perturbé, il en est de même du traitement des informations, à la différence que pour celui-ci, la perturbation peut être auto-générée ou provoquée par l'adversaire.

Le risque d'emballement

Les conditions favorisant la transparence cognitive secrètent leurs propres inconvénients. Le déluge informationnel, ou infobésité, porte le risque de saturer les capacités d'exploitation, même si des algorithmes permettent de mieux trier et pré-analyser un volumineux flux entrant. En effet, l'analyse exige une part cruciale de discernement, qui demeure à ce jour l'apanage de l'humain et qui permet de repérer l'essentiel pour rejeter l'accessoire, de sélectionner les signaux faibles dignes d'intérêt sans se laisser décentrer par le « bruit informationnel ». D'autre part, ce sont des humains qui nourrissent les données de l'IA, celle-ci importe donc pour partie leurs biais cognitifs dans ses algorithmes[144]. Également, les logiciels d'aide à l'exploitation

139. Leonidas d'Epirus ou Thor, voir site meta-defense.fr.
140. Expérimentation américaine d'un blindé Stryker doté d'un laser d'une puissance de 50 Kw ; voir : F. Wolf, « L'US Army percevra ses premiers DE-SHORAD laser Guardian cette année », *Meta Defense*, 14 janvier 2022, disponible sur : https://meta-defense.fr.
Pour une vision plus globale sur les armes à énergie dirigée, consulter P. Gros, N. Vilboux, F. Coste, S. Delory et A. Bondaz, « La compétition dans les technologies de rupture entre les États-Unis, la Chine et la Russie », Observatoire de la politique de défense américaine, Fondation pour la recherche stratégique, juin 2019, p. 26-32.
141. Close-In-Weapons Systems.
142. G. Powis, « Coyote, le drone américain spécialisé dans la destruction de drones », *Air&Cosmos*, novembre 2023.
143. T. Fouillet, *La Guerre au XXIe siècle. Le retour de la bataille, op. cit.* p. 277.
144. J.-C. Noël, « Comment l'intelligence artificielle va transformer la guerre », *Éditoriaux de l'Ifri*, Ifri, 5 novembre 2018.

peuvent créer une forme d'addiction. L'analyste doit aussi pouvoir raisonner par lui-même, ne serait-ce qu'en cas de dysfonctionnement ou de déni de service de ses outils cognitifs. La surinformation peut enfin créer un effet de retenue et inhiber l'analyste qui attend « l'information de plus » avant de prévenir le décideur ; incapacité de ce dernier à arbitrer, car attendant « l'ultime information » pour lever un doute[145]. Acquérir une information obéit à un cercle vicieux qui réclame toujours plus d'informations pour préciser les premières.

La surprise de l'appareil sécuritaire israélien face à l'attaque du Hamas du 7 octobre 2023 est emblématique des phénomènes évoqués. Avec un appareil de renseignement considéré parmi les plus performants au monde, Israël jouit d'une réputation de *start-up nation* particulièrement innovante, y compris dans le domaine de l'IA. Le Hamas, adversaire connu de longue date, est concentré sur une infime portion géographique, la bande de Gaza, *a priori* facile à surveiller. Or, si certains analystes avaient pu mettre en garde, arguant de la conjonction de plusieurs indices, leurs avertissements n'ont pas été pris en compte[146], noyés dans de trop nombreuses hypothèses informationnelles et victimes de différents biais cognitifs, que de rigoureuses mesures SECOPS (Sécurité des Opérations)[147] du Hamas ont confortés. Certaines corrélations peuvent ici être faites avec l'attaque du 11 septembre 2001[148].

Les beaux jours de la manipulation

Outre ces erreurs endogènes d'interprétation, l'analyse peut être pervertie à dessein par l'adversaire, notamment par des actions cyber. Les données peuvent être corrompues[149], biaisant l'apprentissage algorithmique de l'IA à l'insu de l'analyste. Ce dernier a donc tout intérêt à garder la distance nécessaire par rapport au résultat présenté. Pour autant, « l'empoisonnement des données » demeure complexe sur un réseau sécurisé. Plus aisée, une attaque en déni de service empêchera un accès aux données[150]. L'adversaire peut aussi introduire un *malware* espion : le travail des analystes ne sera pas perturbé, mais profitera à l'adversaire, faisant basculer la transparence à son profit.

Les nouvelles technologies de la sphère informationnelle peuvent viser non plus les analystes, mais les décideurs, ou mieux encore, les opinions publiques dont la cohésion est essentielle au niveau stratégique. Cette « ère de la post-vérité » est favorisée par les possibilités techniques de désinformation ou d'intoxication, via le *deepfake* par exemple ou plus généralement *via* les réseaux sociaux (« influenceurs » pilotés par des États

145. Général M. Yakovleff, auditions de la Commission de la défense nationale, *op. cit.*
146. « Selon le *New York Times*, Israël avait eu vent des plans du Hamas », *Le Figaro*, 1er décembre 2023.
147. « Sécurité des opérations » : capacité à agir dans la clandestinité, protection du secret.
148. E. Harding, « How Could Israeli Intelligence Miss the Hamas Invasion Plans? », *CSIS*, octobre 2023.
149. C. Bômont, « Le *cloud* défense. Défi opérationnel, impératif stratégique et enjeu de souveraineté », *Focus stratégique*, n° 107, Ifri, novembre 2021, p. 37.
150. *Ibid.* p. 37.

malveillants, *trolls,* etc.). Ces procédés manipulateurs bénéficient en outre d'un contexte où les sociétés sont en proie au doute systématique, tout en entretenant un « goût pour les récits contradictoires[151] ». La confusion médiatique autour du tir du 17 octobre 2023 sur l'hôpital Al Ahli de Gaza illustre une partie de ces dangers. Immédiatement attribuée à Tsahal par de nombreux organismes de presse, sans recoupement, cette frappe a suscité une vive indignation, l'information se répandant de manière virale. Cette attribution a fait place peu après à de larges doutes, un incident de tir du djihad islamique étant finalement considéré comme une cause plus probable. Le plus important est que la diffusion peu rigoureuse d'une information très sensible a donné prise à une exploitation politique immédiate des passions afin d'obtenir un avantage stratégique[152] : le discrédit de Tsahal. Deux parties en conflit étant en permanence tentées de biaiser le traitement d'une information capitale, la difficulté à interpréter les faits avec lucidité s'en trouve accrue, notamment avec des opinions publiques tendant à ne retenir que les éléments qui concourent à leurs présupposés.

On le voit, cette guerre cognitive, cherchant à altérer le jugement des acteurs militaires, décideurs ou opinions publiques, donne largement le change à la transparence du champ de bataille.

Prime à la transparence dans le champ physique, prime à l'opacité dans le cognitif

La confluence de trois dialectiques : technologique, tactique et stratégique

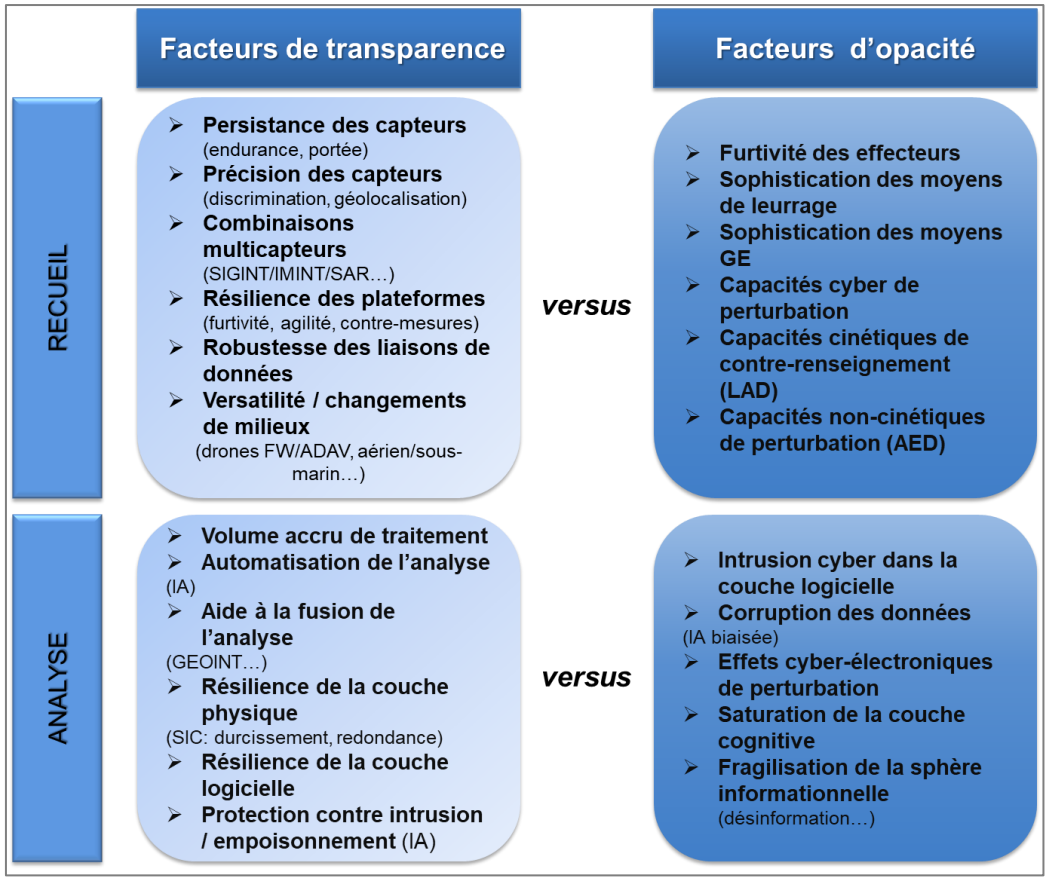
Il ressort de cette analyse essentiellement techno-capacitaire du rapport entre transparence et opacité qu'il existe une différence de nature selon que l'on considère ce qui relève du recueil (critères « physiques ») de ce qui relève de l'analyse (critères « cognitifs »). Des multiples interactions entrevues, on peut déduire qu'il existe, aujourd'hui, une prime à la transparence dans le champ physique (qualités et redondance des capteurs) et une prime à l'opacité dans le champ cognitif (multiples leviers d'intoxication). Comment ce rapport est-il amené à évoluer, étant entendu qu'il dépend de paramètres fluctuants ?

Le phénomène de transparence évolue d'abord au gré des progrès techniques. Si des technologies favorisant la transparence donnent un avantage trop net à un protagoniste, l'adversaire concentrera en réaction ses efforts pour trouver une parade. Une fois trouvé cette parade, une contre-

151. D. Papalardo, « La guerre cognitive : agir sur le cerveau de l'adversaire », *Le Rubicon*, décembre 2021.
152. O. Ubertalli, « Hôpital de Gaza : anatomie d'un naufrage médiatique », *Le Point*, 20 octobre 2023. Voir également D. Leonhardt, « Revisiting the Gaza Hospital Explosion », *The New York Times*, 3 novembre 2023, disponible sur : www.nytimes.com.

réaction s'enclenchera pour élaborer une contre-parade[153], et ceci selon un cercle sans fin. Luttwak décrit très bien ce processus[154], arguant qu'il est rarement rentable de surinvestir sur un avantage précis, puisqu'il finira par être contrecarré. Réfléchir au rapport transparence-opacité implique de prendre en compte un spectre très large de technologies (voir tableau ci-dessous pour une lecture simplifiée de cette dialectique). Nombre de ces technologies sont l'objet d'efforts de recherche de la part d'écosystèmes de PME parmi les plus innovantes, ajoutant au caractère mouvant des équilibres obtenus à un instant donné. On en conclut que l'évolution sur cinq à dix ans de chaque élément de ce spectre n'est pas identifiable avec certitude. Le rapport transparence-opacité devrait donc être fluctuant, dépendant des investissements des principales puissances militaires et des percées technologiques qui, par essence, ne sont pas déterminables à l'avance. D'ici cinq à dix ans donc, un hypothétique conflit interétatique de haute intensité ne façonnera probablement pas le même rapport transparence-opacité que le conflit russo-ukrainien.

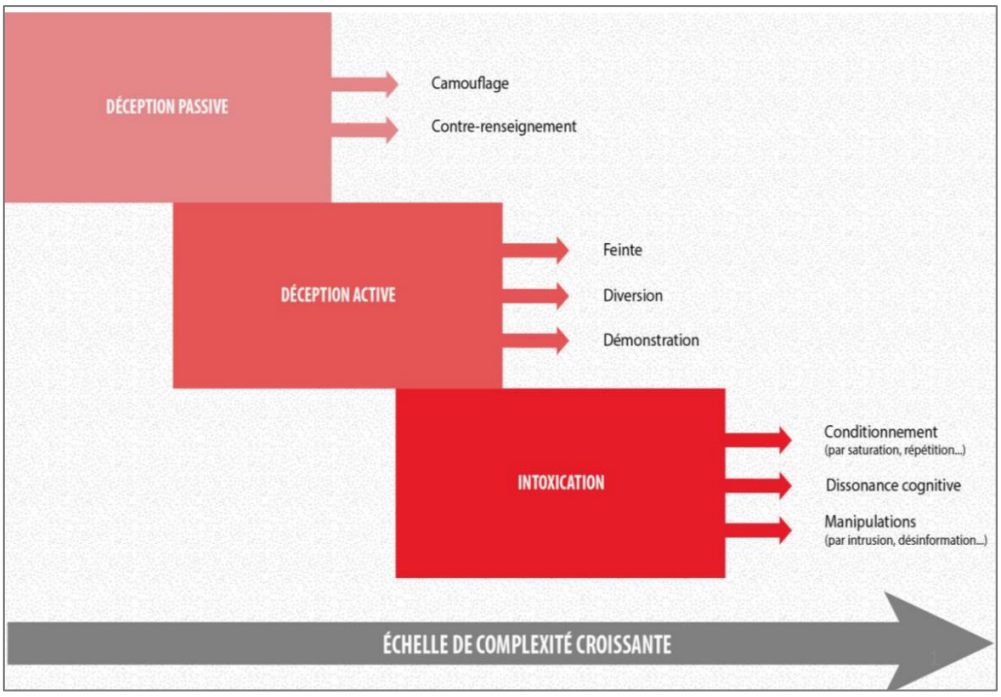
Schéma II-4 : La dialectique transparence-opacité



153. E. Hardy, « La stratégie militaire et le champ opérationnel des compétitions technologiques », *op. cit.*
154. E. Luttwak, *Le Paradoxe de la stratégie*, Paris, Odile Jacob, 1989.

Ensuite, si la transparence perdurait, avec la létalité qui l'accompagne, elle engendrerait, et engendre déjà, des adaptations tactiques. Réapprendre la déception apparaît à cet égard crucial[155]. À ce titre, l'armée de Terre a entièrement réécrit sa doctrine sur la déception en 2024, tenant compte de la réalité d'une transparence accrue du champ de bataille tout en insistant davantage sur la palette d'effets psychologiques qu'elle contribue à créer malgré ou parfois grâce à cette visibilité augmentée. Rappelons que la déception se décline en trois modes.

Schéma II-5 : Les trois modes de la déception



© Guillaume Garnier/Ifri, 2024.

Son efficacité est conditionnée par la combinaison de tout ou partie de ces modes, une combinaison rigoureusement planifiée et dont l'exécution rend la ruse crédible. Il s'agit alors d'inventer un art du subterfuge du XXIe siècle, avec les technologies à disposition et surtout une préparation opérationnelle (doctrine, entraînements) soignée. Se rendre imprévisible, instiller un doute permanent dans le camp opposé compliquera ses calculs, surtout s'il connaît la propension de son adversaire à utiliser la déception. Dès lors, un avantage acquis en matière de transparence sera en partie contourné et ne pourra imprimer à lui seul un résultat décisif.

Le rapport transparence-opacité évoluera enfin en fonction du contexte stratégique. Un contexte de « paix armée » favorisera l'opacité cognitive : des modes d'agression « hybrides » s'appuieront sur une déception fabriquant de l'ambiguïté (intoxication, difficultés d'interprétation). Un tel contexte

155. R. Hémez, « Opérations de déception. Repenser la ruse au 21e siècle », *op. cit.*

devrait privilégier les technologies permettant de neutraliser ou dégrader sournoisement des équipements stratégiques avec des moyens non létaux (cf. partie 4). En revanche, si un conflit majeur se déclenchait entre grandes puissances, qu'il intervienne en Europe ou en Asie, les protagonistes porteraient leurs efforts sur d'autres technologies, afin de s'assurer la supériorité opérationnelle. De cette compétition naîtrait un autre rapport transparence-opacité, qui affecterait aussi les puissances « observant » le conflit, par le truchement du retour d'expérience.

Les limites de la transparence

Au terme de cet exercice comparatif, le rapport transparence-opacité apparaît fluctuant pour les années à venir. Les limites de la transparence du champ de bataille peuvent être considérées selon quatre cas d'espèces, présentés de manière graduée et qui permettent de relativiser son omnipotence supposée.

- **Situation 1 : « Je vois tout, mais je ne comprends pas ».**

Dans ce premier cas, l'erreur d'interprétation sur l'intention adverse est auto-générée, par un défaut d'analyse, lui-même causé par une surinformation, un processus décisionnel inefficient ou plus prosaïquement une grave prise en défaut du commandement (biais cognitifs, perte de jugement). Même les technologies les plus en pointe du XXIe siècle ne permettent pas de se prémunir contre ce type d'écueil. On peut ajouter que ce cas est le plus propice à la sidération : une trop grande confiance accordée à la transparence, déjouée par ses propres erreurs, aura tout lieu de provoquer une crise morale difficile à surmonter.

- **Situation 2 : « Je vois la plus grande partie du théâtre d'affrontement, mais je rate l'essentiel ».**

Il y a ici aussi une erreur d'interprétation, mais elle est provoquée par l'adversaire, ce dernier agissant dans le premier mode de déception (« passif »), la dissimulation. Il parvient à cacher les éléments qui sont décisifs à la mise en œuvre de son mode d'action et complète cette dissimulation par des actions de saturation d'informations pour empêcher l'appareil de renseignement adverse de détecter les indices clés.

- **Situation 3 : « Je crois tout voir et tout comprendre, mais je suis intoxiqué ».**

Ce cas de figure est proche du deuxième, mais plus élaboré. L'adversaire utilise des modes de déception plus subtils. Ce qui est vu est erroné (déception active) et ce leurrage est accompagné d'une intoxication savamment orchestrée. Dès lors, l'interprétation porte à faux. La sidération consécutive au subterfuge global constitue là aussi une épreuve morale pour celui qui la subit, lézardant potentiellement la cohésion (au sein du commandement, entre le commandement et l'appareil de renseignement, etc.).

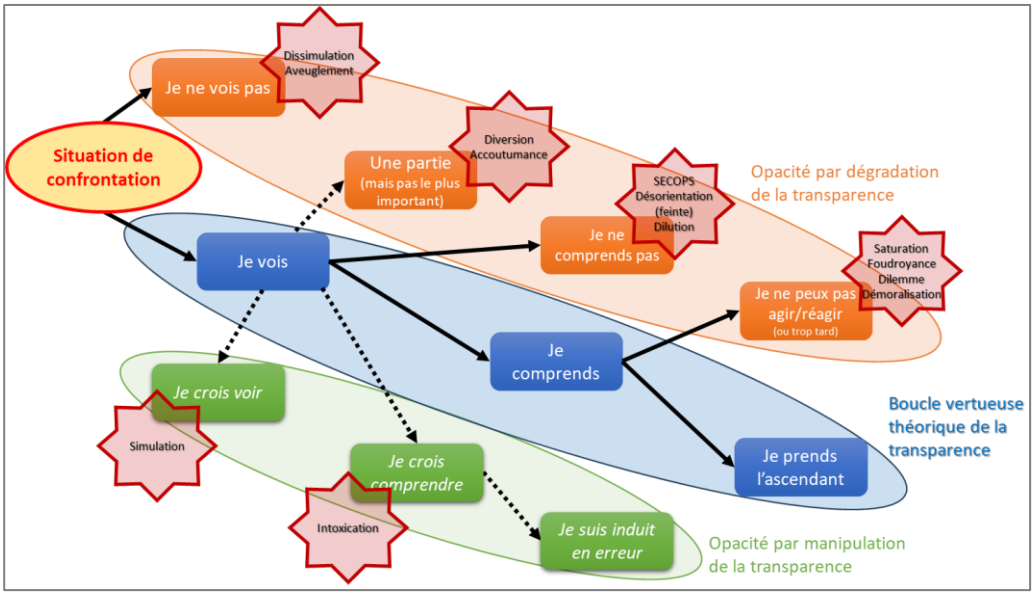
Situation 4 : « Je vois tout, je comprends correctement, mais je ne peux (ré)-agir ».

La transparence a pleinement rempli son rôle, l'appréciation de situation opérationnelle est correctement réalisée. Cependant, les efforts capacitaires pour garantir l'accès à la transparence du champ de bataille ont provoqué des effets d'éviction dans d'autres champs capacitaires. Au final, je manque de moyens pour (ré)-agir et je reste « spectateur de la transparence ».

Une variante de la situation 4 est une paralysie provoquée par l'adversaire, soit par la fugacité de sa manœuvre, trop rapide pour être contrée, soit parce qu'il neutralise au moment décisif notre système nerveux (frappes et cyberattaques), nous aveuglant et dégradant nos nœuds C4ISR.

Les quatre situations proposées laissent entrevoir de nombreuses possibilités pour contourner, voire invalider la transparence. Toutefois, à part les cas où l'erreur est auto-générée, les autres situations impliquent de maîtriser des savoir-faire complexes. Jouer contre la transparence exige le meilleur niveau opérationnel, la meilleure vivacité d'esprit. Le défi n'est pas à sous-estimer.

Schéma II-6 : Plasticité du rapport transparence-opacité



© Pierre Néron Bancel/Ifri, 2024.

En conclusion, cette revue techno-capacitaire permet de mieux saisir la complexité des interactions entre transparence et opacité. Si ce rapport est plus ambigu qu'il n'y paraît, il reste que la transparence s'impose comme un facteur-clé du champ de bataille. Au-delà des solutions technologiques pour dégrader la transparence ou la leurrer, trois approches se distinguent pour repenser la manœuvre en tenant compte de cette nouvelle réalité du champ de bataille.

Combattre dans un champ de bataille plus transparent : un défi plutôt qu'une impossibilité

Élaborer une manœuvre militaire exige de pouvoir concentrer des moyens[156], surprendre au moins partiellement l'adversaire, dissimuler ses éléments les plus indispensables à l'action : autant d'impératifs qui semblent difficilement réalisables dans un contexte de transparence.

Un certain nombre de conditions doivent être remplies pour regagner malgré tout de la liberté d'action. Une nouvelle façon de concevoir la manœuvre doit d'abord mettre l'accent sur la sûreté, ne serait-ce que pour échapper au triptyque détection/acquisition/destruction. Emporter la supériorité informationnelle dans un souci d'intégration multi-milieux/multi-champs (M2MC[157]), tel que voulue par les armées françaises, s'avérerait tout aussi nécessaire. Enfin, inventer de nouvelles formes de surprise pour déjouer la transparence compléterait ces exigences. Ainsi, acquérir la supériorité opérationnelle tout en sachant recréer de l'incertitude dans un champ de bataille rendu plus limpide demeure possible, mais exige une grande compétence du système de forces.

Disparaître des écrans pour survivre : se réapproprier la sûreté

Sur la « ligne zéro » du front ukrainien[158], la survivabilité d'un véhicule est actuellement estimée à moins de dix minutes[159]. Le premier enjeu de l'engagement dans un milieu transparent est donc de survivre avant même de combattre. En appliquant la logique des couches de survivabilité décrite plus haut, recréer une forme d'opacité suppose d'abord de minimiser la surface de détection puis de minimiser la vulnérabilité des systèmes.

---

156. Principe de « concentration des efforts », parmi les trois principes du Maréchal Foch.
157. Le concept M2MC traduit la prise en compte dans la doctrine française des différents milieux (terre, air, mer, espace, cyber) et champs (électromagnétique et informationnel) et de la nécessité de planifier une manœuvre intégrant les actions et effets dans ces différents milieux et champs.
158. Nom donné à la ligne immédiate de confrontation entre les armées sur le front ukrainien, voir : B. Mabillard et S. Shestak, « Guerre en Ukraine : dans l'enfer de la ligne zéro », *Le Point*, 7 février 2024, disponible sur : www.lepoint.fr.
159. Y. Trofimov, « Drones Everywhere: How the Technological Revolution on Ukraine Battlefields Is Reshaping Modern Warfare », *The Wall Street Journal,* 28 septembre 2023, disponible sur : www.wsj.com.

Échapper à la détection

Bien qu'il semble *a priori* impossible de ne pas être vu dans un environnement de combat de plus en plus saturé de capteurs en tous genres, échapper au filet de surveillance adverse reste possible, à condition de faire converger les solutions technologiques avec un retour aux fondamentaux tactiques : la dissimulation, la dispersion et la discrétion.

Au-delà des seuls progrès techniques du camouflage, la dissimulation des positions et des mouvements passe également par la capacité à exploiter « le pouvoir égalisateur des terrains difficiles[160] ». Pour le milieu terrestre, les zones naturellement opaques comme les terrains montagneux, les forêts denses ou la zone urbaine contraignent fortement la visibilité et la transmission des ondes. En zone urbaine particulièrement, il s'agit de pouvoir développer des capacités à combattre sous terre pour exploiter les réseaux souterrains. La maîtrise du combat souterrain par le Hamas à Gaza démontre que la capacité de combat suburbain, aujourd'hui l'apanage d'unités spécialisées dans la fouille opérationnelle (compétence du génie pour la reconnaissance des milieux confinés), gagnerait à être élargie au sein des forces terrestres pour pouvoir disposer d'une expertise approfondie du combat sous terre[161]. L'application de la robotique terrestre dans ce « milieu périlleux » pourrait ainsi bénéficier de la dynamique du programme Vulcain[162] de l'armée de Terre. Dans le domaine du combat aérien, l'exploitation du terrain se traduit par la capacité de pénétration basse altitude tout temps, qui repose sur un savoir-faire opérationnel et sur une solution technique de suivi de terrain. Maintenir cette aptitude rare et reconnue pour échapper aux radars adverses, voire l'ouvrir aux *Rafale* monoplaces de l'armée de l'Air et de l'Espace (AAE), garantirait à la force aérienne un éventail élargi d'options de furtivité et d'imprévisibilité[163].

Une plus grande dispersion des dispositifs est désormais rendue possible par la mise en réseau des unités de combat. Elle permet notamment la diminution des surfaces électromagnétiques et devient une solution viable pour la survie des PC terrestres, mais aussi des forces aéronavales dont la portée des effecteurs rend la concentration moins nécessaire sur le plan tactique. Il ne s'agit pas d'être invisible, simplement de ne pas paraître important pour ne pas justifier le coût d'une frappe. Des solutions techniques réalistes pour appuyer de nouveaux schémas de PC distribués émergent et pourraient limiter les besoins de regroupement des fonctions de commandement, telles que le recours à la réalité virtuelle et aux hologrammes pour limiter les réunions de commandement et de

160. H. Delort-Laval, « Hommes et haute technologie dans les engagements terrestres : vers un mariage de raison ? », *Inflexions*, vol. 4, n° 3, 2006, p. 113-124.
161. R. Franchet d'Esperay, « Combattre en milieu suburbain : la carte du génie », *Areion24.News*, 28 octobre 2023, disponible sur : www.areion24.news.
162. Programme de l'armée de Terre qui vise à concevoir les principes de l'intégration de la robotique dans le combat terrestre à l'horizon 2030-2040.
163. Entretien du 29 novembre 2023.

planification. L'accès à des « *clouds* de combat » rend possible la dissociation des fonctions conduites et planification avec la constitution de PC avancés légers appuyés par un PC principal en *reachback*[164]. De nouvelles formes d'ondes, comme la communication laser par satellite ou comme le *Lifi* (transmission de données par la lumière) peuvent également contribuer à diminuer significativement la signature et le poids logistique des PC ainsi que le temps nécessaire à l'échange de données. Technologie sans fil, le *Lifi* garantit un débit de 2 Gbits/s jusqu'à 5 mètres[165] et devrait fluidifier le déploiement des PC, dont le réseau représente aujourd'hui 8 kilomètres de câbles pour un PC division[166]. L'armée de Terre étudie actuellement comment adapter cette technologie à ses besoins opérationnels.

La discrétion, troisième aptitude pour échapper à la détection, repose en priorité sur l'adaptation des processus et des comportements pour minimiser la surface numérique à l'ère de l'hyperconnectivité. À l'échelle individuelle, elle passe par un comportement numérique sain et responsable vis-à-vis des objets connectés et des réseaux sociaux pour éviter la « numérisation subie du champ de bataille[167] ». Collectivement, l'hybridation des réseaux et des systèmes implique de redoubler de rigueur dans le respect des procédures SECOPS. Limiter la vulnérabilité induite par le rayonnement électromagnétique croissant d'unités de plus en plus intégrées aux réseaux de connectivité nécessite d'effectuer un virage vers une culture de la frugalité numérique pour se réapproprier « les leçons du silence[168] ». Acquérir le réflexe d'éteindre sa signature électromagnétique tout en s'entraînant à conserver sa capacité à commander et contrôler ses effets ne va pas de soi et semble même contre intuitif alors que c'est la connectivité qui garantit la supériorité informationnelle des systèmes de C2. En plus de contribuer à la discrétion, la maîtrise de ce savoir-faire permet de se préparer aux effets du brouillage offensif adverse. L'entraînement aux procédures « EMCON » (*emission control*, ensemble des mesures de réduction de la signature électro-magnétique) doit être considéré comme partie intégrante de l'entraînement au combat en réseau, à l'instar des exercices de type « POLARIS » de la Marine nationale[169] dans lesquels l'entraînement à la frugalité numérique est l'un des principaux objectifs.

La logique de frugalité doit également s'appliquer aux besoins en énergie avec de nouvelles solutions de stockage et de génération d'énergie moins volumineuses, et bien entendu au facteur humain. Dans l'idéal, le PC terrestre du futur exploitera les atouts de la connectivité pour se limiter à

164. « Expertise à distance » en français. Capacité à déporter des ressources ou des capacités en arrière de la zone d'engagement, y compris sur le territoire national.
165. « Le Li-Fi : une solution lumineuse pour les communications militaires ? », ITPublic, consulté le 15 février 2024, disponible sur : www.itpublic.fr.
166. Entretien avec un officier supérieur de l'armée de Terre, 12 décembre 2023.
167. A. Cattaruzza et S. Taillat, « Les enjeux de la numérisation du champ de bataille », *op. cit.*, p. 13.
168. E. Lanquetot, « Le silence relatif », *op. cit.*
169. Exercice interarmées et interalliés de grande ampleur visant à préparer un engagement naval de haute intensité.

quelques véhicules durcis qui pourront se connecter entre eux selon une logique multimodale et rester connectés aux réseaux de commandement malgré les élongations[170]. Les travaux de développement de nouvelles formes d'onde « furtives » à très faible débit pourraient offrir de nouvelles perspectives pour les systèmes de PC à plus long terme[171].

Schéma III-1 : Limiter la visibilité des systèmes de PC

		Vulnérabilités des PC actuels						
		Rayonnement multispectre	Elongations limitées	Empreinte au sol	Poids logistique	Inertie / délais de déploiement	Besoins en énergie	Connectivité complexe
Solutions possibles	Dissimulation	X	X	X				
	Dispersion	X	X	X	X			
	Modularité			X	X	X	X	X
	Allègement			X	X	X		
	Mobilité	X	X	X		X		
	Frugalité	X			X		X	
	Nouvelles formes de stockage d'énergie	X		X	X		X	
	Nouvelles formes d'onde	X	X			X		X
	Hybridité des SIOC	X	X					X

© Pierre Néron Bancel/Ifri, 2024.

Échapper à l'acquisition/destruction

À terme, la détection est cependant presque inéluctable, ce qui impose de développer des solutions complémentaires pour maximiser la survivabilité en dégradant la capacité de l'adversaire à exploiter son renseignement. Cette deuxième couche de sûreté repose sur les mesures de protection actives et passives, la mobilité et la perturbation de la boucle de connectivité adverse.

La protection la plus évidente pour le milieu terrestre est l'enfouissement, comme l'illustre le retour à la tranchée sur le front ukrainien. Creuser et s'enterrer exige de se réapproprier des savoir-faire oubliés et remet au premier plan le besoin d'un appui génie conséquent avec des moyens adaptés à la létalité du front[172], qui rend prégnant le besoin pour l'armée de Terre de disposer à nouveau d'un engin de combat du génie robuste adapté à la haute intensité. Le recours au milieu suburbain existant,

170. M. Beagle, J. Slider et M. Arrol, « The Graveyard of Command Posts », *op. cit.*
171. Entretien avec des officiers de l'EMA, 8 décembre 2023.
172. « Le combat de tranchée », *Légion étrangère,* consulté le 15 février 2024, disponible sur : www.legion-etrangere.com.

comme les parkings souterrains, offre des solutions de protection adaptées aux objets volumineux comme les PC. La protection passe également par le recours à tout ce qui peut gêner les capteurs, à commencer par les fumigènes. Le développement de solutions « *soft kill* », comme le système Pronoïa de Lacroix Défense adapte la protection des dispositifs à la menace nouvelle des munitions télé-opérées et des drones suicides grâce à des dispositifs de masquage et de brouillage multispectraux associés à des systèmes de détection, d'analyse et d'alerte embarqués. Enfin, la centralité de la connectivité impose d'élargir la fonction protection à celle des réseaux et des SIOC. En ce sens, l'hybridation des SIOC, permettant d'exploiter les réseaux de 4/5G civils, pourrait contribuer à renforcer la discrétion des communications et à rendre les systèmes de PC plus résilients, même si ce type de solution requiert une bonne connaissance préalable des réseaux civils dans la zone d'engagement[173].

La mobilité, voire la vitesse pour les milieux aériens et maritimes, est un facteur de survivabilité alternatif à la discrétion et à la furtivité qui permettent de jouer sur la temporalité en limitant le « segment d'intervisibilité[174] », c'est-à-dire la fenêtre d'acquisition d'une cible par la boucle renseignement-feu adverse, tout en retardant la compréhension de l'intention. Le facteur vitesse est autant inhérent à la manœuvre aérienne, qui se planifie à partir du rapport vitesse amie/délais de détection/vitesse de réaction adverse, qu'à la manœuvre navale qui mise sur sa capacité d'accélération pour fermer une fenêtre d'opportunité adverse en sortant du cercle de détection avant la phase d'acquisition.

Sur le champ de bataille terrestre, la mobilité, comprise comme la « capacité à manœuvrer au combat, sur tous les types de terrain et malgré les feux de l'ennemi[175] », est contrainte par la viscosité naturelle et artificielle due à la « désorganisation du terrain[176] », mais également par les frictions internes au déploiement et aux mouvements d'une grande unité comme la division. À titre d'illustration, une division Scorpion représente presque 10 000 véhicules[177], qui vont au cours d'une manœuvre se déployer, se relever, s'imbriquer, se dépasser, le tout sur un nombre contraint d'axes et potentiellement sous le feu. Une telle complexité de mouvements sous le regard de l'ennemi fait de la fonction « appui au mouvement » d'une grande unité un élément critique pour assurer la fluidité des mouvements et de la manœuvre, garantir un bon écoulement des flux et guider les unités sur leurs objectifs, malgré les obstacles et la friction de l'engagement terrestre.

173. Entretien du 12 décembre 2023.
174. F. Chamaud et P. Santoni, *L'Ultime champ de bataille, combattre et vaincre en ville*, Paris, Pierre de Taillac, 2016, p. 18.
175. A. Kranklader, « La mobilité d'une division engagée dans un combat de haute intensité : un facteur-clé du succès tactique », École de Guerre/Armée de Terre, 2023.
176. « Action terrestre future », *op. cit.*, p. 10.
177. A. Kranklader, « La mobilité d'une division engagée dans un combat de haute intensité : un facteur-clé du succès tactique », *op. cit.*

Il semble à ce titre utile de redécouvrir le rôle des unités d'appui au mouvement, dont les missions de circulation, d'escorte, d'appui au franchissement, de renseignement et d'appui aux relèves sont absolument essentielles à l'engagement et à la bonne gestion de l'espace de bataille (*battlespace management*) des grandes unités terrestres en haute intensité. La fonction mouvement gagnerait ainsi à être placée au sein de la chaîne opérationnelle en appui à l'engagement dans une approche intégrée de la manœuvre[178].

La perturbation de la connectivité adverse contribue enfin à la survivabilité des dispositifs en ciblant les nœuds critiques qui garantissent l'accès à la transparence de l'adversaire. Il s'agit de rendre inopérant *a minima* l'une des fonctions clés du réseau adverse pour dégrader significativement l'ensemble de la chaîne de connectivité[179]. Dans cette perspective, il semble de plus en plus nécessaire de se doter de capacités de brouillage offensif à longue portée, que ce soit dans les forces terrestres ou aériennes[180]. L'enjeu est de disposer de solutions de brouillage à la fois compatibles avec les émissions amies et le moins détectable possible pour la guerre électronique adverse. Des solutions de brouillage coopératif, permettant de déporter le signal de brouillage pour fausser la détection, pourraient être déployées dans les domaines aérien et terrestre, y compris *via* le recours à des drones brouilleurs[181].

Le déploiement de capacités cyber au niveau tactique, ou la réalisation d'effets cyber tactiques par le niveau stratégique, sera également indispensable pour dégrader les réseaux adverses et maintenir la supériorité tactique dans les champs immatériels. La destruction physique des capteurs par ciblage, cœur de la *SEAD*, gagnerait à être appliquée dans le milieu terrestre en se réappropriant le concept de « contre-reconnaissance », manœuvre dédiée à l'aveuglement du système de renseignement ennemi par le ciblage de ses capteurs[182]. Le déploiement de solutions de LAD dans les forces terrestres et navales participe de cette logique et devient désormais une priorité majeure.

Survivre sur un champ de bataille rendu transparent peut s'appuyer sur un certain nombre de capacités et de technologies, mais repose avant tout sur une préparation opérationnelle exigeante et réaliste, qui intègre la visibilité permanente des dispositifs. S'entraîner en conditions de transparence semble ainsi particulièrement indispensable pour adapter les comportements et les procédures tactiques à cette nouvelle réalité du combat[183].

178. A. Kranklader, « La mobilité d'une division engagée dans un combat de haute intensité : un facteur-clé du succès tactique », *op. cit.*
179. « Neutralisation des défenses aériennes ennemies », CEIA-3.6.4_SEAD, MINARM, 2022.
180. Entretien du 29 novembre 2023.
181. R. Hémez, « Opérations de déception, repenser la ruse au 21e siècle », *op. cit.*, p. 47.
182. M. Yakovleff, *Tactique théorique,* Paris, Economica, 2009, p. 357.
183. J. Watling et A. Reynolds, « Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive », *op. cit.* p. 23.

Remporter la bataille pour la supériorité informationnelle

Alors que les armées françaises se sont engagées vers la maîtrise de l'intégration M2MC, l'exploitation et l'accélération des boucles de connectivité sont un levier essentiel pour acquérir la supériorité informationnelle. À l'instar de la conquête de supériorité dans les autres milieux, elle ne peut être ni totale ni permanente, et il faut la penser comme une potentialité que le décideur choisit d'exprimer dans un cadre espace-temps donné en vue d'atteindre un objectif défini.

Peut-on tenir les promesses du M2MC ?

La doctrine M2MC prévoit la mise en œuvre d'un « réseau multi-senseurs multi-effecteurs » (RM2SE), compris comme « l'architecture globale des senseurs et des effecteurs interconnectés par des systèmes d'information et de communication[184] ». Cette mise en réseau vise l'obtention dans un espace-temps défini d'une « bulle d'hyper-supériorité[185] » à la fois informationnelle et cinétique. La doctrine équivalente américaine *Joint All-Domain C2* (JADC2) vise dans la même logique à « optimiser la disponibilité et l'utilisation de l'information pour que le cycle d'information et de décision du commandeur fonctionne plus rapidement que les capacités de l'adversaire[186] ». Une telle ambition d'intégration multi-domaines suppose cependant des bonds technologiques et organisationnels exceptionnels en termes de connectivité.

Le premier défi suppose de parvenir à construire une architecture réseau interopérable entre différents niveaux tactiques, à travers l'ensemble des composantes de domaines, et ouvert à différents niveaux aux forces alliées. Cette intégration interarmées représente pour les États-Unis la mise en réseau de plus d'une trentaine de SIOC et reste pour le moment hors de portée[187]. L'interopérabilité entre les différents systèmes rend également nécessaire une compatibilité sémantique et normative pour relier des systèmes de génération et de propriétaires différents[188]. Entre adaptation *bottom up*, qui intègre progressivement les systèmes existants avec leurs limites, et conception *top down,* qui définit d'emblée les standards d'architectures au prix d'une remise à plat de tous les systèmes, les options sont ouvertes mais aucune n'est parfaite. Il faut donc probablement renoncer à une connectivité « fédérée » « de bout en bout » en privilégiant des boucles « métier », c'est-à-dire servant une seule fonction (par exemple les fonctions feux ou défense sol-air) dans un premier temps. Enfin, l'interopérabilité du

184. *Stratégie militaire générale*, EMA, septembre 2023, p. 16-17.
185. *Ibid.*
186. *Summary of the JADC2 Strategy*, *op. cit.*, p. 3.
187. Entretien du 8 décembre 2023.
188. E. Faury, « Les opérations multidomaines : une révolution militaire », *op. cit.*

RM2SE devra être compatible avec les exigences de confidentialité, surtout dans une logique de données partagées, ce qui impose de repenser les processus de cloisonnement et d'accès à la donnée[189].

Ensuite, la transmission des données devra respecter les exigences de vitesse et de débit nécessaires à la transparence, tout en garantissant la sécurité des communications dans un champ électromagnétique encombré et contesté par l'adversaire. La maîtrise technique de nouvelles formes d'onde pour augmenter le débit de données ou rester sous les seuils de détection de la guerre électronique est particulièrement complexe, comme l'illustrent les difficultés de développement des programmes de radio-logicielles en France ou aux États-Unis[190]. L'hybridation des réseaux est une solution qui répond à la fois à la sécurité des communications et au partage du débit, mais la multiplication des formes d'onde sur une même source d'émission pose des problèmes de coexistence électromagnétique, les formes d'onde créant des interférences entre elles qui neutralisent leurs effets[191]. Le déploiement d'une complémentarité radio/communication par satellite (SATCOM), à l'instar de StarLink pour l'armée ukrainienne, semble répondre le mieux aux besoins de résilience du réseau tout en garantissant un haut débit de données. Une telle solution suppose cependant de disposer d'un réseau satellitaire souverain et sécurisé assuré par le déploiement d'une constellation dédiée en orbite basse.

Enfin, la gestion de la donnée elle-même représente un défi de taille, le volume et le flux constant qui caractérise le *big data* rendant nécessaire l'autonomisation de son traitement par l'intégration de systèmes d'IA dans la boucle de connectivité. Pour exploiter pleinement le levier de l'intégration M2MC, il faut trouver les moyens techniques et organisationnels de dépasser la complexité de l'hyperconnectivité. À court terme, il faudrait privilégier une application restreinte du maillage RM2SE sous forme de « bulles de transparence » appliquées dans l'espace et le temps pour un cas d'usage défini en fonction de l'effet recherché, ce qui répond bien à l'ambition d'« hyper-supériorité » acquise localement. Dans ce cadre, l'intégration des flux des capteurs dronisés dans les SIOC de gestion des feux tels qu'ATLAS[192] pourraient constituer un premier pas vers le M2MC.

Le renseignement militaire est-il obsolète ?

L'immédiateté de l'information et la recherche de l'exploitation instantanée, l'accès partagé à la donnée et la contribution croissante de l'OSINT à la

189. *Ibid*.
190. Voir à ce sujet A. Hasday, « Intelligence artificielle dans l'armée : Sébastien Lecornu désavoue Thales et Sopra Steria », *L'Informé,* 22 janvier 2024, disponible sur : www.linforme.com ; M. Sneps-Sneppe, D. Namiot et E. Tikhonov, « On Software Defined Radio Issues », 2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW), Riga (Lettonie), 2022, p. 35-40.
191. Entretien du 8 décembre 2023.
192. Le système ATLAS (Automatisation des tirs et liaisons de l'artillerie sol/sol) est le logiciel de gestion des feux sol-sol qui équipe les régiments d'artillerie de l'armée de Terre.

compréhension de la situation tactique sont autant de dynamiques de la transparence qui vont à l'encontre du fonctionnement traditionnel de la fonction renseignement. Il s'agit donc de distinguer les adaptations nécessaires du renseignement à la réalité du champ de bataille contemporain, tout en redonnant toute sa place à ce qui fait sa force : le recul de l'analyse.

Le besoin d'accès permanent et partagé à l'information selon des logiques civiles de *data as a service*[193] rend nécessaire un changement de culture du renseignement vers un décloisonnement de l'information et l'exploitation du levier de la donnée partagée. Atteindre cet effet suppose repenser la production du renseignement d'abord dans une perspective de diffusion ouverte et d'inverser la logique de restriction en faisant de la confidentialité une exception plutôt que la norme par défaut. Cette évolution va d'ailleurs dans le sens de l'ouverture des réseaux à l'interarmées, voire l'interalliés et aux forces partenaires que sous-entend la doctrine M2MC.

L'intégration des analyses OSINT civiles pourrait constituer une opportunité pour le renseignement militaire. Autant la prise en compte des données en sources ouvertes a été intégrée dans les métiers du renseignement, autant les communautés d'« osinter » civils en ligne (tels que *Oryx.com* ou *Warspotting.com)* représentent une puissance collective d'analyse dont l'exploitation est encore largement sous-estimée. Le frein principal est d'ordre sécuritaire, lié aux enjeux de protection du secret qui exclut d'emblée tout partage d'information avec des cercles non habilités, incluant l'expression du besoin en renseignement lui-même qui en dit déjà long sur l'intention ou des vulnérabilités. L'enjeu est de parvenir à articuler l'offre civile extrêmement riche et précise au besoin militaire, tout en reconnaissant qu'il sera très difficile d'orienter ces communautés civiles dans la logique traditionnelle de la boucle du renseignement, d'une part à cause du profil et des motivations des membres de ces communautés, d'autre part pour des raisons de préservation du secret. La solution pourrait être de développer une plateforme d'interface dédiée qui agirait comme un sas entre les deux mondes et qui permettrait d'exploiter l'intelligence collective de ces communautés selon les principes du *crowdfunding*[194].

La transparence est de plus en plus comprise comme le levier de l'attrition de l'adversaire par les feux, interprétation très marquée par l'influence de la doctrine américaine sur les procédures de l'Organisation du traité de l'Atlantique nord (OTAN). Ce biais crée des effets de bord sur le renseignement militaire qu'il est nécessaire de rééquilibrer en rappelant le rôle essentiel de l'analyse. Les processus de ciblage dans la profondeur ont ainsi pris une place prépondérante dans la manœuvre terrestre, avec pour

193. Modèle de service de données garantissant au client une mise à disposition optimisée de ses données en tout temps tout lieu grâce à internet et aux techniques de *cloud*.
194. « Enjeux, à travers l'exemple ukrainien, du renseignement d'origine sources ouvertes (OSINT) », *op. cit.*

objectif de « modeler » l'adversaire en définissant des *kill contracts* selon lesquels on planifie les manœuvres des capteurs et des effecteurs. Cette priorité de l'avant altère la dimension multidirectionnelle du renseignement en plaçant la priorité sur les capteurs dans la profondeur. Les autres dimensions (la ligne de contact, les côtés, les arrières, le renseignement amont) se retrouvent dès lors moins servies dans une logique de moyens comptés, ce qui représente un premier risque.

Un autre risque est celui d'un certain écrasement de la conduite de la manœuvre par la prépondérance de la conduite des feux, observable par exemple dans les PC de division avec la place qu'a pris la cellule *Joint Air Ground Integration Center* (JAGIC) dans les processus du PC[195]. Privilégier l'accélération de la boucle par l'exploitation immédiate de l'information fait courir le risque d'une perte de capitalisation pourtant nécessaire pour le temps long. La solution technique pour atteindre un équilibre sain entre la production de renseignement « à fin d'action » en accélération constante, et de renseignement « de situation[196] » réside dans l'architecture des systèmes d'information, qui doivent intégrer les deux processus en parallèle et permettre à un PC de traiter les mêmes données dans des processus parallèles aux rythmes différents.

Enfin, les efforts des deux dernières lois de programmation militaires (LPM) vis-à-vis du renseignement masquent l'effacement du volet analyse devant la montée en puissance de la gestion technique de la donnée numérique. Il semble donc nécessaire de veiller à ce que les investissements dans le développement numérique du renseignement ne se fassent pas au détriment des besoins en ressource humaine compétente et en volume suffisant pour faire face aux exigences de l'hyperconnectivité[197].

Risque-t-on de manquer le virage des drones ?

Le rôle croissant des drones dans les conflits en cours met en lumière les enjeux de la prise en compte de la fonction drone dans les armées françaises et de son modèle de développement capacitaire. Alors que les armées françaises adaptent leur réflexion sur les drones à la lumière des enseignements opérationnels récents, deux impératifs méritent d'être pris en compte : le caractère intégral de la composante drone et l'intégration du drone dans les réseaux de commandement et de contrôle existants.

195. Entretien du 4 décembre 2023.
196. Le renseignement « à fin d'action » vise à détecter, localiser et identifier les cibles, alors que le renseignement « de situation » vise « décrit la situation actuelle au niveau stratégique, opératif ou tactique » pour l'appui à la planification et la conduite des opérations. Référence : *Neutralisation des défenses aériennes ennemies*, CEIA-3.6.4_SEAD, MINARM, 2022, p. 42.
197. Entretien du 6 février 2024.

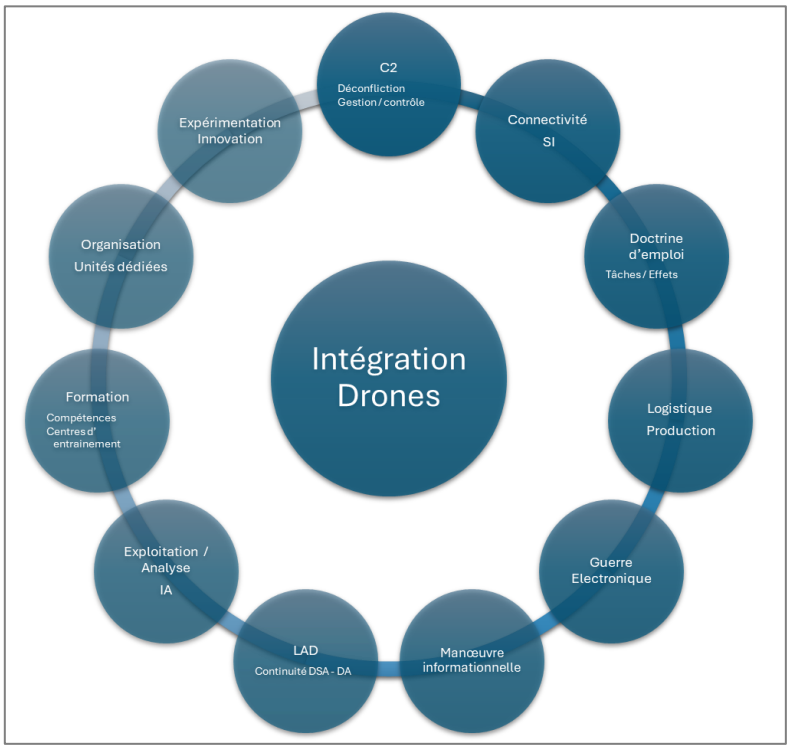
En premier lieu, l'introduction du drone dans les architectures de combat doit être comprise comme une « révolution holistique[198] » qui dépasse le simple appui à la manœuvre, et qui a des effets sur les organisations et les systèmes de commandement ainsi que sur les systèmes d'armes existants. Ainsi, la composante drone ne peut être développée sans penser en parallèle des solutions de LAD et une doctrine duale qui pense l'emploi en même temps que la menace et sa parade. La LAD elle-même doit être imaginée, en capacités comme en emploi, dans un *continuum* avec les couches de défense sol-air (DSA) et de défense aérienne (DA). La rapidité de l'établissement des contre-mesures électroniques impose également de repenser les cycles de développement capacitaires pour les rendre compatibles avec la dynamique d'innovation technologique des drones et de leurs parades[199]. Cette vision globale du drone comme systèmes plaide pour une intégration massive des drones à tous les niveaux selon une logique cumulative d'étagement et de redondance qui permette de couvrir l'ensemble du spectre d'emploi du drone au-delà de sa fonction de reconnaissance.

L'intégration du drone dans les réseaux de C2 est ensuite une condition essentielle de son efficacité. Le drone ne peut donner la pleine mesure de son emploi s'il est employé en boucle fermée par défaut et doit pouvoir échanger en permanence les données qu'il collecte avec les autres acteurs du réseau. Son emploi doit également être articulé avec d'autres capacités, telle que la guerre électronique qui garantit sa mise en œuvre en assurant une nécessaire prise de supériorité en amont de son déploiement, ou comme la fonction feux qui exploite ses données en temps réel. Enfin au-delà de sa contribution à la supériorité informationnelle, le drone contribue à provoquer un triple effet psychologique de sidération, de saturation et de foudroyance[200] qui rend nécessaire de lier son emploi à la manœuvre, dans ses volets cinétiques comme informationnels.

Ces deux impératifs rendent urgent l'appropriation des savoir-faire et procédures liés à l'emploi des drones et incitent à doter dès à présent les unités tactiques de drones d'entraînement, y compris de gamme civile, pour s'entraîner à leur mise en œuvre sans attendre l'aboutissement des programmes d'équipement en cours[201].

198. H. Seydoux, « Microdrones : des innovations inattendues à la lumière du retour d'expérience ukrainien », *Revue Défense Nationale*, n° 865, décembre 2023, p. 35-42.
199. Entretien avec un industriel de défense, 14 avril 2023.
200. L. Lebailleur, « Réflexions prospectives sur l'emploi collaboratif de drones aériens et de l'aviation habitée dans les opérations aériennes militaires » (Mémoire BTEM), 2023.
201. T. Hacker, « How the US Army Can Close Its Dangerous – and Growing – Small Drone Gap », Modern War Institute, 6 mars 2024, disponible sur : https://mwi.westpoint.edu.

Schéma III-2 : Intégration de la composante drones, approche holistique



© Pierre Néron Bancel/Ifri, 2024.

Repenser la surprise : inventer de nouvelles formes de manœuvre

La surprise demeure donc possible malgré la transparence du champ de bataille. Il reste à imaginer comment rétablir concrètement les conditions de sa mise en œuvre dans une manœuvre remise en cause par le triptyque détection/acquisition/destruction. Sous certaines conditions, exigeantes, elle paraît toujours possible, dans un cadre interarmées ou dans chacun des milieux considérés séparément. Le renouveau de la surprise passe par une réappropriation du principe d'incertitude défini par l'amiral Guy Labouérie, qui consiste en « un masquage permanent, y compris pendant l'action, de façon que l'autre reste dans l'incertitude sur le but, le moment, le lieu, la forme, afin qu'il ne puisse pas s'y préparer[202] ». De nouvelles formes opérationnelles de ruse ou d'agilité sont ici proposées, regroupées en trois familles, ces propositions n'épuisant pas le sujet.

202. G. Labouérie, « Des principes de la guerre », *Revue Défense Nationale*, n° 530, 1992.

Créer des fenêtres d'opacité

Le point d'orgue revient ici à se soustraire, au moins temporairement, à l'observation de l'adversaire et à troubler significativement sa compréhension et partant sa riposte. Cela est d'autant plus vrai pour une manœuvre offensive, où le facteur surprise conditionne souvent la réussite de l'opération. Dans ce cadre, on s'efforcera, à un moment soigneusement déterminé, de créer les conditions de son « étourdissement », en exploitant tous les éléments permettant d'obscurcir le champ de bataille. Pour atteindre cet effet global, plusieurs paramètres doivent être combinés, parmi lesquels :

- recherche d'une fenêtre météo favorable (conditions dégradées affectant la précision des capteurs adverses), avec optionnellement une nuit très obscure (niveau 5) ;
- aveuglement initial tactico-opératif des capteurs pour, sinon interdire totalement la détection, tout au moins la réduire ou la retarder ;
- ébranlement initial du système C4ISR adverse, avec efforts sur les PC, pour compliquer l'appréciation globale de la manœuvre offensive en cours ;
- appui non cinétique de ces opérations d'aveuglement/ébranlement par des actions cyber, de guerre électronique, voire une combinaison des deux, cherchant ainsi à élargir le champ de l'opacité, en exploitant tous les effets déceptifs de la guerre électronique[203] ;
- lancement de l'action décisive par une manœuvre offensive débouchant idéalement d'un milieu opaque (dissimulation de l'attaque initiale) ; la furtivité des vecteurs offensifs ou la modification de leurs différentes signatures compléteront cette création de nébulosité.

La coordination de l'ensemble de ces actions serait dans les faits complexes, mais même imparfait, un tel enchaînement pourrait prendre en défaut un système défensif se sentant à l'abri d'une transparence dans laquelle il aurait placé toute sa confiance.

Cette fenêtre d'opacité pourrait mettre à profit l'idée de la « surprise doctrinale », tenant au fait que l'on agit de manière disruptive, non conforme à sa propre doctrine ; cette dernière étant généralement étudiée par le renseignement adverse, on le surprend en agissant différemment[204]. Ainsi, un combat engagé en mode dégradé, par exemple tous émetteurs éteints, ajouterait à la difficulté de la détection en réduisant considérablement la signature électromagnétique. Ce type de procédé oblige à maîtriser des savoir-faire anciens, considérés comme dépassés (radios et GPS coupés, donc

203. Brouillage bien sûr, mais également création de faux réseaux ou intrusions. En clair, tout procédé permettant de créer des effets perturbateurs de « confusion électronique ».
204. M. F. Cancian, « Inflicting Surprise: Gaining Competitive Advantage in Great Power Conflicts », *CSIS*, janvier 2021, p. 43 et 57-58.

déplacements en « croquis d'itinéraires », couloirs d'infiltration avec point à atteindre, sans points de coordination intermédiaires, etc.), un défi à relever alors qu'il importe en parallèle de maîtriser les compétences liées aux dernières technologies. En outre, le mode dégradé peut être subi (panne systémique, déni de service…) et non choisi, aussi apparait-il indispensable de s'y entraîner. La Marine nationale s'est d'ores et déjà exercée en ce sens[205], en réalisant une mission fictive sans liaison-satellite, montrant que ce type de défi peut être relevé.

Dernière réflexion, alors que la zone urbaine est un très bon milieu opaque en défensive, pourquoi ne pas l'exploiter en offensive. On pourrait imaginer ne pas tenir le terrain de manière linéaire (dispositif continu), mais occuper uniquement les villes d'une taille suffisante, dont certaines se révéleraient des points de déclenchement d'une attaque. Tout dépendrait ici de la nature du maillage urbain sur la zone d'opérations. Il y aurait certes des espaces lacunaires, mais le schéma tactique pourrait alors ressembler à une suite de carrés échelonnés de l'époque napoléonienne, lesquels laissaient passer les charges de cavalerie et qui, une fois ces dernières suffisamment affaiblies par des tirs croisés, pouvaient adopter une formation offensive[206]. L'incertitude serait créée par la difficulté à apprécier la posture des différents moles urbains : offensive ou défensive ?

Créer de nouvelles formes de masse

La masse est une qualité qui a quitté l'horizon des forces européennes depuis deux à trois décennies. La dronisation/robotisation partielle du champ de bataille, bien au-delà de la seule fonction ISR (Intelligence, Surveillance, Reconnaissance), permet de réenvisager de nouvelles formes de déception dans sa forme active (simulation). À cette fin, la masse, permettant, à l'échelle tactique, d'établir un rapport de force favorable sur la zone décisive, pourrait s'envisager différemment. Les essaims de drones (ici en fonction d'appui, c'est-à-dire comme leurres ou pour brouiller le spectre électromagnétique), pourraient simuler une manœuvre de feinte ou de diversion. Il serait difficile pour l'adversaire de saisir la cohérence de la manœuvre exercée contre lui, l'obligeant à se dévoiler ou à disperser ses moyens. L'effet de saturation produit créerait *a minima* un stress. Cela permettrait surtout de ne pas exposer exagérément les unités « réelles ». Celles-ci, trop concentrées dans le cadre d'une manœuvre classique, présenteraient pour le coup autant de cibles faciles à détruire du fait de la transparence.

205. Voir R. Ruitenberg, « Back to the "80s" as French Navy Prepares for New Threats », *Defensenews*, janvier 2024.
206. Voir les tableaux de la bataille des Pyramides (Lejeune) ou de Waterloo (Philippoteaux).

On peut décliner cette idée dans les domaines aériens et aéronavals avec les « ailiers dronisés » (« *loyal wingman* ») des plateformes aériennes pilotées dont il a été question. Ces formations pourraient de surcroît être appuyées par des essaims de drones (à l'image des *Gremlins* ou du projet Assydus[207]) pour générer un effet de masse et crédibiliser une diversion. On le voit, d'innombrables combinaisons tactiques sont envisageables dans les différents milieux, au gré des maturations technologiques qui ne manqueront pas de se produire et dont le conflit russo-ukrainien, par sa nature, ne peut se faire l'écho.

La mise en œuvre de tels modes opératoires exigerait une réflexion capacitaire quant au mix idéal entre drones élaborés, rares et chers, et drones consommables, nombreux, mais beaucoup plus faciles à détruire ou perturber. Enfin, la faculté de créer ce type de masse tactique et l'impératif d'en assurer l'épaisseur organique ou de l'utiliser plus d'une fois nécessitent une autre forme de masse, celle au sens stratégique, c'est-à-dire la capacité à produire, maintenir, remplacer un grand nombre de matériels pour tenir dans la durée. Plus cette masse stratégique serait importante (liée au potentiel de la BITD [base industrielle et technologique de défense] et aux stocks pré-conflits réalisés) et plus la combinaison *high-low-mix*[208] qui vient d'être évoquée serait étoffée, plus les possibilités de déception et partant d'actions décisives seraient nombreuses, enclenchant un cercle vertueux.

Retravailler le principe de « l'attaque brusquée »

Si l'adversaire « me voit assurément et a toute chance de comprendre mes préparatifs », en clair, si la surprise est trop dure à obtenir (nature géographique du théâtre d'opérations favorable à la transparence, adversaires à parité technologique, etc.), il ne reste *a priori* plus qu'une option pour prendre l'ascendant : la vitesse d'exécution. Une telle action offensive est dénommée « attaque brusquée » ou « attaque dans la foulée », avec une très courte préparation initiale. Ce procédé requiert des unités bien entraînées, très manœuvrières, ce qui ne s'obtient que par une préparation opérationnelle exigeante. Pour un affrontement terrestre, il s'agit de s'entraîner à opérer des mouvements de concentration rapides à partir d'unités isolées à dessein, et, sans avoir perdu en cohésion, prendre l'ascendant sur une zone décisive.

En d'autres termes, si les conditions de la transparence ne peuvent être contournées, seule l'habileté tactique des unités engagées peut permettre de

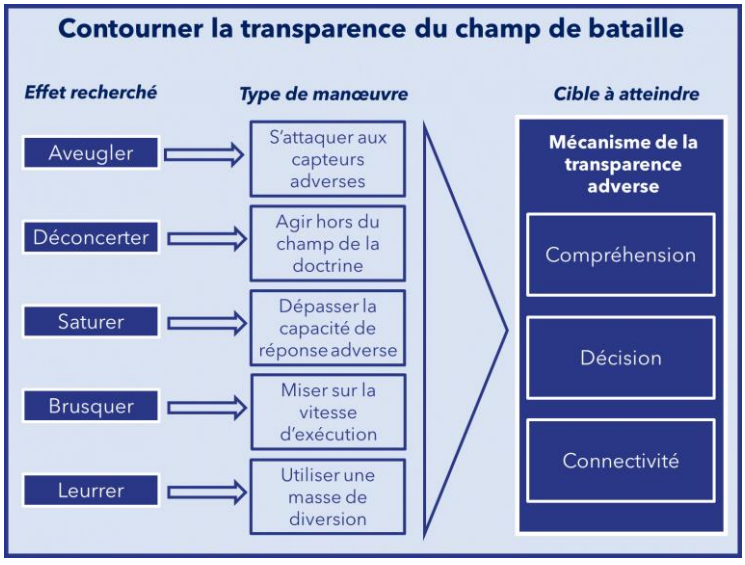
207. Essaim de drones-leurres ; voir : « ASSYDUS – Obtenir une surface équivalente radar (SER) en utilisant un essaim autonome de drones aériens », site du Ministère des Armées (defense.gouv.fr).
208. Voir P. Gros, « Mission d'information sur la préparation à la haute intensité », Assemblée nationale, 17 février 2022, disponible sur : www.assemblee-nationale.fr.

se soustraire à la riposte de l'adversaire, habileté qui doit nécessairement être supérieure à celle de l'adversaire. Le style de commandement (initiative, habitude à opérer avec un C2 déconcentré) y joue un rôle important. La disposition de « kits de dissimulation », s'inspirant des équipements vus précédemment (camouflages intelligents, leurrage des signatures, etc.) aiderait les unités en charge de l'attaque brusquée à retarder leur détection.

Le système de force terrestre français dispose probablement d'un avantage comparatif pour mettre en œuvre ce procédé opérationnel. Il lui est parfois reproché son manque de robustesse, avec un segment « blindé-lourd » incomplet. Parce que système médian, il détient aussi davantage de mobilité, plus à même donc d'exercer des attaques brusquées à l'échelle tactico-opérative, à condition de s'y entraîner. Ce mode opératoire exigerait néanmoins de traiter les carences capacitaires concernant certains appuis, notamment le génie-bréchage et la guerre électronique offensive. Aussi, le maintien d'une composante de combat aéromobile, la plus conséquente en Europe, offre une autre forme d'attaque brusquée, sous réserve de circonvenir la vulnérabilité de ces vecteurs, par exemple avec un nouveau mix hélicoptères-drones d'accompagnement, et de dégrader sérieusement au préalable le dispositif adverse de défense antiaérienne basse-couche[209].

Pour finir, ces trois familles de procédés opérationnels possèdent leur logique propre mais ne sont pas exclusives les unes des autres, offrant donc des possibilités de combinaisons.

Schéma III-3 : Contourner la transparence : quels modes opératoires ?



209. Missions SEAD.

Implications stratégiques sur l'ensemble du spectre de conflictualité

Au-delà de la transparence du champ de bataille, tactique ou opératif, doit être scrutée la transparence à l'échelle stratégique, traduisant la dialectique des volontés au niveau national, déclinée selon les trois registres identifiés dans la vision stratégique du chef d'état-major des armées : compétition, contestation, affrontement.

Affrontement conventionnel : la tentation de la frappe préemptive ?

Associée à la létalité des effecteurs, la transparence du champ de bataille a tout lieu de produire des effets redoutables. Elle offre en effet des cibles plus faciles à traiter aux missiles, en particulier hypervéloces[210], difficiles à intercepter par leurs capacités manœuvrantes (imprédictibilité de la trajectoire) et leur vitesse de vol. Une telle prime à l'engagement offensif pourrait être considérée comme insupportable par un acteur en situation de crise aiguë avec un compétiteur à parité de puissance militaire : le caractère précipité de cette menace potentielle l'amènerait à se sentir trop vulnérable. Dès lors pourrait exister la tentation de « tirer le premier » par une campagne foudroyante de frappes[211]. Elle viserait à aveugler immédiatement l'adversaire, à neutraliser ou désorganiser ses principales liaisons de données, ses nœuds de communication et ses centres de décision. Si l'enjeu est jugé essentiel, les frappes (cinétiques voire impulsions électromagnétiques de grande amplitude) incluraient les satellites du cœur souverain atteignables ou tout satellite civil pouvant avoir des fonctions duales significatives. Cette campagne serait complétée par une offensive cyber, nécessairement planifiée de longue date si elle entend produire des effets pertinents et coordonnés avec les autres lignes d'opération[212] (frappes conventionnelles, agressions spatiales, lutte informationnelle). Le but serait de l'emporter « sans coup férir », en provoquant un double effet de sidération mentale et de paralysie fonctionnelle, les deux effets conjugués interdisant une riposte coordonnée, rapide et efficace.

---

210. Et d'une manière générale tous les types de vecteurs capables d'effectuer des frappes précises (missiles hypersoniques, de croisières, sol-sol BTH (Below-The-Horizon), etc.

211. Global Trends, « The Future of the Battlefield », National Intelligence Council, avril 2021.

212. Voir audition à huis clos du général A. Bonnemaison, commandant de la cyberdéfense. Consulter le compte rendu n° 27 du 7 décembre 2022 sur le site de l'Assemblée nationale.

On perçoit le caractère escalatoire de cette perspective si chaque partie craint la mise en œuvre de cette campagne par l'autre, alimentant la tentation des deux côtés au cas où des intérêts essentiels seraient en jeu. Le tandem transparence/létalité (précision et portée toujours plus élevées des missiles) porte ce risque stratégique, aggravé en cas de défaut mutuel d'appréciation. Pour baisser le degré d'occurrence de ce scénario d'escalade, des mesures de résilience doivent être prévues afin de compliquer le calcul d'une campagne préemptive de frappes : dissimulation, dispersion des moyens stratégiques, durcissement des infrastructures, stocks d'armements enfouis, redondance des systèmes de commandement, réactivité et subsidiarité des forces, et même « esprit de défense » de la nation (force morale collective). Tout ceci produirait un effet de dissuasion, ou à tout le moins présenterait des dilemmes pour celui décidant de tirer le premier. On retrouve aussi dans ce cas de figure la notion de masse stratégique évoquée précédemment, permettant de se rétablir d'un tel coup et même de prendre l'ascendant si celui qui l'a porté n'avait misé que sur ce mode d'action, manquant alors d'épaisseur organique pour s'inscrire dans un conflit prolongé.

Contestation : les leviers déstabilisants de l'ambiguïté et de la manipulation

La confrontation armée peut être jugée trop coûteuse ou trop hasardeuse. Le conflit en Ukraine le redémontre si besoin était. Il pourrait même réinciter à davantage de prudence pour les puissances tentées par l'exercice de la coercition. Aussi, les modes d'agression dits hybrides, sous le seuil du conflit armé, conservent un bon rapport coût-efficacité pour les États souhaitant remettre en question le *statu quo* international.

Ici, l'opacité l'emporte sur la transparence puisqu'il s'agit essentiellement d'agir dans le champ des perceptions. Des actions de déstabilisation peuvent être également portées dans le champ matériel, en utilisant les milieux opaques, au premier rang desquels le cyberespace, mais aussi les fonds marins ou l'espace exo-atmosphérique. Une campagne bien coordonnée pourrait ainsi viser à détériorer des moyens organiques stratégiques, comme certains câbles sous-marins, des réseaux d'infrastructures critiques, des satellites. Ainsi, des armes à énergie dirigée discrètes ou des satellites « butineurs[213] » (satellites effectuant des manœuvres rapprochées avec une intention potentiellement hostile vis-à-vis d'un autre satellite) seraient employées pour éblouir, dégrader, neutraliser temporairement ou définitivement tel ou tel moyen stratégique. Des opérations clandestines compléteraient éventuellement ces actions perturbatrices. L'attribution de l'attaque serait compliquée par la nature

213. Les actions du satellite russe Luch-Olymp K2 aux abords de satellites Eutelsat ont notamment été médiatisées. Voir M. Cabirol, « Comment trois satellites d'Eutelsat ont été espionnés par le satellite russe Luch Olymp 2 », *La Tribune*, novembre 2023.

opaque du milieu utilisé, ceci expliquant le bon rapport politique coût-efficacité du point de vue de l'agresseur.

Pour contrer ces modes d'action, il faudrait pouvoir rétablir la transparence, le renseignement permettant d'anticiper et d'attribuer la menace. Celle-ci ne pouvant être qu'imparfaite dans les milieux opaques, la résilience, dont certaines modalités seraient similaires à celles évoquées *supra* (p. 71), jouerait un rôle essentiel. Une panoplie de capacités centrées autour d'armes à énergie dirigée permettrait en outre de riposter avec une plus grande souplesse politique en présentant au décideur un nombre accru d'options, en graduant la réplique selon la nature des dommages subis. La possession d'une telle panoplie jouerait en outre un rôle dissuasif, rappelant au perturbateur qu'il peut être frappé au bon niveau d'intensité sans provoquer d'escalade.

Compétition : des acteurs infra-étatiques cherchant à déjouer la transparence

Les adversaires infra-étatiques sont également concernés par la dialectique transparence-opacité. Il s'agit pour eux de contourner les avantages comparatifs des armées étatiques en termes de transparence, tout en concevant leur propre transparence.

Sur le premier point, ces acteurs vont exploiter les milieux opaques, notamment le milieu urbain. Les souterrains permettent la dissimulation physique. Surtout, la masse démographique crée pour eux un effet de dilution[214]. Ce dernier point peut également être appliqué au domaine maritime, avec un trafic naval exponentiel permettant de se soustraire à une surveillance[215]. Ainsi que l'ont rappelé les opérations contre Daech, ces organisations sont à même d'inventer des procédés rustiques rendant inopérantes les plus récentes technologies, par des procédés rigoureux de SECOPS (dont le cloisonnement des structures), l'utilisation de pigeons voyageurs, de réseaux de téléphonie filaire ou d'estafettes. Pour dérisoires qu'elles puissent paraître au premier abord, ces mesures ont prouvé leur efficacité[216], même si elles se paient au prix d'une réduction très importante de liberté d'action.

Sur le second point, ces mouvements profitent de la démocratisation de la transparence évoquée plus haut. Capables d'innovations[217], les techno-guérillas[218] ont depuis longtemps démontré leur aptitude à utiliser ou fabriquer des drones de surveillance, recueillir de l'information et des images

214. B. R. Posen, « Command of the Commons: The Military Foundation of U.S. Hegemony », *International Security*, n° 28, été 2003, p. 27-36.
215. J. Bachelier et P. Boulanger, « La "fusion de l'information" : levier de la puissance maritime française ? », *op. cit.*
216. La réussite de l'attaque du Hamas le 7 octobre 2023, déjà évoquée, venant le confirmer.
217. Global Trends, « The Future of the Battlefield », *op. cit.*
218. J. Henrotin, *Techno-guérilla et guerre hybride*, *op. cit.*

via des satellites civils, utiliser le cyberespace à leur profit[219]. Combattant dans un environnement familier, ils bénéficient d'un renseignement humain efficace.

La dialectique transparence-opacité est donc loin d'être jouée dans ce spectre de conflit et il serait bien imprudent pour les armées étatiques de considérer comme garantie la supériorité informationnelle, l'avantage technologique pouvant être déjoué par une connaissance plus fine du milieu humain et son exploitation à des fins subversives.

219. Recrutement, transactions financières, désinformation, etc.

Conclusion

S'assurer d'une plus grande transparence que son adversaire sur le champ de bataille offre indubitablement un avantage militaire conséquent. Autant les NTIC que la démocratisation de cette transparence ouvrent dans cette perspective des possibilités inédites. Pour autant, comme tout phénomène militaire, elle s'inscrit dans des dialectiques croisées (technologiques, tactiques et stratégiques) amenant à considérer avec davantage de prudence les avantages qu'elle procure.

Il s'agit d'abord, en voulant acquérir à tout prix la supériorité en matière de transparence, de ne pas devenir un simple spectateur du champ de bataille. Tout choix capacitaire s'inscrit dans un équilibre systémique complexe : un effort trop prononcé sur un segment donné s'obtient au détriment des autres. Voir et comprendre est une chose, pouvoir agir en conséquence en est une autre. Des réflexions autour d'un modèle *high-low mix*, entrevues précédemment, pourraient offrir des solutions équilibrées, tant sur le plan opérationnel (mise au point de nouveaux modes opératoires à partir de combinaisons originales) que sur le plan stratégique (préserver une aptitude générale à la résilience).

Aussi, il importe de ne pas être prisonnier de la transparence en lui accordant une trop grande confiance. Tout avantage est voué, à plus ou moins long terme, à être contourné, par le bas (à l'exemple des organisations terroristes) ou par le haut (campagnes stratégiques opaques de déstabilisation, nouveau spectre technologique créant de nouveaux subterfuges, etc.). Savoir en jouer tout en sachant faire sans ou avec moins (modes dégradés) paraît à cet égard judicieux. Cela permettrait à tout le moins de conserver une agilité doctrinale, condition pour s'adapter à de nouvelles situations, ou mieux à les provoquer. La transparence ne doit pas devenir un dogme, comme le fût celui de la supériorité du feu dans l'entre-deux-guerres, poussant l'institution militaire française dans une forme de confort intellectuel annonçant le désastre de 1940. Un tel état d'esprit accroît sensiblement le risque de subir une surprise sidérante, un paradoxe saisissant pour celui qui fait de la transparence le parangon ultime de l'art opérationnel.

Au-delà des questions d'ordre technologique (celles qui permettent d'étudier en profondeur les apports et limites de la transparence) ou doctrinal (mise au point des *modus operandi* pour l'exploiter au mieux), il reste à considérer une ressource qui n'appartient à aucun de ces deux domaines : la préparation opérationnelle. Le blocage tactique apparent induit par la transparence n'est pas pour autant une fatalité. Même si le général Zaluzhny, alors chef des armées ukrainiennes, déplorait à juste titre

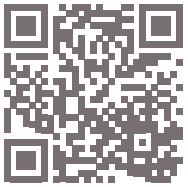
cette impasse tactique, celle-ci s'inscrit dans un contexte opérationnel précis dont tous les éléments ne sont pas reproductibles, chaque conflit ayant sa logique propre, même si un tronc commun peut se dégager à une époque donnée. Aussi, les deux protagonistes ne disposent pas nécessairement de toute la panoplie des capacités modernes de combat interarmées. Il ne rend donc pas forcément compte de toutes les possibilités de manœuvre pouvant être mises au point[220]. Ici intervient l'ardente nécessité d'une préparation opérationnelle au meilleur niveau pour les armées françaises, et ce, à trois titres. D'abord conserver l'avantage de la transparence à son propre profit, ensuite savoir la contourner dans un combat à parité, ce qui requiert une grande habileté tactique comme vue précédemment, enfin et probablement surtout préserver une faculté d'adaptation si tous les paramètres décrits dans cette étude venaient à évoluer très rapidement. En effet, les évolutions technologiques s'opèrent à une vitesse telle qu'il est quasiment impossible de suivre le rythme sur le plan doctrinal.

Aussi, s'attendre à être surpris pourrait bien être le meilleur moyen de résister à la surprise et l'habitude de s'entraîner régulièrement de manière exigeante, en d'autres termes la compétence, constitue l'un des leviers de l'adaptation réactive, procurant, à l'échelle de la nation, un facteur de résilience.

220. On assistera d'ailleurs peut-être à une rupture opérationnelle (doctrinale, organisationnelle ou tactique) avant le terme de ce conflit. Il demeure très difficile de prédéterminer l'adaptation réactive d'une nation (unités sur le terrain, techniciens/ingénieurs civils…), si les moyens sont présents.

Les dernières publications des *Focus stratégiques*

- Jérémy Bachelier et Céline Pajon, « La France dans l'Indo-Pacifique. Pour une posture stratégique pragmatique », *Focus stratégique*, n° 117, Ifri, octobre 2023.
- Élie Tenenbaum et Léo Péria-Peigné, « *Zeitenwende* : La Bundeswehr face au changement d'ère », *Focus stratégique*, n° 116, Ifri, septembre 2023.
- Guillaume Garnier, « La France dans l'OTAN : de l'allié difficile au contributeur essentiel », *Focus stratégique*, n° 115, Ifri, juin 2023.
- Jérémy Bachelier, Héloïse Fayet, Alexandre Jonnekin et François Renaud, « Le signalement stratégique : un levier pour la France dans la compétition entre puissances ? », *Focus stratégique*, n° 114, Ifri, mai 2023.
- Léo Péria-Peigné, « Stocks militaires : une assurance-vie en haute intensité ? », *Focus stratégique*, n° 113, Ifri, décembre 2022.
- Héloïse Fayet, « Quelle posture stratégique pour la France au Moyen-Orient ? », *Focus stratégique*, n° 112, Ifri, novembre 2022.
- Laurent Bansept, « Le retour de la haute intensité en Ukraine : quels enseignements pour les forces terrestres ? », *Focus stratégique*, n° 111, Ifri, juillet 2022.
- Laure de Roucy-Rochegonde, « *Deus ex machina* : les enjeux de l'autonomisation des systèmes d'armes », *Focus stratégique*, n° 110, Ifri, mai 2022.
- Laurent Bansept et Élie Tenenbaum, « Après Barkhane : repenser la posture stratégique française en Afrique de l'Ouest », *Focus stratégique*, n° 109, Ifri, mai 2022.
- Amélie Férey, « Vers une guerre des normes ? Du *lawfare* aux opérations juridiques », *Focus stratégique*, n° 108, Ifri, avril 2022.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org