IFRI
STUDIES

DEFENSE RESEARCH UNIT

FOCUS STRATÉGIQUE No. 118

MAY
2024

“At the Other Side of the Hill”
The Benefits and False Promises of Battlefield Transparency

Guillaume GARNIER
Pierre NÉRON-BANCEL

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit foundation according to the decree of November 16, 2022. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

The opinions expressed in this text are the responsibility of the authors alone.

ISBN: 979-10-373-0916-7

© All rights reserved, Ifri, 2024

Cover: Stridsvagn 122 tank equipped with the Mobile Camouflage System (MCS) 'Barracuda' from SAAB AB © SAAB AB

How to quote this publication:

Guillaume Garnier and Pierre Néron-Bancel, "'At the Other Side of the Hill': The Benefits and False Promises of Battlefield Transparency", *Focus stratégique,* No. 118, Ifri, May 2024.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

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

Email: accueil@ifri.org

Website: Ifri.org

Authors

Pierre Néron-Bancel is a French Army officer working as a military fellow within the Defense Research Unit of IFRI's Center for Security Studies, where his works focus mainly on French security and strategic challenges, more specifically on the future of land warfare, as well as the strategic role of the Army. He is graduated from Saint-Cyr, the French Army officer school, and from the Ecole de Guerre, as well as from the UK Advanced Command and Staff Course and holds two master's degrees in International Relations and Strategy and in Defense Studies. A Foreign Legion officer, he served with the 13th Half brigade of the Foreign Legion in Djibouti, then in the 1st Foreign Cavalry Regiment near Marseille. He has been deployed in many operations overseas in Africa and in Middle-East as well as on the French soil.

Guillaume Garnier is an Associate Research Fellow at Ifri's Security Studies Center. He was a Military Fellow whithin the Defense Research Unit at this Center from 2012 to 2014. He retired from the French Army as a Colonel in 2022. Initially an engineer officer in the Legion, he is graduated from the War School and holds a master degree of geopolitics from the French Institute of Geopolitics (Paris 8). More specifically, he has recently served in domains associated with intelligence, politico-military affairs and foresight analysis. He was assigned to various posts of coordination or conception, in France and abroad (Chad, Turkey, Belgium), and contributed to the French Defense Strategic Review of 2017, as head of office in the DGRIS (Directorate General for International Relations and Strategy).

Executive summary

Recent conflicts have highlighted a key characteristic of contemporary warfare, unprecedented in its scale and impact on the conduct of operations: “battlefield transparency”. Transparency is defined as the ability to acquire and exploit geolocated, near-real-time awareness of a given operational environment thanks to a connectivity architecture linking networks of heterogeneous and redundant sensors, mass data processing systems, and effectors.

However, the visual clarity guaranteed by technology does not automatically lead to the cognitive clarity that is required to understand an opponent’s intentions, or even to predict their actions. This study espouses a reasoned approach to transparency that reflects the permanent dialectic between transparency and opacity, between knowledge and ignorance. In that regard, transparency must be seen as the fruit of a 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 has benefited from the evolution of technology, gradually guaranteeing the tactical leader an increased visibility of his operational environment. At the beginning of the twenty-first century, the digital revolution opened a new chapter in military history, promising to fulfill a long-held ambition of piercing through the fog of war. While it held out the promise of a new art 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 in 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 principles of combat.

It drastically weighs on the character of future conflict due to 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 creates with information and decision-making, affected by the tyranny of immediacy and shared access to permanent, near-real-time information.

However, the transparency of the contemporary battlefield is neither homogeneous nor proven across all domains. Given their disparity and their specific resistance to detection, referring to "transparencies" in the plural would be more apt, 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. The performance, permanency, and pervasiveness of sensors of all kinds, coupled with new trends such as the increasing recourse to open-source intelligence (OSINT), give the impression that battlefield transparency has become 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 it also leads to the development of means of creating opacity, through three families of technological capabilities: concealment, transformation, and sensor disruption. Similarly, new technological 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 and on technological breakthroughs. Despite its advantages, transparency will remain limited by human errors in interpretation, as well as 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 maneuver in the light of this new reality of the battlefield. The first challenge is to survive even before maneuvering and fighting. Recreating a form of opacity thus means finding ways to evade detection by re-embracing tactical fundamentals: concealment, discretion, 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 in the drone segment.

Lastly, fighting in an increasingly transparent battlefield requires rethinking surprise by imagining new forms of maneuver. Whatever form it would take, maneuver could rely on creating "corridors of opacity", space-

time frames that would optimize the effects that contribute to blinding an adversary, which could then be exploited by a maneuver 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 brings with it the risk of escalation because of an enhanced temptation to resort to preemptive strikes.

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

Lastly, non-state adversaries can bypass the comparative advantages of state armed forces in terms of transparency, notably by exploiting opaque environments and by turning the democratization of transparency to their advantage.

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 informationnelle, 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.

Table of contents

Introduction

In May 2022, a Russian motorized battalion was completely destroyed while establishing a crossing over the Donets River, losing over 70 armored vehicles and almost 500 soldiers. The site had been identified beforehand by a Ukrainian drone, enabling artillery strikes to be precisely targeted at the troops concentrated up and downstream of the floating bridges.[1] Beyond comments on the tactical mistakes of the Russian armed forces, there is a school of thought that "ubiquitous surveillance of the battlefield" has left "nowhere for a relatively large formation to hide",[2] heralding the end of tactical surprise. Indeed, both sides' inability to conceal their tactical disposition on the Ukrainian battlefield, because of the profusion of all kinds of sensors along the entire front, is one of the conflict's most widely accepted lessons among analysts.[3] Nevertheless, over the last two years, this unprecedented ability to see the enemy's positions has not spared either side from errors of judgment, serious tactical mistakes, or even command failures.

"Friction", as Clausewitz defined it, remains a reality of the battlefield, as does uncertainty, which is heightened by chance and by the interactive nature of war. The Israeli intelligence community's failure to anticipate or detect Hamas's attack on October 7, 2023, was due to the same kinds of error and seems to suggest that surprise is in fact still a strategic and tactical option. Despite Israel's extensive surveillance system employing the most cutting-edge technologies, Hamas was able to evade Israeli sensors and warning systems in order to deceive its enemy as to its real capabilities and take full advantage of the astonishment caused by its surprise attack. Israel's failure was due primarily to a lack of imagination: the quantity of data being accumulated cannot be worth the quality of that data or the skill with which it is used.[4]

These two apparently contradictory examples raise questions about the reality of what is conventionally known nowadays as "battlefield transparency". This metaphor, which dates back to the formalization of the

1. T. Fouillet, "Guerre en Ukraine: étude opérationnelle d'un conflit de haute intensité (premier volet)", *Recherches & Documents*, No. 2/2023, Fondation pour la recherche stratégique, 2023, p. 50.
2. D. Johnson, "Would We Do Better? Hubris and Validation in Ukraine", *War on the Rocks*, May 31, 2022, https://warontherocks.com.
3. "Les 7 enseignements stratégiques de la guerre en Ukraine", French Ministry of Armed Forces, February 26, 2024, www.defense.gouv.fr; see also M. Zabrodskyi, J. Watling, O. Danylyuk, and N. Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, London: RUSI, 2022.
4. Interview with an Israeli intelligence official, November 19, 2023.

American doctrine of network-centric warfare (NCW) in the 1990s, refers to the unprecedented visibility of elements of the battlefield made possible by rapid progress in information and communication technologies:

> By harnessing satellite technology and the internet, sensors – from the everyday mobile phone proliferating across Ukraine to UAVs – by using AI and Machine Learning to exploit the huge volumes of data we collect, we have seen the battlefield rendered transparent.[5]

This transparency is produced by networking the data collected in an operational environment and sharing it with all the actors in the network in good time. It relies on a system of sensors, capacities for the fusion and analysis of information, and a network architecture, three areas that have seen uninterrupted technological innovation since the 1980s. The term "transparency" was chosen to contrast with the "fog of war" that it seeks to eliminate, a metaphor used by Clausewitz to represent the lack of clarity and the distortion caused by war's inherent uncertainty:

> Three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty [...] all action takes place, so to speak, in a kind of twilight, which, like fog or moonlight, often tends to make things seem grotesque and larger than they really are.[6]

A significant increase in visibility, in the meteorological sense of the term, would thus make it possible to "pierce the fog of war, in other words to achieve a kind of battlefield transparency".[7] It defies the natural opacity of war, which is characterized by patchy and imprecise information in the operational environment. The use of a physical property to describe this phenomenon is, however, problematic in two ways: First, it distorts the original meaning of the word "transparency", which in the physical sciences refers to a property of bodies allowing them to transmit light so that objects are clearly visible through them.[8] This definition is perfectly appropriate in underwater or aerial environments that must be passed through, but it makes little sense when applied to land. Second, it suggests that transparency has become an intrinsic property of the contemporary battlefield, whereas it is actually the result of a process that must be constantly updated and relies on a complex system for capturing and analyzing data. The fragility of transparency makes it a goal rather than a

5. P. Sanders, Speech by the Chief of the General Staff at the International Armoured Vehicles Conference, January 2023.
6. C. von Clausewitz, *On War*, trans. P. Paret and M. Howard, Oxford: Oxford University Press, 2007, pp. 46 and 88–89.
7. P. Samama, "Connecté et robotique: à quoi pourrait ressembler le char du futur de l'armée française", *BFM TV*, October 24, 2023, www.bfmtv.com.
8. "Transparent", *Merriam-Webster*, www.merriam-webster.com.

feature. It has to be conquered and in turn necessitates protection against the transparency achieved by the enemy.

Contrary to the doctrine of NCW, which was based on the tacit assumption that transparency would belong solely to the US armed forces, transparency is not exempt from the dialectical nature of war. In reality, not only are the technologies of transparency not exclusive, but attempts to impair the enemy's understanding are also reciprocal. More fundamentally, transparency continues to perpetuate a number of myths that date back to the period when it was formalized in the 1990s and that involve illusions about its capacity to revolutionize decision-making. These illusions stem from the unwarranted equation of a visual clarity achieved by technological means with a cognitive clarity that supposedly ensures understanding of the enemy's actions or even intentions. We are now approaching the limits of the concept of transparency, which is, after all, the opposite of opacity rather than of uncertainty. While accumulated and shared knowledge can help to reduce opacity, uncertainty remains a fundamental fact of war, intrinsically linked to the human dimension of conflict.

Acknowledging the reality of unprecedented visibility in the operational environment, while remaining within the conceptual limits of uncertainty, we can define transparency as the ability to acquire and exploit geolocated, near-real-time knowledge of a given operational environment thanks to a connectivity architecture linking networks of heterogeneous and redundant sensors, mass data processing systems, and effectors. The revolutionary nature of this new paradigm must be interrogated in order to assess how decisive the information superiority it provides actually is, and how much of a challenge it poses to the operating procedures of contemporary armed forces.

This study defends a reasoned approach to transparency, as the fruit of a fight for information superiority. Transparency should be seen as a potential resource to be won, protected, or denied, with information superiority considered in the same vein as environmental superiorities. Transparency can never be absolute and is inevitably subject to spatial and temporal constraints. It is the result of a compromise in the dialectic between understanding and ignorance, the quest for meaning and deprivation of the senses.

To understand the aims, scope, and limitations of the concept of transparency, we must first draw up a historical and conceptual overview of the quest for visibility and knowledge in the operational environment. This first step also allows us to examine how transparency is changing warfare, while paying attention to how it differs depending on the physical characteristics of the operational environment. Next, an in-depth look at intelligence and analysis capabilities alongside deception and disinformation technologies highlights the profoundly dialectical nature of the fight for transparency. The third section uses this dialectic to identify

and suggest possible ways to guard against, overcome, or exploit the enemy's transparency in a redefinition of information superiority. Finally, the last section explains how an understanding of the challenges of transparency is applicable at a strategic level across the whole spectrum of conflict, and in particular how it encourages escalation by combining detection, speed, and lethality.

Total visibility to ensure victory: An ancient dream, a recent concept

The search for knowledge has always been one of the fundamental needs of any military leader engaged in combat. In the sixth century BCE, Sun Tzu had already identified knowledge—of oneself, one's troops, one's environment, and one's enemy—as the general's most crucial asset to achieve victory.9 Even today, the French Army includes "understanding" as one of the eight "factors of operational superiority" needed to dominate an enemy and win in combat.10 The need to know makes up a large portion of combat actions, as the British general the Duke of Wellington commented:

> All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know by what you do; that's what I called "guessing what was at the other side of the hill".[11]

For a long time, the need to see in order to understand kept battles contained within the limited space that the commander-in-chief could take in from his vantage point. Between battles, by contrast, ignorance prevailed. A series of technological advances extended the battlefield, first gradually and then drastically, and at the same time increased the desire to see further, more accurately, and for longer. At the beginning of the twenty-first century, the connectivity revolution opened a new chapter in military history, fulfilling the ambition to pierce the fog of war that for so long frustrated the greatest military leaders. Promising a new art of war that would consign the old principles and procedures to oblivion, this unprecedented transparency nevertheless generated its own illusions. To distinguish how and to what extent new technologies are actually transforming tactical engagement, we must look at recent technological developments from a long-term historical perspective.

9. Sun Tzu, *The Art of War*.
10. "Action terrestre future", État-major de l'armée de Terre, 2016, pp. 25–27.
11. Duke of Wellington, cited in J. Croker, *The Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, Secretary to the Admiralty from 1809 to 1830*, Vol. 3, edited by L. J. Jennings, London: John Murray, 1885, pp. 276–277.

Long-term transparency: An unattainable grail

Between tactical transparency and strategic opacity

The fog of war is one of Clausewitz's fundamental principles, implying that the battlefield has always been clouded. Nevertheless, a rapid overview of history suggests the contrary. The battlefield, understood in the classical sense as an area of limited dimensions[12] where several protagonists confront one another, was generally a space where most of the enemy's positions and movements could be observed. Although the commander-in-chief could see—with the aid of a "spyglass" from the seventeenth century—most of the battlefield as long as he was positioned in the right place, he could still be misled by the enemy or misinterpret the latter's intentions. The ability to locate enemies is not correlated with the ability to predict their behavior. There are numerous examples of ruses of war, fake retreats to draw an enemy away from a favorable position, feint attacks, or diversions being used to bring about decisive victories despite the essential facts of the enemy's position being known.[13] Even almost total transparency, understood as a view of the enemy's positions, does not predetermine the outcome of a battle. A "material" equation (distance, firepower, terrain, troop density, etc.) that seems easy to understand can be altered by a range of "immaterial" factors, such as interpretation of the sequence of events, contingency (Clausewitz's "friction"), troop cohesion, and the clear-headedness of commanders. However physically transparent the battlefield may be, uncertainty remains around the outcome of the battle. Choosing to "do battle" means accepting an element of chance, even when every last detail has been planned in advance.

Siege warfare is also relatively transparent. The site of confrontation is, by definition, circumscribed. The attacking army often knows the size of the garrison, albeit approximately, and can surmise the state of food reserves and drinking water supplies, material facts that can be acquired from informers. By contrast, it is more difficult to assess the morale of the garrison, and even more so that of the inhabitants: How much hardship are they prepared to endure, and for how long?[14] Here again, knowledge of physical facts does not automatically mean victory, which often also

12. For example, a quadrilateral of around 2 km x 3.5 km for Waterloo, although that was admittedly smaller than the average for the time. See J. Macdonald, *Grandes Batailles de l'histoire mondiale*, Paris: Albin Michel, 1985.
13. J. Latimer, *Deception in War*, New York: Overlook Press, 2001.
14. See V. Melegari, *The Great Military Sieges*, London: Ferndale Editions, 1981.

depends on psychological factors (willpower, cohesion, bluffing[15]). vUncertainty is further heightened by the vagaries of chance (weather conditions, epidemics).

While physical transparency has dominated at the tactical level throughout military history, the transparency-opacity relationship is more ambiguous at the operational and strategic levels. General Beaufre points out that, until the end of the eighteenth century, armies traveled in a single bloc for security and logistical reasons.[16] This made it easy for light cavalry to spot them, rendering operational surprise difficult. The Comte de Guibert's idea to divide armies into divisions, which was perfected by the Napoleonic system of corps d'armée, enabled autonomous corps to move more fluidly within the theater of operations. As a result, opacity regained the upper hand over transparency because of the difficulty of locating each of these large mobile corps. And even when some of them could be located, this did not generally provide enough information about the overall maneuver. Where is the maneuvering mass concentrated? Are some of the forces engaged in an enveloping movement? Should a corps' relative isolation be exploited to attack it, or is it a trap, with other corps positioned near enough to come to its assistance "at the sound of gunfire"? The presence of light reconnaissance units in the vanguard or along the flanks generally did not make it possible to resolve all these unknowns. The Napoleonic system, soon adopted by all the major powers, thus altered the transparency-opacity relationship.

Until that time, then, there was nothing intangible in this relationship. Its fluctuations reflected a transparency that was manifested more at the tactical level, while opacity remained important at the strategic level because of a lack of intelligence collection resources (spies were still the principal means of gathering information).

The acceleration of technological progress from the end of the eighteenth century to the Cold War

Technological advances, initially tentative, tended generally toward greater transparency. The gas balloon[17] used at the Battle of Fleurus (1794) and again at the Battle of Mainz (1795) made it possible to observe movements and impacted the morale of enemy troops who knew they were being watched. The semaphore-based Chappe telegraph system (introduced in

15. When a besieged army pretends (via communications) to be in a comfortable situation (in terms of provisions or the arrival of fake reinforcements); inversely, the threat of mass executions if the besieged army does not surrender immediately, used almost systematically by the Mongols (see T. May, *The Mongol Art of War*, Barnsley: Pen and Sword Military, 2007).
16. A. Beaufre, *Introduction à la stratégie*, Paris: Pluriel, 2012, pp. 82–84.
17. *L'Entreprenant*.

1794) accelerated the dissemination of information, one of the factors of transparency, and did so over long distances as well. It was perfected over the course of the nineteenth century, particularly during the American Civil War, which combined the technological and operational advances of the telegraph and balloons. Airships were still widely used during the First World War.

From the First World War, however, progress increased rapidly, mostly at the tactical level. At the Battle of the Marne, airplanes played an important role on the Allied side by spotting the 1st German Army's change of direction.[18] Photographic equipment soon supplemented and extended the range of the human eye. Advances in radio transmission (on-board wireless transmitters) helped to shorten the detection-processing (trajectory adjustment)-artillery firing loop. These improvements in detection were primarily felt at the tactical level, because the air force had little capacity to operate at depth.[19] There were also advances in terrestrial and naval camouflage.[20] The interception of enemy communications, particularly those sent via undersea telegraph cables, was a new development. The "sword and shield" dialectic tends to be clearly observable in the field of cryptography (information coding), where the desire to listen to the enemy, while preventing the enemy doing the same to you, leads to constant technological developments. This competition in the electromagnetic spectrum is found at all levels, from the tactical to the strategic. Again, the dialectic of this "code war" alone is not enough to influence the outcome of a conflict,[21] but a window of technological superiority can confer an important advantage at a given time.[22]

We do not have space to discuss all the developments that took place during the Second World War. They included technological improvements in reconnaissance capabilities on land, in the air, and at sea, particularly driven in the air-sea domain by the immense size of the Pacific theater, which hampered the detection of fleets. Also worthy of note is the technological breakthrough represented by the use of radar, which played a decisive role in the Battle of Britain in 1940.[23] The invention of ASDIC (Anti-Submarine Detection Investigation Committee), later refined as sonar (sound navigation and ranging), changed the nature of anti-submarine warfare. Deception operations[24] to evade enemy detection or mislead the

18. M. Goya, *S'adapter pour vaincre, comment les armées évoluent*, Paris: Perrin, 2019, pp. 63–64.
19. Other than heavy bombers.
20. Particularly the technique of dazzle painting used to disguise the shape of naval vessels.
21. This code war played an even more important role in the Second World War, when the Enigma machine made it possible to decipher German communications.
22. When a former student of the École polytechnique, Georges Painvin, managed to decipher a German message, Foch's GHQ was able to thwart the offensive launched near Compiègne on June 2, 1918. Similarly, the interception of the famous Zimmermann telegram, which proposed a German scheme to use Mexico against American interests, contributed to the United States' decision to join the war.
23. M. Williamson, *War in the Air 1914–1945*, London: Cassell, 2002.
24. R. Hémez, *Les Opérations de déception. Ruses et stratagèmes de guerre*, Paris: Perrin, 2022.

enemy reached an unprecedented level of sophistication in terms of both scale and technicality, whether in concealing large concentrations of units (the Soviet *maskirovka*[25]) or developing full-scale maneuvers at the strategic level combining all the deception techniques[26] (concealment, simulation, disinformation): Operation Fortitude[27] was the culmination of this approach. Thus, even when dealing with massive concentrations of resources, it is possible to alter battlefield transparency.[28]

The Cold War gradually added the space domain to the equation. Driven initially by the urgent need to detect the launch of intercontinental nuclear missiles, the development of military satellites soon expanded to other operational uses: intelligence (listening, optical or radar imaging), meteorology, long-range secure telecommunications, and, toward the end of the period, geolocation (GPS systems).

As this historical overview shows, the question of transparency takes different forms at the tactical, operational, and strategic levels. It is embedded firmly within the sword-shield dialectic (a given advance is often counteracted by another), reflecting the fluidity of the relationship between transparency and opacity. Finally, "seeing" (or "listening") is not the same as "understanding" the enemy's maneuver: misinterpretations are always possible, whether due to human error or skillfully devised subterfuges on the part of the enemy. These errors of judgment are made more likely by the sheer number of factors that must be taken into account, both material and immaterial, as well as the inherent uncertainty of combat.

The emergence of connectivity: When transparency becomes possible

Network-centric warfare: The RMA and the connectivity turn

The idea of a new battlefield "transparency" emerged in the wake of the spectacular development of new information and communication technologies (NICTs) and positioning technologies (GPS). Reaching maturity at the end of the Cold War, these technologies were combined into a coherent theory by advocates of the "revolution in military affairs" (RMA),[29] who saw the convergence of information acquisition and processing capabilities and the precision of targeting equipment as the

25. For example, Operation Bagration (Summer 1944) decimated the German Army Group Center.
26. See Diagram II-5, "The three modes of deception", p. 49 of this study.
27. The operation was supervised by Churchill himself and aimed to deceive the Germans into believing that a landing would take place in the Pas-de-Calais instead of Normandy.
28. See B. Whaley, *Stratagem: Deception and Surprise in War*, Boston: Artech House, 2007.
29. B. Tertrais, "Faut-il croire à la 'révolution dans les affaires militaires?'", *Politique étrangère*, Vol. 63, No. 3, Ifri, September 1998, pp. 611–629.

ingredients for a new art of war. In the 1970s, General William Westmoreland (Chief of Staff of the US Army from 1968 to 1972) displayed keen foresight when he predicted that battlefields would be "under 24 hour real or near real time surveillance of all types" and that "enemy forces will be located, tracked, and targeted almost instantaneously through the use of data links, computer assisted intelligence evaluation, and automated fire control". Military commanders would be "continually aware of the entire battlefield panorama" and would be able to "destroy anything we locate through instant communications."[30] In the same context, US Colonel John Boyd modeled decision-making by suggesting that operational superiority depends essentially on a system's ability to complete its decision loop more quickly than its opponent. He was referring to the well-known OODA loop (observe, orient, decide, act), with the goal being to shorten the time between observation and action.[31]

This networked convergence saw its first deployment in the 1990–1991 Gulf War. The technological expertise of the US-led coalition established the superiority of the network-centric warfare model, which was first explicitly theorized in 1998.[32] This model relies on connectivity and a rapid decision cycle.[33] Information technologies gave the coalition the "quality of firsts"[34]—"see first, decide first, act first"[35]—needed to impose their decision cycle on the enemy. The US-led coalition's emphatic victory over the Iraqi Army validated the model and opened the door to a new form of warfare. The aim was to control information by seeking "total" battlefield transparency, giving decision-makers perfect, constant, and real-time visibility of the operational environment. Transparency, understood as the ability to "see everything in a given area",[36] became an operational goal, with military effectiveness measured in terms of the ability to ensure a one-to-one "equation"[37] between the detection and immediate destruction of a target.

From the 2000s, the RMA was gradually superseded by *transformation*, which enshrined "total battlespace awareness" as the key to dominating the enemy. One example is the concept of "dominant

30. W. Westmoreland, "Battlefield of the Future", *US Army Aviation Digest* 16-2, Department of the Army, 1970.
31. See D. Fadok, *La Paralysie stratégique par la puissance aérienne*, Paris: Economica, 1998.
32. A. Cebrowksi and J. Garstka, "Network-Centric Warfare: Its Origin and Future", *Proceedings*, Vol. 124, No. 1, January 1998; see also M. Shurkin, R. Cohen, and 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*, London: Brassey's, 2004.
34. H. McMaster, "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.
36. É. de Durand, "'Révolution dans les affaires militaires': 'Révolution' ou 'transformation'?", *Hérodote*, Vol. 2, No. 109, 2003, pp. 57–70.
37. J. Henrotin, "Les mutations du renseignement militaire, dissiper le brouillard de la guerre?" *Focus stratégique*, No. 71, Ifri, January 2017.

battlespace knowledge",[38] which suggested that "automatic data processing, sensor technology, and telecommunications" would be integrated into a system-of-systems enabling the US Army to acquire "dominant battlespace knowledge" by 2005. Likewise, the concept of "rapid dominance" seen in the "shock and awe" doctrine implemented in Iraq in 2003 was based on "near total or absolute knowledge and understanding of self, adversary, and environment".[39]

Counterinsurgency operations soon raised doubts about the reality of this transparency, however. Opacity is still a key feature of the counterinsurgency environments in which the Western armed forces have operated since the 2000s.[40] Asymmetry makes domination by information less decisive and limits the effectiveness of the hyper-technological approach that seeks to master war through perfect knowledge of the parameters of the operational environment.[41] In that respect, the Gulf War, which was exceptional in terms of its "information asymmetry",[42] skewed perceptions about the decisive nature of the information and technological superiority provided by network-centric warfare.

Perfect visibility of the battlefield: From hope to illusion

In the quest to dominate the enemy by means of information, the network became the means to make information itself into simultaneously a weapon, a lever, and a target,[43] in a new model known as "data-centric warfare". This ambition to control information was based on four major hopes regarding the benefits of transparency: improving command and control (C2), mastering the environment, strengthening friendly forces, and maximizing enemy attrition.

The deepest illusion, and the one most closely associated with the metaphor of transparency, is that of omniscience and certainty. It stems from a confusion between perceiving the battlefield accurately and controlling all its parameters, understanding its dynamics, or predicting the enemy's intentions. This intellectual slippage from knowledge to understanding and prediction is currently being repeated in the context of the potential applications of AI. The mirage of perfect knowledge has been strongly influenced by the ideas of the US Admiral Bill Owens, particularly in his book *Lifting the Fog of War*, which made "an omniscient view of the

38. S. Johnson, "DBK: Opportunity and Challenges", in S. Johnson and M. Libicki (eds.), *Dominant Battlespace Knowledge*, Washington, DC: National Defense University, 1996, pp. 17–20.
39. H. Ullman, J. Wade et al., *Shock and Awe: Achieving Rapid Dominance*, Washington, DC: National Defense University, 1996.
40. J. Henrotin, "Les mutations du renseignement militaire".
41. P.-M. Léoutre, *Comment l'Occident pourrait gagner ses guerres*, Nancy: Le Polémarque, 2013.
42. T. Benbow, *The Magic Bullet?*, p. 118.
43. DCDC, JCN 2/18, *Information Advantage*, UK Ministry of Defence, 2018.

battlefield in real time"[44] the key to military victory.[45] But understanding ultimately depends on a commander's ability to make sound judgments, which requires not just information and contextual knowledge, but also discernment, insight, and clear-sightedness: human qualities that are inevitably fallible and imperfect.[46]

This illusion of technological perfection continues to regularly influence US strategic culture.[47] A more sober way to understand transparency is as a lever for accelerating the decision cycle. The ability to enjoy a permanent "information advantage",[48] thanks to both near-perfect knowledge of the situation and the continuous denial of such knowledge to the enemy, is seen as a key factor in operational superiority, accelerating the operational tempo by making decisions "at information speed" and straining the enemy's decision cycle to the point of implosion. Robert Leonhard considers speed to be the most important advantage offered by transparency.[49]

The ambition to master the environment comes from the constant expansion of arenas of confrontation over increasingly large and open spaces. Like in naval combat, where the vast size of the environment makes knowledge of the enemy's position a prerequisite for gaining a tactical advantage, the quest to master the operational space results in "a continuous effort to scan an ever-greater area at ever-greater speed".[50] The twofold challenge of space and time makes it useful to interpret the operational situation in the form of a shared, geolocated, and up-to-date common operational picture (COP). This model for representing the operational environment seeks to master the parameters of combat but is challenged by the growing tactical need to acquire knowledge ever more quickly, accurately, and further away.[51]

Shared, near-real-time knowledge of the friendly situation is in itself a unique phenomenon in military history, the full implications of which have yet to be understood.[52] Military commanders now have a complete, tailored view of their own tactical disposition and of the state of their forces. Blue

44. B. Owens, *Lifting the Fog of War*, New York: Farrar, Straus and Giroux, 2000.
45. M. T. Owens, "Reflections on Future War", *Naval War College Review*, Vol. 61, No. 3, US Naval War College Press, 2008, pp. 61–76.
46. "Action terrestre future", p. 25.
47. I. Reynolds, "Seeing, Knowing, and Deciding: The Technological Command Dream That Never Dies?", *War on the Rocks*, July 13, 2022, https://warontherocks.com. See also A. Cattaruzza and S. Taillat, "Les enjeux de la numérisation du champ de bataille", *Dynamiques internationales*, No. 13, 2018, p. 2.
48. *Summary of the Joint All-Domain Command and Control (JADC2) Strategy*, US Department of Defense, 2022.
49. R. Leonhard, *The Principles of War for the Information Age*, Novato: Presidio Press, 1998.
50. T. Lavernhe and 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 (ed.), *Guerre et manœuvre*, Paris: Economica, 2009.

force tracking (BFT), which can geolocate friendly units with ever-higher refresh rates,[53] helps to reduce the risk of friendly fire, improve the distribution of forces on the ground, and gain a better understanding of their maneuvering capabilities. On the logistical side, embedded sensors and advances in AI will also strengthen friendly forces by making it possible to constantly monitor the logistical parameters of each deployed unit, to scale support in line with actual operational needs, and to improve the operational availability of equipment thanks to progress in predictive maintenance and the optimization of repair diagnostics. This transparency is less about lifting the fog of war than eliminating the causes of Clausewitz's "friction". Drawing very optimistic conclusions from the cumulative progress in friendly and enemy knowledge associated with the precision of fires, Guy Hubin has even claimed, no doubt prematurely, that the move away from saturation fire will de facto lead to a drastic reduction in logistical flows[54] and a loosening of resupply constraints.

From an early stage, the hope of acquiring perfect visibility of the battlefield went hand in hand with the hope of being able to instantaneously destroy any target discovered. Unprecedented advances in sensor technology, whether in performance, redundancy, or durability, coupled with progress in connectivity and the increased range of terrestrial and aerial effectors (see section 2), have led to transparency being conceived almost exclusively in terms of attrition, limiting the new art of war to two technical actions: "finding targets and hitting them"[55] by means of a "reconnaissance-fire loop"[56] or an optimized kill chain. This gives rise to a model of battles waged by and for fires and oriented primarily toward enemy attrition. This tendency to think about transparency solely in terms of targeting is reinforced by the increasing precision of indirect fire, as seen on the Ukrainian front,[57] and the lethality of a battlespace saturated with means of observation. The ultimate goal for this optimization would be to make strikes almost immediate by reducing the decision loop to a few seconds.[58] Instantaneous visibility would equate to instantaneous effect in a combat environment where to be discovered would amount to being destroyed.

53. The speed with which tactical information (including positioning) is updated.
54. G. Hubin, *Perspectives tactiques*, Paris: Economica, 2009.
55. M. Libicki, "The Small and the Many", in J. Arquilla and D. Ronfedlt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND Corporation, 1997, pp. 191–216.
56. Interview with a senior officer in the French Army, December 4, 2023.
57. J. Watling and N. Reynolds, "Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive", *Special Report*, RUSI, 2023.
58. Interview with a senior officer in the French Army, February 6, 2024.

Connectivity, the fragile nervous system of transparency

Beyond questions of doctrine, transparency is essentially the product of a system that networks data in time and space, based on:

- sensors that collect a variety of data in large quantities, constantly, and throughout the entire operational environment;
- tools for fusing and analyzing this data, giving it temporal and spatial meaning (geolocation, harmonization, and up-to-date overviews);
- a network to enable instantaneous transmission of the collected and processed data and so ensure its validity, in other words its operational value.

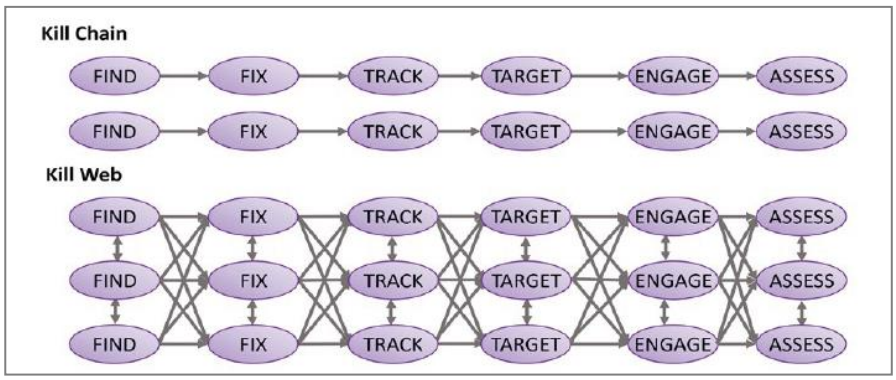
This synergy of data in time and space gives decision-makers a kind of "panoptic" view, understood as the capacity to take in the entire battlespace at a glance.[59]

Connectivity is the key to this system, the "digital backbone" of contemporary capability models, into which "all sensors, effectors and deciders will be plugged"[60] and without which they lose their inherent superiority. It requires a network that is stable and powerful enough to circulate the vast quantities of data generated by contemporary sensors at ever-greater speeds. The dimensions of connectivity networks are expanding in a breathtaking change of scale, opening the way to the era of "hyperconnectivity".[61] The 4G network currently consists of around 20.4 billion connected devices around the world, or around 60,000 devices per square kilometer. The 5G network will support more than a million devices in the same area.[62] To take an example from the military domain, the volume of data shared between future FDI (defense and intervention frigates) will be a million times higher than that currently shared between FREMM (multi-purpose frigates).[63] Similarly, the video streams from the drones crisscrossing Ukrainian airspace would be unusable without the 100 megabits per second (Mbit/s) that the Starlink network guarantees to command posts (CP) equipped with its terminals.[64]

59. This idea comes from Jeremy Bentham's "panoptic" prison, which is designed to be completely visible to the observer. It was developed further by Michel Foucault in *Discipline and Punish*. See C. Laval, "Surveiller et prévenir: la nouvelle société panoptique", *Revue du MAUSS*, No. 40, 2012, pp. 47–72.
60. N. Carter, speech given at Policy Exchange, September 30, 2020, www.gov.uk.
61. L. Meny, "L'art de la guerre dans un monde hyperconnecté", *Revue Défense Nationale*, HS no. 4, 2021, pp. 155–168.
62. N. Monaco, S. Minneman and K. Joseff, *The Hyperconnected World of 2030-2040*, IFTF, 2020.
63. Interview with an executive in the defense industry, December 6, 2023.
64. S. Skove, "What the US Military Can Learn from Ukrainian Command Posts", *Defense One*, January 12, 2024, www.defenseone.com.

The technological complexity of contemporary connectivity is compounded by the increasing complexity of the purposes it serves. The "intelligence-fire" loop or "kill chain" provides a good example of the density of the connectivity mesh required to network the functions on which it depends. In reality, "seeing" is far from enough, and it overlies a much more complex reality. The data capture function consists of several successive or simultaneous stages: "find, fix, track, target, engage, assess".[65] The primary objective is to close the chain as quickly as possible, but also to be able to run several identical loops simultaneously, which increases connectivity demands further. Vulnerability to enemy cyber-electronic actions also necessitates redundancy to ensure network continuity, transforming the "chain" into a "web".[66]

Diagram I-1: The evolution of connectivity, from "chain" to "web"

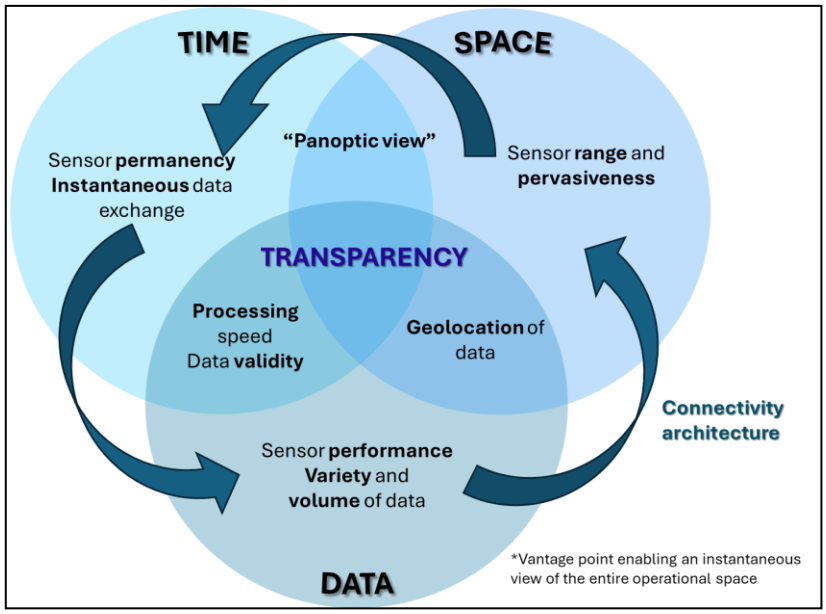


Source: H. Penney, "Scale, Scope, Speed, & Survivability: Winning the Kill Chain Competition", Policy Paper, Mitchell Institute, 2023.

Transparency is thus the desired outcome of a capability model designed around data and linked via a connectivity network set up to capture, fuse, store, and disseminate this data. Transparency depends on technical optimization (network design, management of bandwidths and frequency range saturation), but also procedural and organizational optimization to organize and manage the mass of data generated and ensure a fluid, rapid, and constant decision loop. By contrast, an enemy only has to target one link in this connectivity chain to significantly impact the transparency delivered at the end of the chain.

65. H. Penney, "Scale, Scope, Speed, & Survivability: Winning the Kill Chain Competition", *Policy Paper*, Mitchell Institute, 2023.
66. The term used in French doctrine is a "*réseau multi-senseurs/multi-effecteurs*" (multi-sensor/multi-effector network), or RM2SE.

Diagram I-2: The transparency model



© Pierre Néron-Bancel, Ifri, 2024.

The end of uncertainty?

"There is no sanctuary on the battlefield"[67]

Against the positive view of transparency as a factor of operational superiority, recognition of its reciprocity[68] casts doubt on its absoluteness. The possibility of the enemy acquiring transparency suggests it should instead be analyzed in terms of the restrictions it places on the battlefield and the principles, procedures, and capabilities that it undermines or invalidates.

The most drastic restriction imposed by transparency, especially in the land domain, is the increase in lethality. The continuity and quality of contemporary means of surveillance have a significant negative impact on the factors that ensure survivability, which is like an onion formed of "successive layers that structure a combat engagement": "detect without being detected; if you are detected, don't be identified; if you are identified, don't be fixed; if you are fixed, don't be hit…".[69] The impossibility for an armored vehicle to move around the Ukrainian front line by day is testament to the massive impact of sensor saturation on survivability. Even the safety of infantrymen sheltering underground or protected by armor is

67. M. Zabrodskyi et al., *Preliminary Lessons*, p. 53.
68. Interview with a researcher, December 13, 2023.
69. R. Hémez, "La survivabilité sur le champ de bataille. Entre technologie et manœuvre", *Focus stratégique*, No. 72, Ifri, March 2017.

challenged by the development of suicide drones known as "FPVs",[70] which can detect and hit targets in trenches.

The rear, previously considered a sanctuary beyond the range of enemy sightlines or tactical fires, can no longer be seen as safe. This is confirmed by the obsolescence of current models for the deployment of logistics bases and command posts, which are already struggling to deal with the expansion of effector ranges. The Ukrainian strikes on the Berdyansk and Luhansk airfields on October 17, 2023, which destroyed nine Russian helicopters,[71] illustrate this increased vulnerability in rear areas and the conceptual difficulty in adapting to this new reality. Nevertheless, we should take a measured view of the actual extent of transparency at depth. As distance from the frontline increases, it becomes increasingly difficult to identify valid objectives.[72]

More broadly, however, it is the very concepts of discretion and secrecy that seem to be challenged by the advent of enemy transparency, raising the question of the new necessary conditions for tactical surprise.[73] The two fundamental factors of surprise are speed and secrecy, but the unprecedented legibility of tactical disposition severely limits discretion and makes the use of tactical surprise uniquely difficult. Nevertheless, the ability of the Ukrainian armed forces to conceal preparations for the Kharkiv counteroffensive, gathering five armored and mechanized brigades in one place without the knowledge of Russian intelligence in August 2022, suggests that discretion remains viable under certain conditions.[74]

The same challenges around discretion are likely to arise by 2050 in the underwater domain, where the converging trends of artificial intelligence, advances in maritime detection, and underwater communications systems will have a radical impact on the natural opacity of the environment and submarine counter-detection measures.[75] A shift in the opacity-transparency balance toward the latter would, of course, have major implications for the security of naval materiel, in particular that associated with nuclear deterrence.[76] Any challenge to submarine discretion would compromise submarines' ability to "fade" into their environment, which is precisely what gives submarine combat its characteristic

70. "First-person view". See "Killer Drones Pioneered in Ukraine Are the Weapons of the Future", *The Economist*, February 8, 2024, www.economist.com.
71. "Guerre en Ukraine: des frappes destructrices sur des aérodromes de l'armée russe revendiquées par l'Ukraine", *Le Figaro*, October 18, 2023, www.lefigaro.fr.
72. Interview with a senior officer at the CPCO, January 16, 2024.
73. R. Hémez, "L'avenir de la surprise tactique à l'heure de la numérisation", *Focus stratégique*, No. 69, Ifri, July 2016, pp. 19–22.
74. M. Goya, "1918 en Ukraine", *La voie de l'épée*, October 29, 2022, https://lavoiedelepee.blogspot.com.
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, No. 2, 2024, https://tnsr.org.

uncertainty. This prospect is being fiercely debated in the most advanced navies, which closely follow scientific progress in the area and strive to remain two steps ahead by optimizing carrier stealth.

The increased legibility of tactical positions also raises questions about the validity of the principle of concentration of forces.[77] Force concentration is no longer desirable, because it can be immediately detected, or even possible, because it can be immediately targeted. Does this spell the end of the principle of concentration?[78] The challenge is now to concentrate resources rapidly and to keep tactical movement fluid in order to stay ahead of enemy detection. What is at stake is the future of maneuver itself, which is currently being neutralized on land by a twofold phenomenon. On one side, advances in transparency are pinning maneuver to a fixed front, while on the other, the linearity of maneuver is magnifying the effects of transparency, particularly attrition.[79] In the classic American doctrinal debate between maneuver and attrition,[80] proponents of attrition argue that the omnipresence of battlefield surveillance has "killed maneuver" by amplifying the dominance of fires over mobility, limiting future land battles to artillery duels above a "dangerous no man's land".[81] Although RMA theorists saw domination by information as the means to achieve decisive "*foudroyance*",[82] it seems as if the decisive nature of transparency will be canceled out by its reciprocity.

The effects of hyperconnectivity on C2

Shared access to continuous, real-time data is also profoundly transforming command processes, leading to questions about how transparency might change relationships to information and decision-making processes. Contemporary NICTs facilitate exchange between users of a network by accelerating the expression and fulfillment of needs, but also by significantly expanding the available range of options thanks to the addition of an increasing number of sensors and effectors to the network.

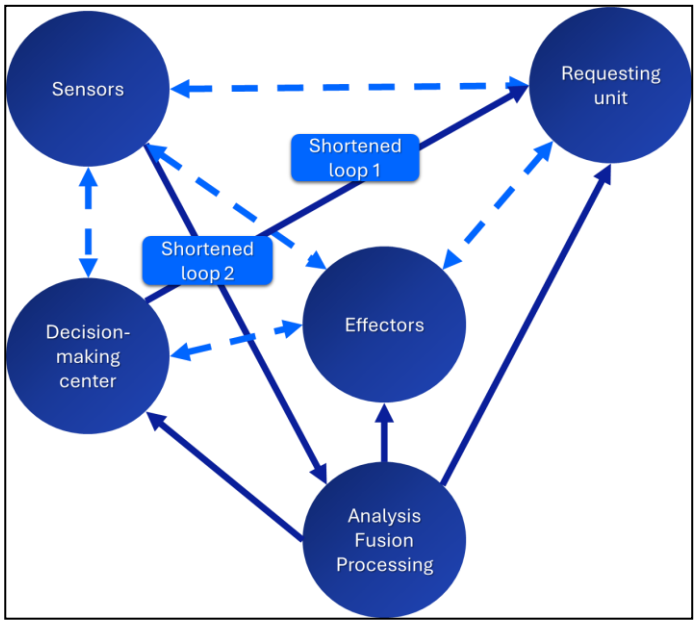
In this sense, hyperconnectivity leads to the "Uberization"[83] of data, suggesting a new relationship to command network organization, which is

77. A. Faurichon de la Bardonnie, "Le paradoxe de la surprise et de la transparence", *Revue Défense Nationale*, HS No. 13, 2023, pp. 46–62.
78. G. Hubin, *Perspectives tactiques*.
79. Interview on December 13, 2023.
80. See P. Garrett and F. Hoffman, "Maneuver Warfare Is Not Dead, But It Must Evolve", *Proceedings*, No. 149/11, November 2023; F. S. Gady, "Manoeuvre Versus Attrition in U.S. Military Operations", *Survival*, Vol. 63, No. 4, August–September 2021, pp. 131–148.
81. A. Fox, "Manoeuvre Is Dead? Understanding the Conditions and Components of Warfighting", *The RUSI Journal*, Vol. 166, April 2022, pp. 10–18.
82. "The Ability to Strike Powerfully, Quickly, and Suddenly in Order to Surprise and Shock", CIA 01, *Concept d'emploi des forces*, État-Major des Armées, 2021.
83. To be understood here not in the sense of a challenge to the traditional economic model, but rather as the development of a model for directly linking geolocated client needs to available services in real

oriented toward continuous optimization of the information cycle. The desire to make surveillance systems more efficient and profitable by accelerating the decision loop is reflected in a physical shortening of the loop, allowing requesters to link sensors directly to effectors without necessarily having to analyze the information first or receive approval from decision-makers. The choice to keep the loop short necessarily leads to the development of horizontal structures and the reduction of vertical interaction. It can also reinforce a tendency to privilege the sensor's "information" over the analyst's "intelligence".

If the sensor is managed directly at the highest decision-making level, however, the direct sensor-effector link in a shortened loop can have the opposite effect of removing the receiving unit from the loop. Operational needs are thus at risk of being overwhelmed by the transparency loop's logic of efficiency. This bias can be seen in the repeated refusals by the Ukrainian higher echelons to provide the smoke cover requested by units in contact on the basis that they wanted to prioritize visibility for their drones.[84] In another example of this "fascination with sensors",[85] Ukrainian CPs with a video link to their drones tend to primarily target objectives covered by the drones in the depth, while neglecting objectives in contact with units issuing fire requests.[86]

Diagram I-3: The shortened connectivity loop



© Pierre Néron-Bancel/Ifri, 2024.

time. See C. Parker, "Uber-Style Technology Helped Ukraine to Destroy Russian Battalion", *The Times*, May 14, 2022.
84. J. Watling and N. Reynolds, "Stormbreak", *op. cit.*, p. 22.
85. J. Henrotin, "Les mutations du renseignement", *op. cit.*, p. 17.
86. Interview on February 6, 2024.

The effects of transparency on command posts

The vulnerability of ground tactical command posts is at the heart of current debates around battlefield transparency. Two mutually reinforcing trends can be observed:

- first, contemporary sensors are increasingly capable of detecting the multispectral signature of the CPs of large units, making it much more complicated to conceal them;
- second, the centrality of data in command systems limits the discretion of CPs and significantly increases their footprint in all fields (size and composition, logistical weight and trail, thermal signature, digital signature, and electromagnetic radiation), while also making them an essential node in the connectivity system, such that destroying them significantly degrades a force's combat capability.

Since 1945, command systems have undergone an "inflationary drift"[87], leading to an expansion of their functions, growing demand for precision and comprehensiveness encouraged by the post-Cold War context of "operational comfort", and increasingly complex procedures and doctrines.[88] This inflation has been fueled by requirements regarding the quality and volume of information and the quest for ever-greater control over the operational environment, requiring ever more specialists, servers, and monitoring and datalink systems,[89] not to mention the resulting multiplication of defense staff processes.

Modern CP systems must obey two contradictory imperatives: they must accelerate their processes and be more connected in order to gain a better understanding of the operational environment, while also drastically diminishing their electromagnetic footprint in order to be more discreet and limit their vulnerability. Their growing dependence on operational information and communication systems (CIS) makes it impossible for them to reduce their digital and electromagnetic footprint without impacting their effectiveness. This logic also applies to warships, whose electromagnetic signature reduces the discretion of naval deployments at sea.[90]

87. General Alabergère, cited in S. Caplain and R. Hémez, "Haute intensité: la survie des postes de commandement", *DSI*, No. 153, Areion Group, May–June 2021, www.areion24.news.
88. S. Caplain, "La fourmilière du général: le commandement opérationnel face aux enjeux de haute intensité", *Focus stratégique*, No. 89, Ifri, June 2019.
89. M. Beagle, J. Slider, and 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*, March 2023, www.armyupress.army.mil.
90. E. Lanquetot, "Le silence relatif, une condition de la foudroyance", *DSI*, No. 163, Areion Group, January–February 2023, pp. 70–75.

Multiple transparencies with very different realities

To define the degree of transparency of the contemporary battlefield, we must take account of the disparity between different environments and their resistance to detection. It would, in fact, be more appropriate to talk about "transparencies" in the plural, adapting the concept to the specific characteristics of each domain, focusing here on the physical environments that elicit a human presence.

Since the refinement of radar technology, airspace has been the most transparent environment. Because airspace is by nature devoid of human activity, aerial activity is necessarily temporary and so discontinuous, making it a more easily detectable anomaly.[91] Beyond stealth or certain forms of deception jamming, the air force has learned to deal with the transparency of its environment and maintain ambiguity around its intentions, exploiting speed and mobility to delay detection to the last possible moment and limit the enemy's window of opportunity to react. In that sense, air maneuver seeks surprise, as defined by Leonhard, who sees it as resulting "from the interaction of two components: perpetual unreadiness and time".[92] Nevertheless, possessors of stealth technologies seem to have regained a form of opacity not seen since 1940.

As the interface between the land, air, and underwater domains, the sea is the most paradoxical environment when it comes to transparency: highly legible but vast on the surface, and extremely opaque and complex underwater. Coastal areas, meanwhile, are particularly impervious to surveillance from the sea, while making maritime approaches more clearly visible from land. Naval maneuver seeks to exploit the uncertainty generated by the ability to fade into the immensity of the environment while striving to gain some control over this uncertainty to protect itself, for which purpose it devotes significant resources to maintaining the dilemma of the dispersal of means.[93]

The high opacity of the land environment[94] is due firstly to its highly heterogeneous and discontinuous nature, secondly to a lack of depth of view (vegetation, topography, built-up areas), and finally to the extreme diversity of human activities continually taking place there, which subject it to constant change.[95] These activities generate a continuous mass of information, a veritable "information chaos",[96] that complicates

91. Interview with a high-ranking officer in the French Air and Space Force, November 29, 2023.
92. R. Leonhard, *Principles of War*, *op. cit.*, p. 183.
93. T. Lavernhe and F.-O. Corman, *Vaincre en mer*, *op. cit.*, p. 260.
94. E. Tenenbaum, "Le rôle stratégique des forces terrestres", *Focus stratégique*, No. 78, Ifri, February 2018.
95. "RFT 3.2.0 – Concept d'emploi des Forces terrestres", CDEC, 2021.
96. "Action terrestre future", *op. cit.*

interpretation of the operational environment. Land maneuver relies on the optimal exploitation of the terrain but must always be aware of the human environment in which it operates, which may represent an objective, a shield, or a constraint. Security depends on concealment and mobility, both of which are made more complex by the "viscosity" of the environment and its vulnerability to air and space, which facilitate the detection of variables in an essentially fixed environment.

The space domain has, until now, been seen as a factor amplifying the transparency of other environments thanks to its observation, communication, and geolocation capabilities. Its evolution toward an operational domain in its own right has necessitated the development of military space surveillance, which is currently the preserve of a few powers because of the technological complexity of means of surveillance. Although detection is accessible, precise identification remains extremely difficult, leading to ambiguity and uncertainty,[97] especially in more distant orbits. Advances in transparency technologies are making it harder to hide in the most opaque environments and forcing a rethink of maneuver in these environments in terms of how to maintain or recreate conditions of uncertainty.

Table 1-4: Characterization of natural environment

	Air environment	Sea environment (surface)	Underwater environment	Land environment	Space environment
Natural characteristics of the domain	Smooth", homogeneous environment	"Smooth", relatively homogeneous (other than the coast), fluid, hostile environment	"Smooth", homogeneous, and fluid environment	"Solid", heterogeneous, coarse, and viscous environment	"Smooth", homogeneous, and deterministic environment
Density	Very low to zero	Low, except the coast	Average to low	High	Low to average
Depth / extension	Almost infinite	Finite but vast 3D interface	Finite but vast and multidimensional	Finite and very compartmentalized	Infinite
Detectability of physical phenomena	Very good in all spectra depending on weather	EM: good Optical/sound: very poor	Optical/EM: very poor Sound: very good but complex	Average to poor in all spectra, very restricted Very high within a close detection range	Optical/EM: Excellent
Obstacles	Weather Topography	Weather Coastal zones Maritime activity	Seabed Bathythermy Bathymetry	Topography Vegetation Urbanization Human activity	Detection distance
Densité of human activity	Very low (discontinuous activity) Easy target discrimination	Very low to very high (coasts, shipping lanes, choke points) Difficult target discrimination	Almost zero Easy target discrimination (if detected)	High to very high Permanent and essential occupation of space Complicated target discrimination	Zero to high Complicated target discrimination (nature and purpose)

Source: C. Paulin, M. Asencio et al., "Vers une vision réaliste des opérations en reseau", Recherche et Documents, No. 2, 2009, Fondation pour la recherche stratégique.

97. M. Friedling, "L'Espace : un enjeu stratégique et un nouveau champ de confrontation militaire", *Revue Défense Nationale*, 2019, pp. 67–73.

Table 1-5: Characterization of combat domains

	Air Domain	Sea domain (surface)	Underwater domain	Land domain	Space domain
Military mobility **Speed in the domain**	Very high Speed and surprise	High Maneuverability	Very high Ubiquity	Low and very restricted Stability	High but restricted
Characteristics of military presence	Low density Highly dispersed Limited and discontinuous presence	Low density Highly dispersed Sustained but limited presence	Very low density Extremely dispersed Sustained presence	High density Not very dispersed Permanent presence	Low density Almost permanent presence
Integration in the domain	Transit	Control	Dilution	Occupation	Transit
Ability to represent the operational environment (situation awareness)	Comprehensive view Rapid acquisition Dynamic representation	360° comprehensive view on the surface Dynamic representation	Restricted view	Fragmented, patchy view Distortion of view depending on level Static representation	Comprehensive view reliant on means of observation Representation via catalogue
Theoretical "transparency" of the domain	**Transparent**	**Mostly transparent**	**Opaque**	**Rather opaque**	**Transparent**

Source : C. Paulin, M. Asencio et al., "Vers une vision réaliste des opérations en reseau".

The dialectic of transparency and opacity in terms of technological capabilities

Transparency is often seen as a fundamental characteristic of the operational art of the twenty-first century and as unavoidable due to technical progress in sensors, the most widely reported being drones. This view is mostly accurate but needs to be put in perspective. Objective consideration of the transparency-opacity relationship in terms of technological capabilities is essential for getting a precise picture of its development and potential limits in each of its two major strands: data collection (physical field) and data processing (cognitive field).

Spectacular improvements in sensors, major progress in analytical capabilities

The all-round development of drones

The last twenty years have seen exponential progress in technical intelligence gathering capabilities, particularly in drones. Now that this term has become so generic, we ought to examine the variety of functions it encompasses. The modern battlefield features surveillance drones at the tactical level (from nano or mini drones to the Safran Patroller) as well as at the operative or strategic level, with MALE (medium-altitude long-endurance) drones like the MQ-9 Reaper or HALE (high-altitude long-endurance) drones like the RQ-4 Global Hawk.

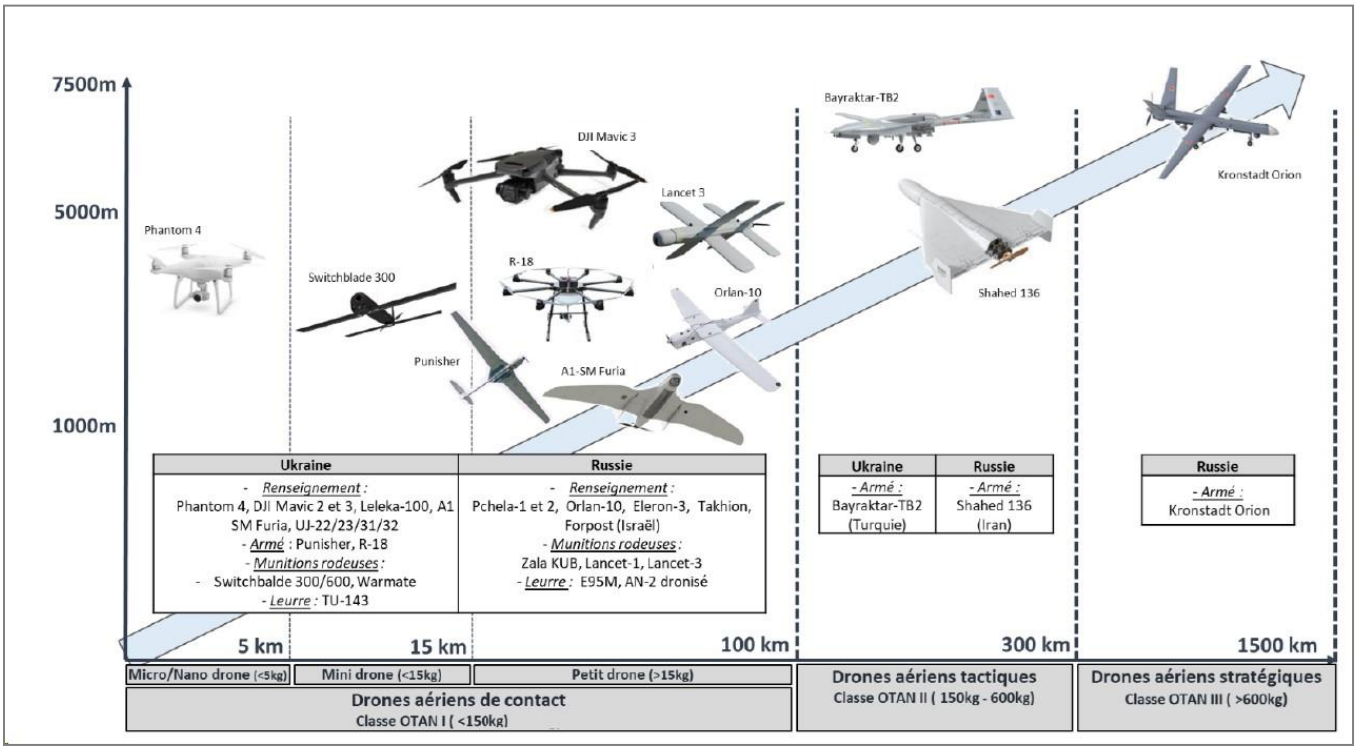
Drones all across this broad spectrum have improved rapidly in terms of range, endurance, connectivity, and payload. Their on-board equipment boasts constantly improving target discrimination capabilities, particularly when it comes to resolution. A single “ultisensory” drone can be equipped with multiple devices (optronic or electromagnetic sensors, etc.). In a manner of speaking, a sophisticated drone single-handedly provides multisource intelligence. For example, the RQ-4 has a maximum endurance of 24 to 36 hours, a range of over 22,000 km, and can carry a total payload of 1,360 kg split between various sensors (high-resolution electro-optical, infrared, synthetic aperture radar [SAR]/moving target indication [MTI]).

Drones act like an "aerial occupying force"[98]: their sheer numbers guarantee almost continuous surveillance.

Besides surveillance drones, the drone spectrum also includes loitering munitions. These can now combine detection and strike functions, as seen in the recent Nagorno-Karabakh War and the Russo-Ukrainian War. One-way loitering munitions[99] attack their target as soon as it is detected. They should be distinguished from combat drones, which jettison their munitions and are designed to be reused. The war in Ukraine has seen the proliferation of microdrones of varying technological complexity, both one-way and reusable, that are available at the lowest tactical levels (combat platoons). They have two principal functions: to improve understanding of units' tactical situation; and to shorten and refine the detection-strike loop for artillery fires. Numerous civilian drones, of a lower quality than current military drones, can be added to the existing inventory during conflicts and contribute, in their own way, to transparency. Their attrition rates are high, but they are easily replaced and can exploit an agile ecosystem (reactive adjustments on the ground, startups and innovative industrial small and medium-sized enterprises [SMEs][100]). To address the vulnerability of drones in high-intensity contexts, long-term programs are underway to devise hypersonic drones (Lockheed Martin SR-72)[101] or stealth drones (Northrop Grumman RQ-180).[102]

98. J.-C. Noël, "Occuper sans envahir, drones aériens et stratégie", *Politique étrangère*, Vol. 78, No. 3, Ifri, September 2013, pp. 105–117.
99. Also known as suicide drones, kamikaze drones, or exploding drones.
100. For example, in France: Parrot, Delair, Drone XTR, Drone Volt, Elistair, Novadem, etc.
101. Mach 6 speed.
102. Also in this category is Boeing Australia's MQ-28 Ghost Bat, although it is primarily a multirole drone. See T. Fouillet (ed.), *La Guerre au XXIe siècle. Le retour de la bataille*, Paris: Éditions du Rocher, 2023, p. 277.

Diagram II-1: Classification of drone systems and use in the Russo-Ukrainian conflict



Source: A. Cervera and O. Entraygues, Russie-Ukraine: Dix-huit mois de guerre totale, CDEC, September 18, 2023.

Outside the air-land domain, progress in drones has also been seen in the sea domain.[103] The RQ-4 has a maritime counterpart, the MQ-4C Triton. The reconnaissance UAV Camcopter S-100 can be launched from a naval platform.[104] Some countries, like Turkey, are considering a drone carrier program to replace aircraft carriers.[105] The Blackwing, an American project, is a multi-environment drone that can be launched from a submarine and carry out surveillance missions in the air. Underwater drones (UUV)[106] are also seeing rapid progress, as are highly autonomous and discreet underwater gliders.

In conclusion, the capability development of all kinds of drones, whether aerial or naval, is creating a kind of "surveillance continuum" that facilitates detection in all environments and at all levels.

103. See L. Péria-Peigné, "La dronisation navale, une opportunité pour la Marine nationale de 2030?", *Briefings de l'Ifri*, Ifri, August 25, 2022.
104. Tested on Mistral-class helicopter carriers. The Camcopter is slated to be replaced by the SDAM (système de drone aérien pour la Marine, naval aerial drone system).
105. Y. Smaldore, "Drones, VTOL, convertibles: quel avenir pour les aéronavales embarquées?", *Deftech,* August 2023.
106. Unmanned underwater vehicles.

Other means of surveillance: Redundancy and continuity

Other means of surveillance or detection, starting with radar, have experienced technical progress as well. Airborne early warning (AEW) platforms have seen constant improvements to their sensors (range, resolution, target discrimination, simultaneous processing capacity, resilience, etc.), as have reconnaissance pods (like the TR Pod for the Rafale F5, which combines current Reco-NG pods with TALIOS pods).[107] As well as radars on board air or naval platforms, ground-based radars are also being continuously refined, with progress hinting at possible breakthroughs in passive, over-the-horizon, and low-frequency radar,[108] or even future radars incorporating quantum technology. The latter offers unmatched computing power and could call into question the stealth of weapons delivery systems, among other conceivable use cases.[109] Radar performance will also be enhanced by AI.

Far above the classic aerial battlefield, HAPS (high-altitude pseudo-satellites) operate at the edge of the stratosphere.[110] They offer months, rather than hours of surveillance time. These large, highly energy-efficient machines, like Thales Alenia Space's Stratobus airship project (250 kg payload)[111] or Hemeria's more recent BalMan maneuvering stratospheric balloon, could be assigned observation, COMINT, or SIGINT missions for military, environmental, or scientific purposes. Their image resolution is better than that of satellites because of their greater proximity to the ground or ocean surface.

In the future, these weapons delivery systems, drones, aircraft, or HAPS could be equipped with hyperspectral imaging sensors. This developing technology can capture numerous (several hundred) very narrow spectral bands,[112] massively expanding the possible field of analysis. It could enable the precise detection of underground tunnels, among other uses, although interpretation techniques remain complex.[113]

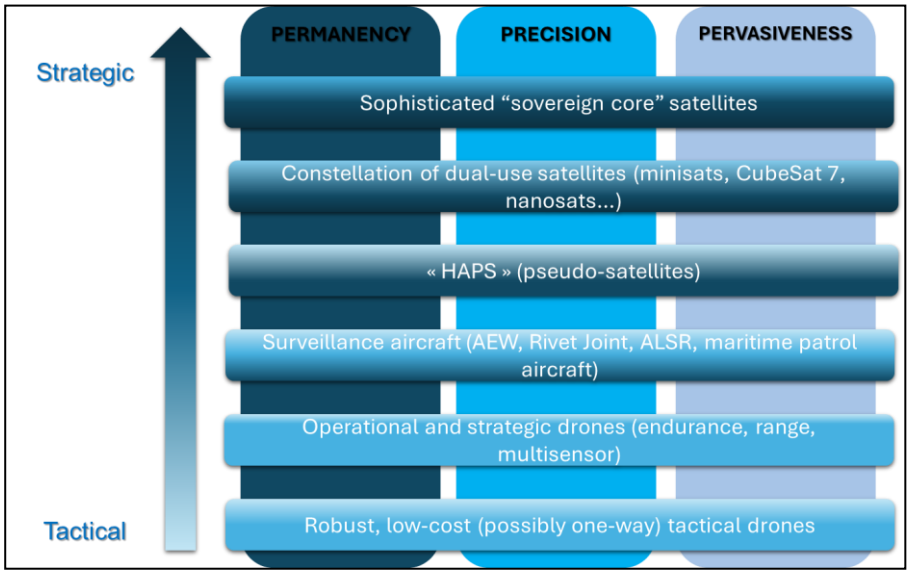
Satellites, which are essentially strategic instruments, have also seen fast-paced development, beginning earlier than that of drones but still increasing in recent years thanks to progress in civilian uses, particularly in

107. L. Lagneau, "Le *Rafale* F5 sera équipé du 'POD TR', qui fusionnera les capacités des nacelles TALIOS et RECO NG", *OPEX360*, June 2023.
108. M.-A. Eva, "Vitesse, furtivité: la quête de survivabilité", *Revue Défense Nationale*, No. 809, April 2018, pp. 78–82.
109. E. Hardy, "La stratégie militaire et le champ opérationnel des compétitions technologiques", *Revue Défense Nationale*, HS No. 4, 2021, pp. 214–226.
110. In terms of sovereignty, anything beyond the stratosphere is legally a "commons".
111. M. Cabirol, "Thales Alenia Space: si, si le projet de dirigeable stratosphérique Stratobus respire encore", *La Tribune*, September 2022.
112. Conventional imaging perceives three bands (red, green, blue, or in other words what the human eye sees). Multispectral imaging analyzes around half a dozen others as well.
113. But AI could certainly facilitate this work.

the NewSpace sector. Advances in the most sophisticated "sovereign core"[114] satellites are undeniably increasing transparency for observations (optical or radar imaging) as well as COMINT, telecommunications (range and bandwidth), or geolocation and GPS-guided munitions. Technical improvements are constant: panchromatic resolution, higher revisit rates (frequency of image updates), or increased resilience (new, more robust countermeasures), to mention only the most important parameters.[115]

In parallel, the last five to ten years have seen astonishing advances in the civilian space sector, most of which also have uses in the military sector. Constellations of mini or nanosatellites, from tens to hundreds of objects the size of a shoebox, are already in space. The Ukrainian army's use of SpaceX's Starlink network (as many as 42,000 satellites planned[116]) has been amply discussed and serves as a reminder that these constellations, resilient thanks to their redundancy, can complement the "sovereign core" in the event of conflict, or even replace it if necessary due to attrition. This is true of all the sectors mentioned above (observations, communications, datalink). As another example, the French startup Unseenlabs offers a constellation of nanosatellites that can geolocate ships by detecting their passive electromagnetic emissions, increasing transparency in the sea domain.[117]

Diagram II-2: The permanency and ubiquity of air and space surveillance



© Guillaume Garnier/Ifri, 2024.

114. France's thirteen existing military satellites. See X. Pasco and P. Wohrer, "La mise en œuvre de la Stratégie spatiale de défense française: vers la maîtrise de l'espace?", *Note de la FRS*, No. 12, Fondation pour la recherche stratégique, April 2023.
115. See "Rapport d'information no 506 (2019-2020)", Délégation parlementaire au renseignement, June 2020, pp. 199–212.
116. M. Borowitz, "The Military Use of Small Satellites in Orbit", *Briefings de l'Ifri*, Ifri, March 4, 2022.
117. J. Bachelier and P. Boulanger, "La 'fusion de l'information': levier de la puissance maritime française?", *Briefings de l'Ifri*, Ifri, December 7, 2023.

The democratization of access to transparency

As well as sovereign military resources, transparency can also be based on a plethora of civilian resources, including satellites and drones[118] (see above), 4G/5G network antennae, connected objects, etc., so that it seems to be inescapable. Although these objects are much less protected or sophisticated than their military counterparts, their sheer numbers make them almost inexhaustible, and the associated network of startups is evolving so quickly that it seems likely to always be able to offer a suitable solution for the provision of transparency-related services in the event of transparency being reduced.

This democratization of access to transparency is also reflected in open-source intelligence (OSINT). This is not a new development[119]: OSINT has long been as a major source of intelligence.[120] Again, the Russo-Ukrainian conflict has served to reveal and accelerate progress. Civilian analysts, often organized into communities of "osinters",[121] can monitor tactical actions with a level of granularity that was previously impossible. Social networks help to amplify their findings. A website like oryxspioenkop.com can document Russian material losses supported by evidence. Another website, understandingwar.org, publishes location maps and operational assessments that resemble defense staff work.

On the ground, combatants use applications from the civilian sector. For example, the Ukrainians use the "Diia" mobile app, which itself hosts the "Delta" app enabling the real-time exchange of tactical data.[122] They also have access to a dozen other pieces of software, including MilChat (secure messaging) or MyGun (ballistic calculator). Data can be georeferenced and time-stamped, shortening the targeting loop and making it easier to destroy enemy units. Smartphones have become an essential tool on the battlefield, perfect as both weapon and target. This democratization of access to transparency could obviously be an advantage to non-state actors, enabling them to carry out combat actions without the dedicated support of conventional military means[123]: transparency thus also plays into the hands of non-state adversaries who are capable of reactive adaptation.[124]

118. P. Cheminade, "Quand les militaires draguent les drones civils", *La Tribune*, October 2023.
119. Henrotin, "Les mutations du renseignement militaire".
120. See issue No. 186 of *Hérodote*, "OSINT: Enquêtes et terrains numériques", 3rd quarter, 2022.
121. See the hearings of the Commission de la défense nationale et des forces armées: "Enjeux, à travers l'exemple ukrainien, du renseignement d'origine sources ouvertes (OSINT)", November 23, 2022.
122. General J. M. Wasielewski, "L'emploi de la cyber-électronique en Ukraine", *Revue Défense Nationale*, No. 859, April 2023.
123. See J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris: Nuvis, 2014.
124. K. Crombe and J. Nagl, "A Call to Action: Lessons from Ukraine for the Future Force", *Parameters*, Vol. 53, No. 3, Autumn 2023.

To conclude this discussion of information gathering, it is worth noting that all the phenomena described (drones, satellites, OSINT, etc.) seem to be self-sustaining and self-maintaining. Satellites appear to be at the heart of this "intelligence-gathering system-of-systems", if only because of the connectivity they provide to both sensors and effectors. Nevertheless, the quality of intelligence gathering is only decisive if the information transmitted is properly exploited.

From physical transparency to cognitive transparency

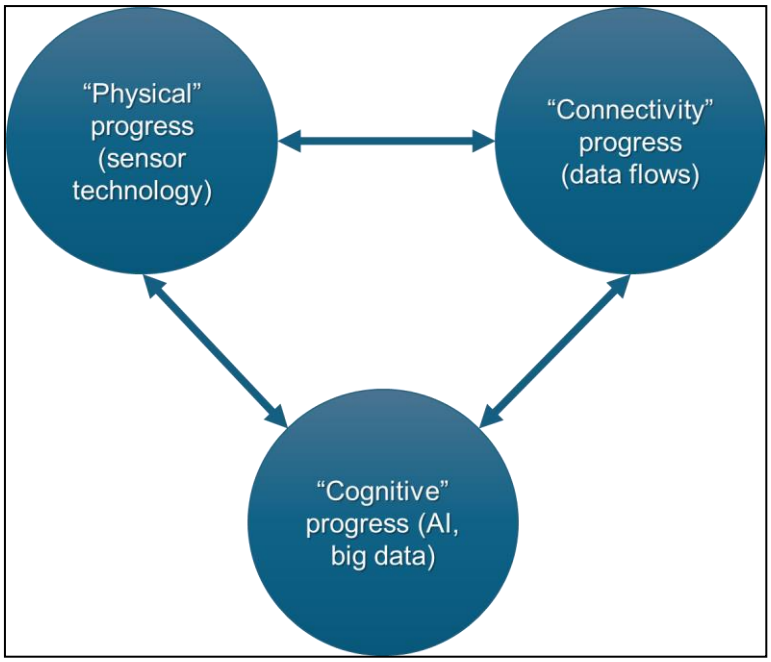
Of the five phases in the intelligence cycle,[125] the exploitation phase, essentially cognitive, is central to the provision of effective intelligence support. Here again, technical progress is impressive, particularly thanks to artificial intelligence.

Although there is a limit to the amount of information human analysts can exploit, they can now deploy a range of software tools to assist them. AI can help to extract the most relevant information from mass data by optimizing the indexing and selection of data (data mining). This allows analysts to concentrate on more complex aspects that require judgment, general knowledge, or a combination of multidisciplinary, specialized skills. For example, target dossiers that model the pattern of life[126] of terrorist groups based on a variety of statistics can be partly produced with AI assistance: the algorithm deals with the lower end of the cognitive scale, while human operators focus on more complex aspects of analysis. Experience so far shows that AI is particularly good at analyzing (or pre-analyzing) imagery data and acoustic data/signals. This allows analysts and their organizations to work more quickly and effectively by focusing on high-added value tasks.

Defense staff processes can be refined so as to derive maximum benefit from these advances. Geospatial intelligence (GEOINT),[127] which is both a capability and a collaborative work technique, aggregates multidisciplinary (multilayer and ultisensory) and georeferenced data. The fusion of data from various superimposed layers of analysis enables highly sophisticated exploitation.

125. Direction, Collection, Processing, Analysis and production, Dissemination.
126. Study of the habits or social organization of a given group, generally for targeting purposes.
127. J. Bachelier and P. Boulanger, "La 'fusion de l'information'", *op. cit.*

Diagram II-3: Cumulative progress in transparency



© Guillaume Garnier/Ifri, 2024.

Tricking transparency: The wide spectrum of deception

While technologies and tools that increase transparency have developed at an unprecedented rate, giving the impression of ubiquitous and continuous intelligence gathering, it is important not to underestimate the progress being made, albeit less rapidly, in measures to combat transparency. These measures can be divided into three families of technological capability: concealment, transformation, and disruption. And there is always also the option of destroying the means of transparency.

Distorted intelligence gathering

More effective concealment

Concealment relies equally on collective expertise and technological advances that make it possible to become invisible, at least partially. This increases the probability of survival.

In terms of technology, new forms of camouflage are appearing, although at different levels of technical maturity. There are several such initiatives in France. They include, in the land domain, the "bariolage multi-environnement" (BME) for combatants, a camouflage uniform suitable for use in different environments. The BME is designed to be a trompe l'oeil

and is expected to increase detection time by 25%.[128] Nevertheless, it is seen as no more than a precursor to a future combat uniform made of intelligent textiles that automatically adapt to the surrounding environment, like a chameleon. The CAMTAC (tactical camouflage) system, meanwhile, contains a set of stickers that can be affixed to a vehicle to conceal its shape and delay detection.[129] Even more effective camouflage will seek to hinder the detection of multiple signatures: visual, of course, but also thermal (infrared frequency range) and even radar, in order to deceive various types of sensor. This is the goal of Saab's Barracuda MCS multispectral camouflage system, which consists of a net that covers a vehicle. Taking another approach, the concealment potential of smoke bombs can be significantly improved[130] and could even absorb or deflect lasers.[131] Finally, the acoustic signature of vehicles can be lessened by using more discreet engines (hybrid or electric).

In the more fluid air and sea domains, progress in concealment relies essentially on stealth, thanks to technologies using radar-absorbent materials (RAM) that reduce the radar echo reflected by platforms and alter their perceived shape. La Fayette-class frigates, designed to reduce the radar cross section (RCS), were a precursor to this technology in the naval domain more than thirty years ago. The F-35 is now its most iconic example in the air domain. Again, it is more about hampering or delaying detection than producing a perfect "invisibility cloak". In the underwater domain, anechoic coverings reduce or distort reflected sonar waves and muffle the submarine's sounds.

Transforming in order to deceive

More subtle than pure concealment, modification of one's appearance can make it possible not just to hide, but also to trick the enemy. In the land domain, the Direction générale de l'Armement (DGA) has for several years been coordinating the Caméleon-Salamandre project to give vehicles cryptic camouflage.[132] The project aims to change vehicles' appearance using an intelligent system of pixelated screens managed by an AI algorithm that can give them a different signature. BAE's ADAPTIV system has already implemented this type of principle, but with a limited range of infrared signatures. It uses a covering of heat-reactive plates that can be modified by

128. N. Gain, "Vers un 'bariolage multi-environnement' unique pour les armées françaises", *FOB*, May 2022.
129. N. Gain, "Eurosatory 2022: l'armée de Terre veut 'passer à l'échelle' sur le futur camouflage de ses véhicules", *FOB*, June 2022.
130. R. Hémez, "Derrière un écran de fumée. Perspectives sur l'emploi des fumigènes dans la manœuvre terrestre", *DSI*, No. 168, December 2023.
131. R. Hémez, "Opérations de déception. Repenser la ruse au 21e siècle", *Focus stratégique*, No. 81, Ifri, June 2018, p. 46.
132. In the animal or plant world, camouflage is described as "cryptic" when it enables an organism to blend in with its natural surroundings. For a military application, see L. Lagneau, "Révolutionnaire: le 'camouflage adaptatif en milieu terrestre' pourrait être prêt en 2025", *OPEX360*, November 2021.

the on-board computer: a tank observed through a thermal camera is thus transformed into a simple car. Simpler and more economical, decoys can simulate the presence of non-existent equipment. The CAESAR self-propelled howitzer now comes in an inflatable version, produced by the Czech firm Inflatech,[133] which can reproduce the original's thermal signature and imitate its radar cross section. This combination of tricks makes the illusion much more convincing.

Deception capabilities in air combat have been the focus of recent efforts. Uncrewed decoys are already available, like Raytheon's ADM-160 MALD (miniature air-launched decoy), which duplicates the signature and flight profile of a combat aircraft to trick air defense systems into revealing themselves and making them easier to destroy for the "real" fighter planes, located further away on a SEAD (suppression of enemy air defenses) mission. The jamming variant of the MALD can then complete the action. The desire to refine this system is behind plans to develop future combat aviation standards, with a more integrated distribution of tasks between the aircraft and its loyal wingmen thanks to a shared digital architecture. These wingmen can test the ground-air defense network (decoys), saturate it (swarms coordinated by AI),[134] disrupt it (jamming), and commence attrition (air-ground fires). This would at the very least reduce the transparency of the defense system, and at best render it inoperative. Crewed aircraft could then deliver the final blow.

Disrupting, impairing, or eliminating sensors

All sensors depend, in various ways, on the electromagnetic spectrum. By disrupting it, electromagnetic warfare (EW) can modify and even prevent the gathering of information. Jamming enemy equipment is effective as long as it does not also jam friendly systems, as the Ukrainian theater has shown. It is easier to jam more basic sensors, like low-cost drones.[135] Electronic deception techniques like spoofing (the emission of decoy signals indicating a false relative speed or location) can be used.[136] As well as information gathering devices, the whole system-of-systems that enables transparency can also be disrupted[137]: sensors, CPs where information is received and fused, and effectors. Datalink backup is essential and highlights the need to dominate the electromagnetic spectrum in order to

133. N. Gain, "Faux CAESAR et autres idées pour doter l'épée d'un bouclier", *FOB*, December 2023.
134. This kind of swarm flight has already been tested, for example swarms of X-61 Gremlins.
135. "[Russian] anti-drone systems like the Shipovnik-Aero are responsible for shooting down more than 50% of the 10,000 Ukrainian drones destroyed each month", in: J. Henrotin, "La loi de programmation militaire face aux leçons de la guerre en Ukraine", *DSI*, HS No. 191, August–September 2023.
136. P. Gros, "Les opérations en environnement électromagnétique dégradé", Note 357, Fondation pour la recherche stratégique, May 2018, pp. 10–11; P. Gros, "Navigation Warfare et positionnement, navigation, synchronisation (PNT)", Note 3, Report 193, Observatoire des conflits futurs, May 2022.
137. Particularly C4ISR nodes, which are needed for the system to function.

ensure the continued operation of the C4ISR chain (command, control, communications, computers, intelligence, surveillance, reconnaissance) in the three classic domains (land, air, sea), but even more importantly the integrity of the link between them and the space domain. Electromagnetic disruption can be supplemented by cyberattacks. Closely coordinated EW and cyber effects require "cyber-electronic" actions,[138] a nascent but promising field.

Other non-kinetic means can impair sensors, particularly optical sensors or antennae: directed-energy weapons (DEW). Lasers or microwave weapons are being refined with a view to destroying drones, whose tactical and psychological impact (the sense that nowhere is safe) has been demonstrated in the conflicts in Nagorno-Karabakh and Ukraine.

Several studies are currently being conducted in the field of anti-drone warfare (ADW) to determine the most cost-effective solution for coherently deploying these different means. The structure remains to be decided, with several conceivable combinations of electromagnetic pulse (EMP) weapons such as microwave cannons,[139] high-energy laser systems,[140] high-rate-of-fire anti-aircraft guns, including CIWS,[141] and anti-drone drones,[142] to name just a few. On a different scale, lasers and DEWs can be used against satellites (dazzling, overheating components, etc.).[143]

Current capabilities and technologies, as well as those in development or likely to be available in the short to medium term, thus encompass a wide variety of techniques to trick or at least reduce transparency by seeking to impact intelligence gathering. These efforts have a variety of more or less complex effects, ranging from concealment to decoy, or the disruption or elimination of sensors.

Flawed analysis

If the collection of information can be disrupted, so too can its processing, with the difference that in the latter case, the disruption can be self-inflicted or caused by the enemy.

138. O. Letertre, P. Justel, R. Lechâble, and S. Dossé, "Regards croisés sur la guerre électronique", *Focus stratégique*, No. 90, Ifri, July 2019.
139. Epirus Leonidas or THOR, see https://meta-defense.fr.
140. US trial of an armored Stryker equipped with a 50-kilowatt laser; see F. Wolf, "L'US Army percevra ses premiers DE-SHORAD laser Guardian cette année", *Meta Defense*, January 14, 2022. For a broader view of directed-energy weapons, see P. Gros, N. Vilboux, F. Coste, S. Delory, and 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, June 2019, pp. 26–32.
141. Close-in weapons system.
142. G. Powis, "Coyote, le drone américain spécialisé dans la destruction de drones", *Air&Cosmos*, November 2023.
143. T. Fouillet (ed.), *La Guerre au XXIe siècle*, *op. cit.*, p. 277.

The risk of overload

The conditions conducive to cognitive transparency generate their own drawbacks. Information overload, or infobesity, can saturate exploitation capacities, despite algorithms to improve the sorting and pre-analysis of the masses of incoming data. Analysis requires a crucial measure of discernment, currently still a human prerogative, in order to identify the essential and discard the incidental, to select weak but important signals without being distracted by "informational noise". Moreover, it is humans who feed AI with data, and our cognitive biases are partly incorporated into its algorithms.[144] Data exploitation software can also create a form of addiction. Analysts must be able to think for themselves, if only in case of the malfunction or denial of service of their cognitive tools. Finally, excess information can have a restrictive effect, inhibiting analysts who always want "more information" before sending it to decision-makers, or making the latter incapable of deciding because they are waiting for "the final piece of data" to clear up a doubt.[145] The acquisition of information follows a vicious circle where more information is always needed to clarify existing information.

The fact that Hamas's attack on October 7, 2023, was able to take the Israeli security apparatus by surprise exemplifies the phenomena discussed above. With an intelligence apparatus that is considered to be among the best in the world, Israel has a reputation as a particularly innovative "startup nation", including in the field of AI. Hamas, its long-standing adversary, is concentrated in a tiny geographical area, the Gaza Strip, which is by nature easy to monitor. Although a few analysts issued warnings based on the conjunction of several lines of evidence, their concerns were ignored,[146] lost in the flood of hypotheses and undermined by various cognitive biases, which were exacerbated by Hamas's rigorous OPSEC (operations security)[147] measures. It is possible to draw certain similarities between this situation and the attacks of September 11, 2001.[148]

The golden age of manipulation

Other than these internal errors of interpretation, analysis can be impaired as a result of deliberate action by the enemy, particularly cyberattacks. Data can be corrupted,[149] skewing the AI algorithm without the analyst's knowledge. It is thus in the interest of analysts to maintain the necessary

144. J.-C. Noël, "Comment l'intelligence artificielle va transformer la guerre", *Éditoriaux de l'Ifri*, Ifri, November 5, 2018.
145. General M. Yakovleff, hearings of the Commission de la défense nationale.
146. "Selon le *New York Times*, Israël avait eu vent des plans du Hamas", *Le Figaro*, December 1, 2023.
147. "Operations security": the capacity to operate clandestinely and maintain secrecy.
148. E. Harding, "How Could Israeli Intelligence Miss the Hamas Invasion Plans?", *CSIS*, October 2023.
149. C. Bômont, "Le *cloud* défense: défi opérationnel, impératif stratégique et enjeu de souveraineté", *Focus stratégique*, No. 107, Ifri, November 2021, p. 37.

distance from findings. Nevertheless, "data poisoning" remains difficult to accomplish in a secure network. An easier option is a denial-of-service attack, which prevents access to data.[150] The enemy can also introduce spyware that does not disrupt the analysts' work but shifts the balance of transparency in the enemy's favor.

New technologies in the information sphere can now target not analysts, but decision-makers, or better still, public opinion, the unity of which is essential at the strategic level. The "post-truth era" is fueled by the technical possibilities for fake news or disinformation, for example using deepfakes or more generally via social networks ("influencers" directed by rogue states, trolls, etc.). These manipulation processes are particularly effective in the current context, with societies in the grip of systematic doubt while also developing a "taste for conflicting narratives".[151] Media confusion around the strike on Al-Ahli Hospital in Gaza on October 17, 2023, illustrates some of these dangers. Immediately attributed to the Israel Defense Forces (IDF) by numerous press outlets, which had not cross-checked the information, the strike was met with outrage and the news went viral. Major doubts were subsequently cast over this attribution, however, and a rocket fired by Islamic Jihad was ultimately considered to be the most likely cause. The important thing here is that the careless dissemination of sensitive information presented an opportunity for the immediate political exploitation of emotions in order to obtain a strategic advantage[152] by discrediting the IDF. Because both sides in a conflict are always keen to skew the presentation of key information, it is difficult to interpret the facts clearly. This particularly affects public opinion, because people tend to only retain details that confirm their preconceptions.

This form of cognitive warfare, which seeks to influence the judgment of military actors, decision-makers, or public opinion, can thus significantly reduce battlefield transparency.

150. C. Bômont, "Le *cloud* défense", *op. cit.*, p. 37.
151. D. Pappalardo, "La guerre cognitive: agir sur le cerveau de l'adversaire", *Le Rubicon*, December 2021.
152. O. Ubertalli, "Hôpital de Gaza: anatomie d'un naufrage médiatique", *Le Point*, October 20, 2023. See also D. Leonhardt, "Revisiting the Gaza Hospital Explosion", *The New York Times*, November 3, 2023, www.nytimes.com.

A premium for transparency in the physical field, and a premium for opacity in the cognitive field

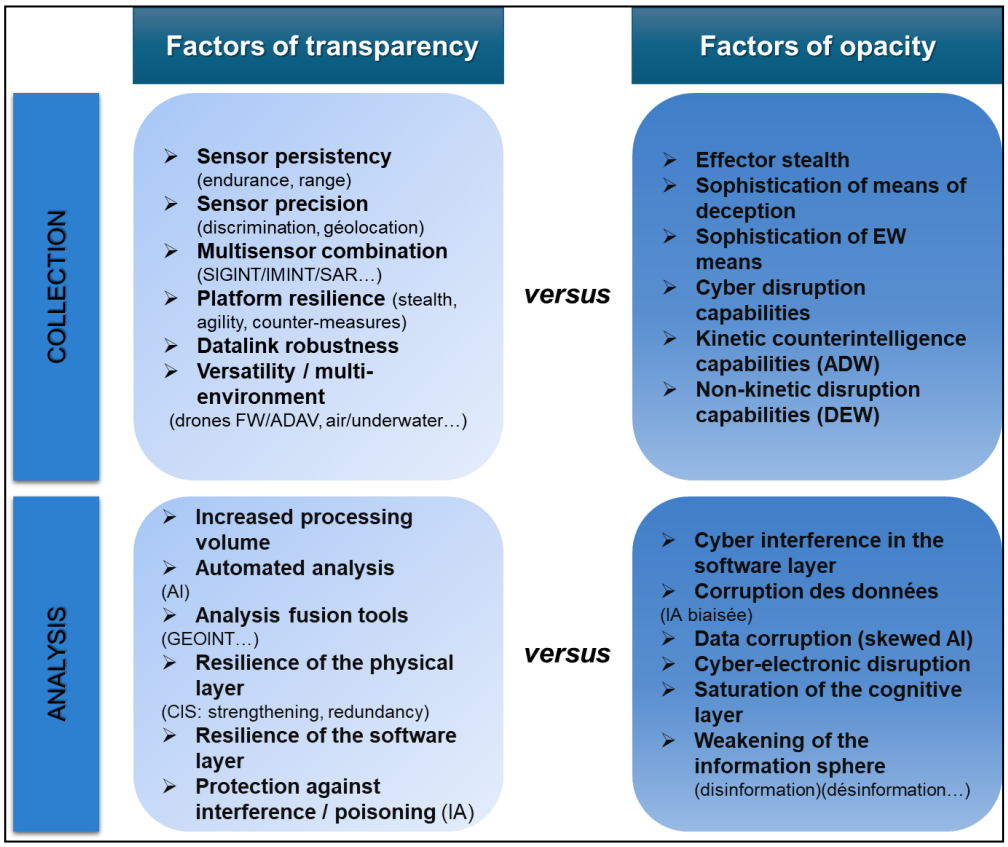
The convergence of three dialectics: Technological, tactical, and strategic

Our technological capability analysis of the relationship between transparency and opacity shows that there is a fundamental difference between what is classed as collection ("physical" criteria) and analysis ("cognitive" criteria). From the multiple interactions we have seen, we can deduce that there is currently a premium on transparency in the physical field (quality and redundancy of sensors) and a premium on opacity in the cognitive field (multiple forms of disinformation). How is this relationship likely to develop, given that it depends on fluctuating parameters?

The phenomenon of transparency is evolving, primarily due to technological advances. If technologies that increase transparency give too clear an advantage to one side, the other will respond by focusing on ways to block it. This prompts the first side to develop a counter-block,[153] and so on in an endless cycle. Luttwak describes this process clearly,[154] pointing out that it is rarely profitable to overinvest in a specific advantage because it will end up being counteracted. Reflecting on the transparency-opacity relationship means taking a very broad spectrum of technologies into account (see the table below for a simplified presentation of this dialectic). Many of these technologies are currently being researched by ecosystems of the most innovative SMEs, rendering any equilibrium achieved at a given moment subject to change. As a result, it is impossible to predict with any certainty how a particular element in this spectrum will evolve in the next five to ten years. The transparency-opacity relationship is therefore necessarily fluctuating, depending on investments by the major military powers and on technological breakthroughs, which by definition cannot be known in advance. A hypothetical high-intensity interstate conflict taking place five to ten years from now will probably not have the same transparency-opacity relationship as the Russo-Ukrainian conflict.

153. E. Hardy, "La stratégie militare", *op. cit.*
154. E. Luttwak, *Le Paradoxe de la stratégie*, Paris: Odile Jacob, 1989.

Diagram II-4: The transparency-opacity dialectic

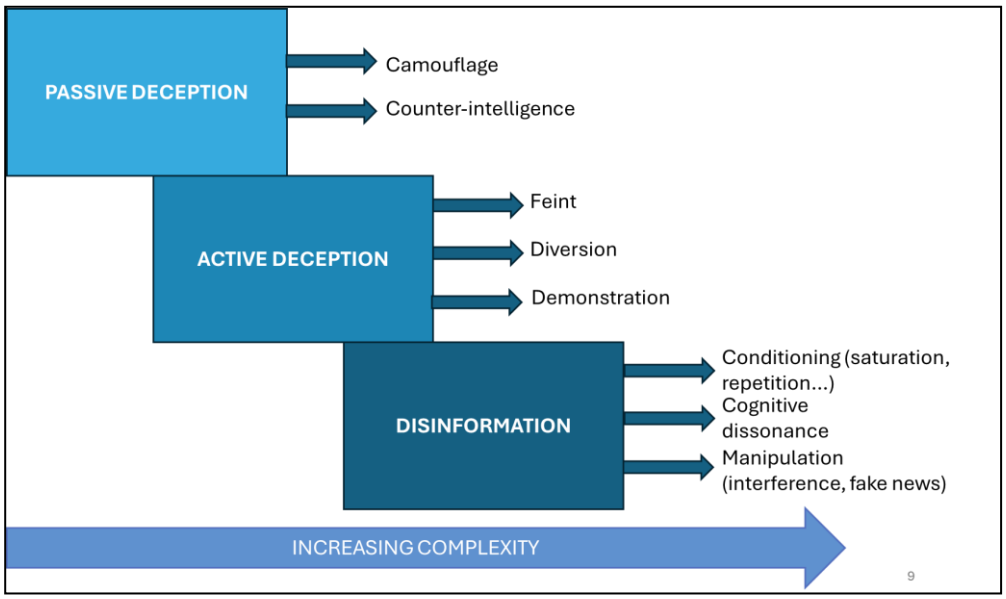


© Guillaume Garnier/Ifri, 2024.

Moreover, if transparency were to persist, along with its accompanying lethality, it would bring about, and is already bringing about, tactical adaptations. Rethinking deception seems crucial in this respect.[155] In 2024, the French Army completely rewrote its doctrine on deception to take account of increased battlefield transparency while paying greater attention to the range of psychological effects it produces despite, or sometimes thanks to, this heightened visibility. Remember that there are three modes of deception.

155. R. Hémez, "Opérations de déception. Repenser la ruse au 21e siècle".

Diagram II-5: The three modes of deception



© Guillaume Garnier/Ifri, 2024.

Its effectiveness is determined by the combination of all or some of these modes, a combination that must be rigorously planned and whose credibility depends on correct execution. The challenge now is to invent an art of subterfuge for the twenty-first century that makes use of available technologies and, above all, is based on careful operational preparation (doctrine, training). The aim is to be unpredictable, to instill permanent doubt in the enemy's mind in order to complicate their calculations, especially if they are aware of their adversary's tendency to use deception. As a result, any advantage gained in terms of transparency will be partly circumvented and will never be sufficient in itself to ensure a decisive result.

Finally, the transparency-opacity relationship changes depending on the strategic context. An "armed peace" situation will favor cognitive opacity: "hybrid" forms of aggression will rely on deception to create ambiguity (disinformation, problems of interpretation). This kind of context would place a premium on technologies that can surreptitiously neutralize or impair strategic equipment using non-lethal means (see section 4). By contrast, if a major conflict were to break out between superpowers, whether in Europe or in Asia, the belligerents would focus their efforts on other technologies in order to ensure operational superiority. This competition would give rise to a different transparency-opacity relationship that would also affect the powers "observing" the conflict.

The limits of transparency

As this comparison has shown, the transparency-opacity relationship seems likely to fluctuate over the coming years. The limits of battlefield transparency can be illustrated by four scenarios, presented in a graduated way, that cast doubt on its supposed omnipotence.

- **Scenario 1: "I can see everything, but I don't understand"**

In this first case, my erroneous interpretation of the enemy's intention is self-inflicted because of faulty analysis, itself caused by an excess of information, an inefficient decision-making process, or, more prosaically, a serious command error (cognitive bias, impaired judgment). Even the most cutting-edge twenty-first-century technologies cannot prevent this pitfall. Moreover, this scenario is the most prone to cause shock: excessive confidence in transparency, when let down by my own errors, is liable to provoke a moral crisis that can be difficult to overcome.

- **Scenario 2: "I can see the majority of the theater of confrontation, but I am missing key information"**

This also involves an error of interpretation, but this time caused by the enemy's use of the first ("passive") mode of deception: concealment. The enemy manages to conceal elements that are crucial to the implementation of its course of action and supplements this concealment with information saturation actions to prevent my intelligence apparatus detecting key indicators.

- **Scenario 3: "I think I can see and understand everything, but I have been given false information"**

This scenario is close to the second, but more developed. The enemy uses more subtle modes of deception. What is visible is false (active deception), and this deception is accompanied by skillfully orchestrated disinformation. As a result, my interpretation is incorrect. The shock that follows complete subterfuge also constitutes a moral challenge for the victim, potentially leading to cracks in cohesion (within the command, between the command and the intelligence apparatus, etc.).

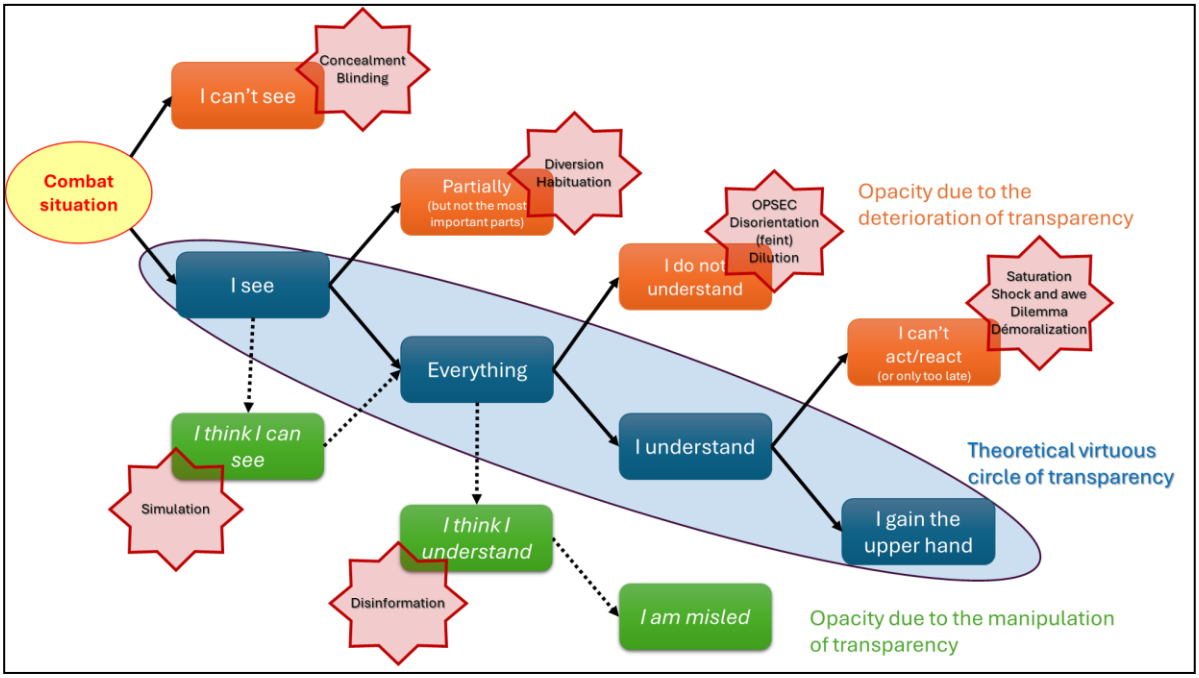
- **Scenario 4: "I can see everything, I interpret it correctly, but I cannot (re)act"**

Transparency has performed its task perfectly, and the operational situation has been correctly assessed. Nevertheless, capability efforts to ensure access to battlefield transparency have led to the neglect of other capability domains. Ultimately, I lack the means to (re)act and I remain a "spectator of transparency".

Another variant of the fourth scenario involves paralysis provoked by the enemy, whether by maneuvering too swiftly for me to do anything about it, or by neutralizing my nervous system at the decisive moment (strikes and cyberattacks), blinding me and impairing my C4ISR nodes.

The four scenarios presented above reveal numerous ways in which transparency can be circumvented or negated. Nevertheless, other than when the error is self-inflicted, they all require the enemy to have mastered complex skills. Competing against transparency demands the highest operational level, the most agile mind. The challenge should not be underestimated.

Diagram II-6: The malleability of the transparency-opacity relationship



© Pierre Néron-Bancel/Ifri, 2024.

In conclusion, this review of technological capabilities reveals the complexity of the interactions between transparency and opacity. While this relationship is more ambiguous than it might seem, it remains true that transparency is becoming a key factor on the battlefield. Beyond technological solutions to impair or deceive transparency, there are three different approaches for rethinking maneuver to take account of this new battlefield reality.

Fighting on a more transparent battlefield: A challenge but not an impossible task

Devising a military maneuver requires the ability to concentrate resources,[156] to take the enemy at least partly by surprise, and to conceal the operation's most indispensable elements: all things that seem difficult to accomplish in a context of transparency.

A number of conditions must be met in order to regain liberty of action despite all this. A new way of thinking about maneuver must focus first on security, if only to evade the detection/acquisition/destruction triptych. Achieving information superiority through multi-domain integration (known in France as M2MC, *multi-milieux/multi-champs*[157]), as planned by the French armed forces, is also necessary. The final requirement is the invention of new forms of surprise to thwart transparency. In other words, it is still possible to acquire operational superiority while being able to recreate uncertainty on a more transparent battlefield, but it demands great skill from the whole system of forces.

Disappearing from screens in order to survive: Reclaiming security

On the "zero line" of the Ukrainian front,[158] a vehicle's survivability is currently estimated at less than ten minutes.[159] The first challenge of engagement in a transparent environment is, therefore, to survive before even starting to fight. Applying the model of layers of survivability described above, recreating a form of opacity means first minimizing the detection surface and then minimizing the vulnerability of systems.

156. The "concentration of efforts" is one of Marshal Foch's three principles.
157. The M2MC concept reflects French doctrine's incorporation of various domains (land, air, sea, space, cyber) and fields (electromagnetic and information) and the need to integrate actions and effects in these different domains and fields when planning maneuvers.
158. The name given to the line of direct confrontation between the armies on the Ukrainian front. See B. Mabillard and S. Shestak, "Guerre en Ukraine: dans l'enfer de la ligne zéro", *Le Point*, February 7, 2024.
159. Y. Trofimov, "Drones Everywhere: How the Technological Revolution on Ukraine Battlefields Is Reshaping Modern Warfare", *The Wall Street Journal*, September 28, 2023.

Avoiding detection

Although it might seem impossible to avoid being seen in a combat environment increasingly saturated with all types of sensors, escaping the enemy's surveillance net remains possible as long as technological solutions are combined with a return to tactical fundamentals: concealment, dispersal, and discretion.

Beyond technological advances in camouflage, the concealment of positions and movements also requires an ability to exploit "the equalizing potential of difficult terrains".[160] In the land domain, naturally opaque zones like mountainous regions, dense forests, or urban areas all significantly reduce visibility and wave transmission. Particularly in urban areas, it is important to develop underground combat capabilities in order to exploit subterranean networks. Hamas's mastery of underground combat in Gaza suggests it would be sensible to expand training in urban underground combat capabilities, currently the preserve of units specializing in military search (engineering skills for the reconnaissance of confined environments), to the land forces in order to give them more in-depth knowledge of underground combat.[161] The use of ground robots in this "dangerous environment" could also be boosted by the momentum of the French Army's Vulcain program.[162] In the air combat domain, exploitation of the terrain translates into the all-weather low-altitude penetration capability, which requires operational expertise and terrain-monitoring technologies. Maintaining this rare, proven ability to evade enemy radars, and even extending it to the single-seater Rafales used by the Air and Space Force (AAE), would expand the air force's stealth and unpredictability options.[163]

Wider dispersal of forces is now possible thanks to the networking of combat units. Crucially, this enables the reduction of electromagnetic footprints, making it a viable solution for the survival of ground CPs, as well as for the air-sea forces, whose long-range effectors make concentration less necessary at the tactical level. The aim is not to become invisible, but merely to seem unimportant enough for the cost of a strike to be unjustifiable. Realistic technological solutions to support new, more dispersed CP arrangements are being developed and could limit the need to concentrate command functions in one place. For example, the use of virtual reality and holograms could cut down command and planning meetings. Access to "combat clouds" makes it possible to dissociate the

160. H. Delort-Laval, "Hommes et haute technologie dans les engagements terrestres: vers un mariage de raison?", *Inflexions*, Vol. 4, No. 3, 2006, pp. 113–124.
161. R. Franchet d'Esperey, "Combattre en milieu suburbain: la carte du génie", *Areion24.News*, October 28, 2023, www.areion24.news.
162. This program aims to devise principles for integrating robotics into ground combat between 2030 and 2040.
163. Interview on November 29, 2023.

planning and execution functions by setting up several light, forward CPs supported by a central "reachback"[164] CP. New waveforms, like laser satellite communication or Li-Fi (which transmits data via light) can also help to significantly reduce CPs' signature and logistical weight as well as speeding up information exchange. Wireless Li-Fi technology guarantees throughput of 2 Gbit/s up to a distance of 5 meters[165] and should streamline the deployment of CPs, given that a single division CP currently requires an 8-kilometer cable network.[166] The French Army is currently researching how to adapt the technology to its operational needs.

In the era of hyperconnectivity, discretion, the third skill needed to escape detection, relies primarily on adapting processes and behaviors so as to minimize digital footprints. At the individual level, this means safe and responsible digital behavior when using connected objects and social networks in order to avoid the "digitalization of the battlefield".[167] Collectively, the hybridization of networks and systems demands extra rigor around OPSEC procedures. Limiting vulnerability caused by the growing electromagnetic radiation emitted by units that are increasingly integrated into connectivity networks requires a shift toward a culture of digital frugality and careful attention to "the lessons of silence".[168] Learning how to extinguish one's electromagnetic signature while retaining the capability to command and control its effects is no simple task and even seems counterintuitive given that the information superiority of C2 systems depends on connectivity. As well as contributing to discretion, mastery of this skill helps build readiness to deal with enemy jamming attacks. EMCON (emissions control, measures to reduce electromagnetic footprints) training should be seen as an integral part of networked combat training, as in the French Navy's POLARIS exercises,[169] which include digital frugality training as one of their principal objectives.

The logic of frugality should also be applied to energy needs, with new, less bulky energy storage and generation solutions, as well as to human resources. In the ideal world, the future ground CP would exploit the advantages of connectivity to limit itself to a few hardened vehicles able to connect to each other multimodally and remain connected to command networks despite greater distances between them.[170] Work to develop new

164. The capacity to shift resources or capabilities to behind the zone of engagement, including into national territory.
165. "Le Li-Fi: une solution lumineuse pour les communications militaires?" *ITPublic*, consulted on February 15, 2024, www.itpublic.fr.
166. Interview with a senior officer in the French Army, December 12, 2023.
167. A. Cattaruzza and S. Taillat, "Les enjeux de la numérisation du champ de bataille", *op. cit.*, p. 13.
168. E. Lanquetot, "Le silence relatif", *op. cit.*
169. Large-scale joint forces, inter-allied exercise designed to prepare for a high-intensity naval engagement.
170. M. Beagle, J. Slider, and M. Arrol, "The Graveyard of Command Posts", *op. cit.*

very low-rate "stealth" waveforms could open up new horizons for CP systems in the longer term.[171]

Diagram III-1: Limiting the visibility of CP systems

		Vulnerabilities of current CPs						
		Multispectral radiation	Limites range	Surface area	Logistical weight	Inertia / deployment time	Energy needs	Complex connectivity
Possible solutions	Concealment	X	X	X				
	Dispersal	X	X	X	X			
	Modularity			X	X	X	X	X
	Reduction			X	X	X		
	Mobility	X	X	X		X		
	Frugality	X			X		X	
	New ways to store energy	X		X	X		X	
	New waveforms	X	X			X		X
	Hybrid CIS	X	X					X

© Pierre Néron-Bancel/Ifri, 2024.

Avoiding acquisition/destruction

Given time, however, detection is almost inevitable, making it essential to develop complementary solutions to maximize survivability by reducing the enemy's ability to exploit its intelligence. This second layer of security involves active and passive protection measures, mobility, and disruption of the enemy's connectivity loop.

The most obvious form of protection in the land domain is burial, as shown by the return of trenches on the Ukrainian front. The ability to dig and hide underground requires relearning forgotten skills and highlights the need for extensive engineering support, with resources adapted to the lethality of the front.[172] This makes it all the more important for the French Army to acquire a robust military engineering vehicle suitable for high-intensity combat. Use of the existing urban underground environment, such as underground parking lots, could offer protection for bulky objects like CPs. Protection also includes anything that can hamper sensors, starting with smoke munitions. To address the new threat posed by remotely controlled munitions and suicide drones, "soft-kill" solutions, like Lacroix Defense's Pronoïa system, are developing updated protection measures

171. Interview with officers in the French Defense Staff, December 8, 2023.
172. "Le combat de tranchée", *Légion étrangère*, consulted on February 15, 2024, www.legion-etrangere.com.

such as multispectral masking and jamming devices linked to on-board detection, analysis, and warning systems. Finally, the centrality of connectivity makes it essential to expand protection to networks and CIS. In that sense, the hybridization of CIS, enabling the exploitation of civilian 4G and 5G networks, could help to make communications more discreet and CP systems more resilient, although this type of solution requires good prior knowledge of civilian networks in the zone of engagement.[173]

Mobility, or speed in the air and sea domains, is an alternative to discretion and stealth when it comes to increasing survivability. It plays on temporality by reducing the "interval of intervisibility",[174] in other words the window in which the enemy's kill chain can acquire a target, and simultaneously delaying the enemy's understanding of friendly intentions. Speed is as integral to air maneuver, which is planned around the relationships between friendly speed, detection time, and enemy reaction speed, as to naval maneuver, which relies on acceleration to close the enemy's window of opportunity by moving out of detection range before the acquisition phase.

On the land battlefield, mobility, understood as the "capacity to maneuver during combat, over all types of terrain and despite enemy fires",[175] is restricted by the natural and artificial viscosity caused by the "disorganization of the terrain",[176] but also by internal frictions affecting the deployment and movement of a large unit like a division. By way of example, a Scorpion division comprises almost 10,000 vehicles,[177] which in the course of a maneuver must spread out, relieve each other, join forces, and overtake each other, all along a limited number of axes and potentially under fire. This kind of complex maneuvering in sight of the enemy makes a large unit's "movement support" function crucial for ensuring the fluidity of movements and maneuvers and the efficiency of flows, and for guiding units to their objectives despite obstacles and the inevitable friction of ground engagements.

In that sense, it would be useful to reestablish the role of movement support units, whose missions of circulation support, escorting, crossing support, intelligence, and unit relief support are absolutely essential to the engagement and to effective battlespace management of large land units in high-intensity contexts. Movement as an operational function should be

173. Interview on December 12, 2023.
174. F. Chamaud and 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", *op. cit.*

incorporated into the operational chain to support engagement in an integrated approach to maneuver.[178]

Finally, the disruption of enemy connectivity contributes to survivability by targeting critical nodes that provide access to the enemy's transparency apparatus. The aim is to render at least one of the enemy network's key functions inoperative in order to significantly impair the entire connectivity chain.[179] From this perspective, it seems increasingly necessary to acquire long-range offensive jamming capabilities in the land and air forces.[180] The challenge is to acquire jamming solutions that are both compatible with friendly emissions and as difficult as possible for the enemy's EW to detect. Cooperative jamming solutions, which allow jamming signals to be diverted to evade detection, could be deployed in the air and land domains, including by means of jamming drones.[181]

The deployment of cyber capabilities at the tactical level, or the use of cyber-tactical effects at the strategic level, will also be indispensable for impairing enemy networks and maintaining tactical superiority in the intangible domains. The physical destruction of sensors by targeting, the central pillar of SEAD, could usefully be applied in the land domain by reclaiming the concept of "counter-reconnaissance" maneuvers, which blind the enemy's intelligence system by targeting its sensors.[182] The deployment of anti-drone solutions in the land and naval forces is guided by this logic and is now becoming a major priority.

Survival on a transparent battlefield depends in part on certain capabilities or technologies, but is determined above all by meticulous, realistic operational preparation that takes into account the continuous visibility of forces. Training in transparent conditions seems to be particularly important for adapting behaviors and tactical procedures to this new combat reality.[183]

Winning the battle for information superiority

With the French armed forces committed to mastering M2MC integration, the exploitation and acceleration of connectivity loops are an essential way to gain information superiority. Like superiority in other domains, it can never be total or permanent, and it should be understood as a form of potential that the decision-maker chooses to realize at a given time and place with the aim of achieving a specific objective.

178. *Ibid.*
179. "Neutralisation des défenses aériennes ennemies", CEIA-3.6.4_SEAD, MINARM, 2022.
180. Interview on November 29, 2023.
181. R. Hémez, "Opérations de deception. Repenser la ruse au 21e siècle", *op. cit.*, p. 47.
182. M. Yakovleff, *Tactique théorique*, Paris: Economica, 2009, p. 357.
183. J. Watling and N. Reynolds, "Stormbreak", *op. cit.*, p. 23.

Can the promises of M2MC be met?

The M2MC doctrine envisions the implementation of a "multi-sensor/multi-effector network" (*réseau multi-senseurs multi-effecteurs*, RM2SE), understood as an "overall architecture of sensors and effectors connected by information and communications systems."[184] This networking is supposed to create a "hyper-superiority bubble",[185] both informational and kinetic, at a specific time and place. The equivalent US doctrine, Joint All-Domain Command and Control (JADC2), likewise aims to "optimize the availability and use of information to ensure that the commander's information and decision cycle operates faster relative to adversary abilities".[186] Nevertheless, this goal of multi-domain integration will require exceptional technological and organizational progress in terms of connectivity.

The first challenge is to build a network architecture that is interoperable between different tactical levels and across all domain components and accessible in varying degrees to allied forces. For the United States, this joint forces integration would require the networking of over thirty information systems and remains unattainable for the time being.[187] Interoperability between different systems also requires semantic and normative compatibility to connect systems of different generations and with different owners.[188] Both bottom-up adaptation, which gradually integrates existing systems as-is, including their limitations, and top-down design, which defines architecture standards in advance but requires a thorough overhaul of all systems, are possible but imperfect solutions. It will, therefore, probably be necessary to give up on the idea of "federated", "end-to-end" connectivity and instead focus initially on "vocational" loops, in other words loops that serve a single purpose (for example fires or surface-to-air defense). Finally, RM2SE interoperability must be compatible with confidentiality requirements, particularly when it comes to shared data, which means rethinking compartmentation and data access processes.[189]

Next, the transmission of data should meet the speed and throughput requirements of transparency while guaranteeing secure communications in a congested and contested electromagnetic field. Acquiring technical mastery of new waveforms to increase the data rate or remain under the EW detection threshold is particularly complex, as shown by the difficulty of developing software-defined radio solutions in France or the United

184. *Stratégie militaire générale*, EMA, September 2023, pp. 16–17.
185. *Ibid.*, pp. 16–17.
186. *Summary of the JADC2 Strategy*, *op. cit.*, p. 3.
187. Interview on December 8, 2023.
188. E. Faury, "Les opérations multidomaines: une révolution militaire", *Revue Défense Nationale*, "2020: chocs stratégiques - Regards du CHEM - 69e session", 2020.
189. *Ibid.*

States.[190] The hybridization of networks would enable both secure communications and throughput sharing, but the proliferation of different waveforms at a single emissions source jeopardizes electromagnetic coexistence because interference between waveforms neutralizes their effects.[191] The deployment of a satellite-based radio/communication system (SATCOM), like Starlink for the Ukrainian army, seems to be the best solution for meeting network resilience needs while ensuring a high data rate. Nevertheless, it depends on a secure, sovereign satellite network being provided by a dedicated, low-Earth orbit constellation.

Finally, data management itself represents a major challenge. The volume and constant flow of big data make it essential to autonomize data processing by integrating AI systems into the connectivity loop. To fully exploit the potential of M2MC integration, technical and organizational ways must be found to cope with the complexity of hyperconnectivity. In the short term, the focus should be on a restricted application of the RM2SE mesh in the form of spatially and temporally limited "transparency bubbles" created to achieve a desired effect in a specific use case. This would accomplish the aim of acquiring local "hyper-superiority". In this context, the integration of flows from drone-based sensors into fires management OICS like ATLAS[192] could constitute a first step toward M2MC.

Is military intelligence obsolete?

The immediacy of information, the demand for instantaneous processing, shared access to data, and the growing role of OSINT in understanding tactical situations are all drivers of transparency that challenge the traditional *modus operandi* of intelligence services. It is important, therefore, to identify the necessary steps for adapting intelligence to the reality of the contemporary battlefield while also reasserting the primacy of its core strength: analytical perspective.

The need for permanent, shared access to information, in line with civilian data-as-a-service models,[193] demands a cultural shift within the intelligence community toward the decompartmentalization of information and exploitation of the benefits of shared data. This means rethinking the production of intelligence with a view to open dissemination and inverting

190. See A. Hasday, "Intelligence artificielle dans l'armée: Sébastien Lecornu désavoue Thales et Sopra Steria", *L'Informé*, January 22, 2024, www.linforme.com; M. Sneps-Sneppe, D. Namiot, and E. Tikhonov, "On Software Defined Radio Issues", *2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW)*, Riga (Latvia), 2022, pp. 35–40.
191. Interview on December 8, 2023.
192. The ATLAS system (Automatisation des tirs et liaisons de l'artillerie sol/sol; automated fire control and ground-to-ground artillery links) is the ground-ground fire control software used by the French Army's artillery regiments.
193. A data service model guarantees optimized, anytime/anywhere availability of client data thanks to the internet and cloud techniques.

the logic of restriction, making confidentiality an exception rather than the default. This evolution is consistent with the M2MC doctrine's underlying goal of opening networks up to other branches of the armed forces, and even allies and partners.

The integration of civilian OSINT analysis could represent an opportunity for military intelligence. Although the use of open-source data has been integrated into intelligence jobs, online civilian "osinter" communities (like Oryx.com or Warspotting.com) constitute a still largely underexploited source of collective analytical power. The principal obstacle here has to do with security, with secrecy requirements ruling out any sharing of information with unauthorized people. This includes even the direction phase, which in itself can reveal much about intentions or vulnerabilities. The challenge is to match this rich, meticulous civilian work to military needs while recognizing that it will be extremely difficult to direct these civilian communities in line with the traditional logic of the intelligence loop, partly because of the profiles and motivations of their members, and partly for reasons of secrecy. One solution could be to develop a dedicated interface platform to act as an airlock between the two worlds and to make it possible to exploit the collective intelligence of these communities using a crowdfunding model.[194]

Transparency is increasingly understood as a means to increase enemy attrition by fires, an interpretation that has been strongly shaped by the influence of US doctrine on the procedures of the North Atlantic Treaty Organization (NATO). This bias has implications for military intelligence that must be remedied by recalling the essential role of analysis. Land maneuver now relies heavily on deep-targeting processes, which aim to "shape" the enemy by defining kill contracts that are used to plan the movements of sensors and effectors. This priority on forward actions alters the multidirectional dimension of intelligence by tilting the balance in favor of sensors in enemy territory. As a result, the logic of limited resources means that other dimensions (line of contact, flanks, rear, upstream intelligence) are less well served, which represents a first risk.

Another risk is the overshadowing of maneuver management by fires control, as seen for example in the place taken by the Joint Air Ground Integration Center (JAGIC) in division-level CP processes.[195] Prioritizing acceleration of the loop via the immediate exploitation of information risks losing knowledge capitalization capabilities that are vital in the long term. The technical solution for achieving a healthy balance between the constantly accelerating production of "actionable" intelligence and

194. "Enjeux, à travers l'exemple ukrainien, du renseignement d'origine sources ouvertes (OSINT)".
195. Interview on December 4, 2023.

"situational" intelligence[196] lies in the architecture of information systems, which must integrate both processes in parallel and allow a CP to handle the same information in parallel processes at different speeds.

Finally, the provisions on intelligence in France's two recent military programming laws (LPM) mask the fact that analysis has been overshadowed by the increasing importance of the technical management of digital data. It therefore seems necessary to make sure that investment in the digital development of intelligence does not lead to neglect of the need for skilled human resources in sufficient numbers to meet the demands of hyperconnectivity.[197]

Is the drone revolution passing us by?

The increasing role of drones in current conflicts highlights the challenges around integrating drones into the French armed forces and their capability development model. Although the French armed forces are adapting their thinking on drones in light of lessons learned in recent operations, two imperatives need to be considered: the all-encompassing nature of the drone segment and the integration of drones into existing command and control networks.

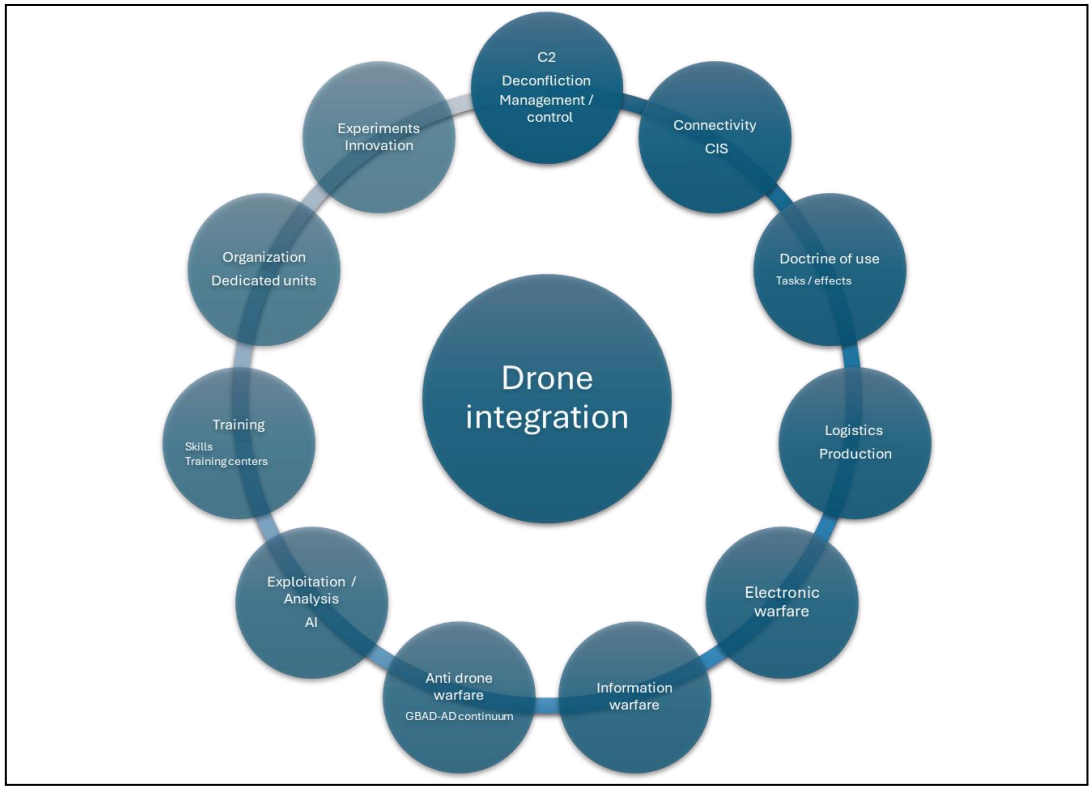
First, the addition of drones to combat architectures should be understood as a "holistic revolution"[198] that goes beyond simple maneuver support and has an impact on command structures and systems and on existing weapons systems. The drone segment cannot be developed without simultaneous reflection on anti-drone solutions and a dual doctrine that considers the use of drones alongside the threat they pose and how to combat it. Anti-drone combat itself should be understood, in terms of capabilities as well as use, as part of a continuum with the ground-based air defense (GBAD) and air defense (AD) layers. The speed with which electronic countermeasures are developed also makes it essential to rethink capability development cycles and bring them in line with the pace of technological innovation in drones and anti-drone defenses.[199] This comprehensive vision of drones as systems calls for the extensive integration of drones at all levels, using the principles of cumulative stacking and redundancy to cover the entire spectrum of drone use beyond reconnaissance alone.

196. "Actionable" intelligence aims to detect, locate, and identify targets, while "situational" intelligence aims to "describe the current situation at the strategic, operational, or tactical level" to support planning and operations management. See "Neutralisation des défenses aériennes ennemies", p. 42.
197. Interview on February 6, 2024.
198. H. Seydoux, "Microdrones: des innovations inattendues à la lumière du retour d'expérience ukrainien", *Revue Défense Nationale*, No. 865, December 2023, pp. 35–42.
199. Interview with a defense manufacturer, April 14, 2023.

Another prerequisite for drones to be effective is their integration into C2 networks. Drones can only fulfill their potential if employed in a closed loop, and they must be able to constantly share the information they collect with other actors in the network. Their use must also be coordinated with other capabilities, such as electronic warfare, which guarantees the necessary superiority prior to their deployment, or fires, which exploits information from drones in real time. Finally, beyond their contribution to information superiority, drones also cause a triple psychological effect of stupefaction, saturation, and surprise,[200] meaning their use must be integrated with maneuver at both a kinetic and informational level.

These two imperatives make the acquisition of expertise and procedures for using drones absolutely essential. They also suggest that tactical units should be immediately equipped with training drones, including civilian models, to practice using them without waiting for the completion of equipment programs currently in progress.[201]

Diagram III-2: Drone integration, a holistic approach



© Pierre Néron-Bancel/Ifri, 2024.

200. L. Lebailleur, "Réflexions prospectives sur l'emploi collaboratif de drones aériens et de l'aviation habitée dans les opérations aériennes militaires", BTEM dissertation, 2023.
201. T. Hacker, "How the US Army Can Close Its Dangerous – and Growing – Small Drone Gap", *Modern War Institute*, March 6, 2024, https://mwi.westpoint.edu.

Rethinking surprise: Inventing new forms of maneuver

Surprise thus remains possible despite battlefield transparency. The challenge now is how to reestablish, in practice, the conditions for achieving surprise during maneuvers in the face of the detection/acquisition/destruction triptych. Under certain strict conditions, this still seems possible, whether in a joint forces context or in each domain considered in isolation. Restoring surprise means reinstating the principle of uncertainty defined by Admiral Guy Labouérie, which consists of "permanent masking, including during action, so that the other side always remains uncertain about intentions, times, places, and means, and is thus unable to prepare".[202] This section suggests new operational forms of deception or agility, grouped into three broad categories, with no claim to exhaustiveness.

Creating windows of opacity

The key point here is to evade enemy observation, at least temporarily, and to significantly disrupt the enemy's understanding and thus their response. This is especially true for offensive maneuvers, where the surprise factor often determines the success or failure of the operation. The aim is to try, at a carefully chosen moment, to create the conditions for the enemy's "intoxication" by exploiting anything that might serve to obscure the battlefield. Several parameters must be combined to produce this effect. They include:

- finding a favorable weather window (poor conditions that reduce the accuracy of enemy sensors), preferably on a very dark night (level 5);
- initial tactical-operational blinding of sensors to at least reduce or delay, if not completely prevent detection;
- initial disruption of the enemy's C4ISR system, including CPs, to make it more difficult for the enemy to gain an overall understanding of the ongoing offensive maneuver;
- non-kinetic support for these blinding/disruption operations via cyber, EW, or combined cyber-electronic actions that seek to expand the area of opacity by exploiting all the deceptive techniques of EW[203];
- launching the decisive action with an offensive maneuver, ideally from an opaque environment (concealment of the initial attack); using stealthy offensive weapons delivery systems or modifying their signatures can also contribute to the creation of this haze.

202. G. Labouérie, "Des principes de la guerre", *Revue Défense Naionale*, No. 530, 1992.
203. Jamming, of course, but also the creation of false networks or interference. In short, any procedure that can create disruptive "electronic confusion" effects.

Coordinating all these actions will be complicated, but even when imperfect, this kind of sequence could catch out defensive systems that feel protected by a transparency in which they have complete trust.

This window of opacity could utilize the concept of "doctrinal surprise" by acting in a disruptive way that runs counter to our own doctrine, which the enemy will usually have studied.[204] Fighting in degraded mode, for example with all transmitters turned off, would make detection more difficult by substantially reducing one's electromagnetic signature. This type of approach requires mastery of old, seemingly outdated skills (no radio or GPS means using "route cards", infiltration corridors with destinations but no intermediate coordination points, etc.). This challenge must be addressed while also, in parallel, mastering skills in the most cutting-edge technologies. Moreover, degraded mode may be imposed (system failure, denial of service…) rather than deliberately chosen, making training in degraded mode indispensable. The French Navy is already well-practiced in this area,[205] having carried out a fictitious mission with no satellite link, showing that this kind of challenge can be overcome.

Lastly, while urban areas provide an excellent opaque environment for defense, they could also be exploited in attack. For example, instead of holding terrain in a linear way (continuous disposition of forces), one could solely occupy sufficiently large towns, some of which would turn out to be trigger points for an attack. In this scenario, everything would depend on the nature of the urban mesh over the zone of operation. Of course, there would be some gaps, but the tactical arrangement could resemble a succession of staggered squares as seen in the Napoleonic era, which allowed cavalry charges to pass through, and then, once the cavalry had been sufficiently weakened by crossfire, could adopt an offensive formation.[206] The uncertainty would come from the difficulty of understanding the stance of the various urban moles: offensive or defensive?

Creating new forms of mass

Mass is a quality that has been neglected by European forces for the last two or three decades. The partial dronization/robotization of the battlefield, which extends well beyond ISR (intelligence, surveillance, reconnaissance), is making it possible to reconsider new forms of active deception (simulation). To that end, mass, which at the tactical level helps to establish a favorable balance of power in the decisive area, could be understood differently. Drone swarms (here used in support, in other words as decoys

204. M. F. Cancian, "Inflicting Surprise: Gaining Competitive Advantage in Great Power Conflicts", *CSIS*, January 2021, pp. 43 and 57–58.
205. See R. Ruitenberg, "Back to the '80s' as French Navy Prepares for New Threats", *Defensenews*, January 2024.
206. See paintings of the Battle of the Pyramids (Lejeune) or Waterloo (Philippoteaux).

or to jam the electromagnetic spectrum) could simulate a feint or a diversionary maneuver. Unable to grasp the internal logic of maneuvers directed against them, enemies would be forced into revealing themselves or dispersing their resources. The saturation effect would at the very least cause a strain. Above all, this would help "real" units avoid excessive exposure. Too concentrated in classic maneuvers, transparency would make them easy targets for destruction.

This idea could also be adapted to the air and air-sea domains using "loyal wingmen" to support piloted air platforms. These formations could also be supported by drone swarms (like Gremlins or the ASSYDUS project[207]) to generate mass and make diversionary maneuvers more credible. Clearly, countless tactical combinations are possible in different environments, depending on the technological advances that are bound to take place and which the Russo-Ukrainian conflict, by its nature, cannot reflect.

The implementation of these kinds of operational approach will demand reflection on capabilities to determine the ideal mix of sophisticated drones, which are scarce and expensive, and single-use drones, which are numerous but easily destroyed or disrupted. Finally, the ability to create this type of tactical mass, as well as the need to ensure organic depth or to reuse it, rely on another kind of mass, strategic this time: the capacity to produce, maintain, and replace the large volumes of materiel needed in order to stay the distance. This depends both on the potential of the defense industry and on stocks built up prior to the conflict. The greater this strategic mass is, and the more the high-low mix discussed above is optimized,[208] the more possibilities there will be for deception and so for decisive actions, marking the start of a virtuous circle.

Reworking the principle of "rushed attack"

If the enemy "can see me clearly and has every chance of understanding my preparations", in short, if surprise is unattainable (because the geography of the theater of operations favors transparency or when facing enemies with technological parity, etc.), there is only one possible way to gain the upper hand: speed. This kind of offensive action, with a very short initial preparation phase, is called a "rushed attack" or a "hasty attack". It requires well-trained and highly agile units, which can only be guaranteed by rigorous operational preparation. For a land confrontation, it is important to practice rapid concentration movements starting with deliberately isolated units and, without losing cohesion, to gain the upper hand in a decisive zone.

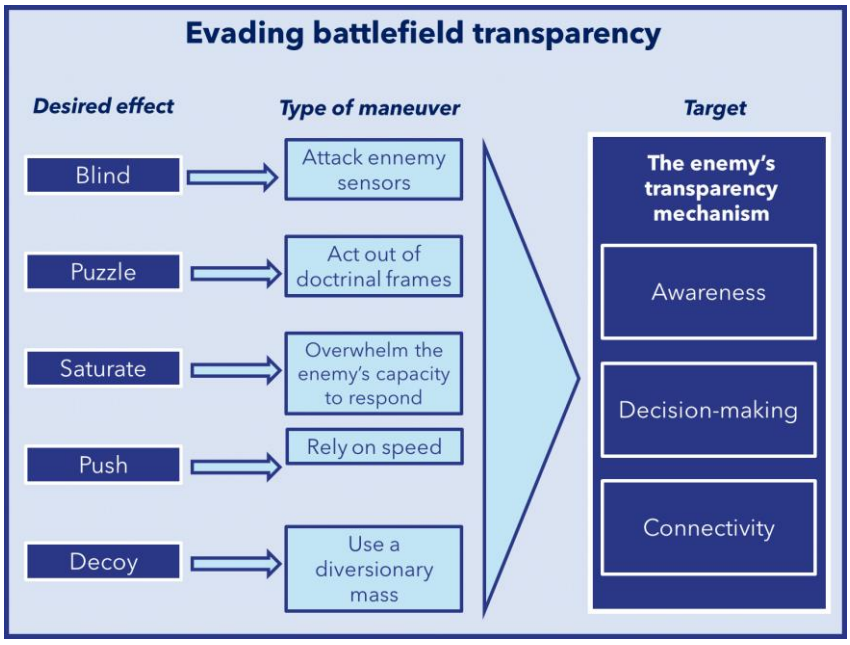
207. Swarm of decoy drones; see "ASSYDUS – Obtenir une surface équivalente radar (SER) en utilisant un essaim autonome de drones aériens", French Ministry of Armed Forces, defense.gouv.fr.
208. See P. Gros, "Mission d'information sur la préparation à la haute intensité", Assemblée nationale, February 17, 2022, www.assemblee-nationale.fr.

In other words, if the conditions of transparency cannot be avoided, only the tactical skill of engaged units can make it possible to evade the enemy's response. This skill must necessarily be superior to that of the enemy. Command style (initiative, familiarity with a dispersed C2) plays an important role here. The provision of "concealment kits" making use of the equipment discussed above (intelligent camouflage, signature decoys, etc.) would help units conducting a rushed attack to delay detection.

The French ground forces system probably has a comparative advantage when implementing this operational procedure. It is sometimes criticized for its lack of robustness, with an incomplete "heavy armored" section. Because it is a mid-range system, however, it has greater mobility and so is in a better position to carry out rushed attacks at the tactical-operational level, subject to the appropriate training. Nevertheless, this operational approach would require the rectification of capability gaps in certain support fields, particularly breaching engineering and offensive EW. France's airmobile force, the largest in Europe, offers the possibility of another form of rushed attack, as long as the vulnerability of these weapons delivery systems is addressed, for example with an improved mix of helicopters and support drones, and as long as the enemy's low-level air defense system has been significantly damaged in advance.[209]

To conclude, these three categories of operational approach all have their own internal logic but are not mutually exclusive, offering a variety of different combinations.

Diagram III-3: Evading transparency: Operational approaches



© Léo Péria-Peigné/Ifri, 2024.

209. SEAD missions.

Strategic implications for the entire spectrum of conflict

Beyond tactical or operational battlefield transparency, transparency also needs to be examined at the strategic level, where it reflects the dialectic of wills at the national level, which can be broken down into the three registers identified in the Chief of the Defense Staff's strategic vision: competition, dispute, confrontation.

Conventional confrontation: The temptation of preemptive strikes?

When combined with lethal effectors, battlefield transparency is likely to have devastating effects. It makes it easier for missiles to hit targets, particularly hypervelocity missiles,[210] which are difficult to intercept because of their maneuverability (unpredictable trajectory) and flight speed. This kind of premium on offensive engagement could be seen as intolerable by an actor in an acute crisis situation with a competitor of comparable military power: the abrupt nature of the potential threat would leave such an actor feeling excessively vulnerable. This could create a temptation to "strike first" in a sudden, unexpected salvo.[211] The aim would be to blind the enemy immediately, and to neutralize or throw into disarray its principal datalinks, communications nodes, and decision-making centers. If the situation was deemed to be critical, strikes (kinetic or high-amplitude electromagnetic pulses) would also target accessible satellites in the sovereign core or any civilian satellites with significant dual-purpose potential. This strike campaign would be supplemented by a cyber offensive, which would have to be planned well in advance in order to produce relevant effects coordinated with other operational axes[212] (conventional strikes, space attacks, information warfare). The goal would be to win without encountering resistance by provoking a double effect of mental stunning and functional paralysis. The combination of the two effects would prevent a coordinated, rapid, and effective response.

210. And more generally all weapons delivery systems capable of carrying out precise strikes (hypersonic missiles, cruise missiles, ground-to-ground OTH [over the horizon], etc.).
211. Global Trends, "The Future of the Battlefield", National Intelligence Council, April 2021.
212. See the in-camera hearing of General A. Bonnemaison, commander of the French cyber defense command. Report No. 27 from December 7, 2022, can be consulted on the website of the Assemblée nationale.

Clearly, this situation could lead to escalation, with both parties fearing the launch of a preemptive strike campaign by the other, fueling tension on both sides if essential interests are at stake. This strategic risk, inherent in the transparency-lethality duo (increasing accuracy and range of missiles), would be exacerbated by a mutual lack of understanding. To reduce the likelihood of this escalation scenario, resilience measures should be planned to complicate the enemy's calculations for a preemptive strike campaign: concealment, dispersal of strategic resources, more robust infrastructures, buried weapons stockpiles, redundant command systems, responsiveness and subsidiarity, and even the nation's "defense spirit" (collective moral force). All this would have a deterrent effect, or at least present a dilemma for whoever decides to strike first. The concept of strategic mass discussed above also plays a role in this scenario, making it possible to recover from a preemptive strike and even gain the upper hand if the initiator is relying solely on the strike and lacks the organic depth to engage in a prolonged conflict.

"Contestation": The destabilizing power of ambiguity and manipulation

Armed confrontation may be deemed too costly or risky. The conflict in Ukraine is ample proof of this, if proof were needed. It may even encourage more caution on the part of powers tempted to use coercion. So-called hybrid forms of attack, which fall below the threshold of armed conflict, are a cost-effective option for states wanting to challenge the international status quo.

Here, opacity outweighs transparency because the aim is essentially to act in the field of perceptions. Destabilization actions can also be conducted in the material field by exploiting opaque environments, first among them cyberspace, but also the deep sea or outer space. A well-coordinated campaign could aim to damage strategic organic resources, such as undersea cables, critical infrastructure networks, or satellites. Discreet DEWs or "stalker" satellites,[213] which maneuver close to other satellites and have potentially hostile intentions toward them, could be employed to dazzle, damage, or temporarily or permanently neutralize a particular strategic resource. Clandestine operations could supplement these disruptive actions. Attribution of the attack would be complicated by the opacity of the environment, improving the political cost-benefit ratio for the aggressor.

213. The actions of the Russian Luch-Olymp K2 satellite in the vicinity of Eutelsat satellites have been reported in the media. See M. Cabirol, "Comment trois satellites d'Eutelsat ont été espionnés par le satellite russe Luch Olymp 2", *La Tribune*, November 2023.

Countering these modes of action would require the ability to restore transparency, using intelligence to anticipate and attribute threats. Because intelligence is inevitably imperfect in opaque environments, resilience, some forms of which would be similar to those described above, would play an essential role. A panoply of capabilities centered around DEWs would make it possible to respond with greater political flexibility by giving decision-makers more options to calibrate the response to the nature of the damage suffered. Possession of such a panoply would also have a deterrent effect, reminding disrupters that they could be struck at the appropriate level of intensity without provoking escalation.

Competition: Non-state actors seeking to exploit transparency

Non-state adversaries are also affected by the transparency-opacity dialectic. For them, the aim is to negate the comparative transparency advantages of state armed forces while at the same time developing their own transparency.

To achieve the first of these objectives, non-state actors will exploit opaque environments, particularly urban areas. Underground tunnels enable physical concealment. Above all, population density allows them to fade into the environment.[214] This last point is also applicable to the sea domain, with exponentially increasing sea traffic making it possible to evade surveillance.[215] As the fight against ISIS made clear, these organizations are capable of coming up with rudimental procedures to render the most cutting-edge technologies inoperative, including rigorous OPSEC processes (such as compartmentation) and the use of homing pigeons, landline telephone networks, or couriers. As trivial as these measures may seem at first sight, they have proved their worth,[216] although they have the downside of significantly reducing liberty of action.

To achieve the second objective of developing their own transparency, non-state actors will take advantage of the democratization of transparency discussed above. Skilled innovators,[217] techno-guerrillas[218] have long demonstrated their ability to use or create surveillance drones, to collect information and images via civilian satellites, and to exploit cyberspace for their benefit.[219] Fighting in a familiar environment, they benefit from effective human intelligence.

214. B. R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony", International Security, No. 28, Summer 2003, pp. 27–36.
215. J. Bachelier and P. Boulanger, "La 'fusion de l'information'", *op. cit.*
216. As confirmed by the success of Hamas's attack on October 7, 2023, discussed above.
217. Global Trends, "The Future of the Battlefield".
218. J. Henrotin, *Techno-guérilla et guerre hybride*, *op. cit.*
219. Recruitment, financial transactions, disinformation, etc.

The transparency-opacity dialectic, therefore, is far from settled in this spectrum of conflict, and it would be imprudent for state armed forces to consider information superiority as guaranteed. Technological advantages can be negated by more detailed knowledge of the human environment and its exploitation for subversive purposes.

Conclusion

Ensuring we have greater transparency than the enemy on the battlefield undoubtedly offers a significant military advantage. NICTs and the democratization of transparency are opening up unprecedented possibilities in this area. Nevertheless, like any military phenomenon, transparency is affected by interrelated dialectics (technological, tactical, and strategic) that call for greater caution regarding its advantages.

First, it is important to make sure that the desire to gain the upper hand in transparency at any cost does not turn us into a mere spectator of the battlefield. All capability decisions affect a complex systemic equilibrium: too much investment in one segment comes at the expense of others. Seeing and understanding is one thing, being able to react accordingly is another. Reflection on the optimum high-low mix, briefly touched on above, could offer balanced solutions, both at the operational level (developing new operational approaches based on novel combinations) and at the strategic level (maintaining overall resilience).

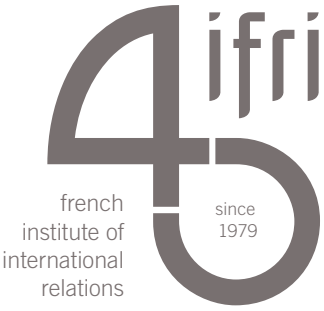
It is also crucial not to become a hostage to transparency by placing too great a trust in it. Any advantage is bound to be negated in the short or long term, whether from below (for example by terrorist organizations) or from above (opaque strategic destabilization campaigns, new technological spectrum enabling new types of subterfuge, etc.). Knowing how to exploit transparency while also being able to manage without it, or with less of it (degraded mode), seems sensible. At the least, it would help to conserve the doctrinal agility needed for adapting to new situations, or even better to provoke them. Transparency must not become a dogma, as happened to fire superiority in the interwar period, lulling the French military establishment into a form of intellectual complacency that led to the disaster of 1940. This kind of mindset considerably increases the risk of suffering a devastating shock, a striking paradox for those who make transparency the ultimate paragon of the operational art.

Beyond questions of technology (which enable in-depth examination of the benefits and limitations of transparency) or doctrine (the refinement of ways to exploit transparency), there is another resource that does not belong to either of these categories: operational readiness. The apparent tactical stalemate imposed by transparency is not necessarily inevitable. This tactical deadlock was justifiably lamented by General Zaluzhnyi, then Commander-in-Chief of the Armed Forces of Ukraine, but it is the product of a specific operational context that cannot be reproduced in its entirety: every conflict has its own internal logic, although conflicts in a given period may share a common core. Moreover, the two sides will not necessarily

have access to the entire panoply of modern joint combat capabilities. A particular conflict will not always reflect all the possible maneuvers that can be developed.[220] As a result, there is an urgent need for the optimum operational readiness of the French armed forces, in three respects. First, to keep the benefits of transparency for ourselves; second, to be able to subvert transparency in an equal conflict, which as seen above requires great tactical skill; and finally, and probably most importantly, to retain the ability to adapt if all the parameters discussed in this study undergo rapid evolution. In effect, technological progress moves so quickly that it is almost impossible for doctrine to keep up.

Thus, expecting to be surprised could well be the best way to resist surprise. Developing the habit of regular and rigorous training, in other words competence, is one of the factors of reactive adaptation and so, at the national level, of resilience.

220. We might witness an operational rupture (doctrinal, organizational, or tactical) before the end of this conflict. It remains very difficult to predetermine the reactive adaptation of a nation (units on the ground, technicians/civil engineers) if the resources are available.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org