LES DEEP FAKES DANS LA STRATÉGIE MILITAIRE, UN NOUVEL OUTIL DE LA MASKIROVKA ?

Philippe BELLISSENT
philippe@bellissent.com
Université Côte d'Azur, France

Abstract: *Deepfakes, produced through artificial intelligence, are becoming tactical and strategic instruments in military communication. By falsifying the voice, image or identity of political leaders, commanders or soldiers, they extend older practices of deception, from Sun Tzu and Clausewitz to the Russian doctrine of maskirovka. Unlike ordinary fake news, deepfakes rely on audio-visual embodiment. Their persuasive force comes from the apparent presence of an authoritative speaker. They therefore combine disinformation, credibility, plausibility and speed. In the military field, this speed is decisive: a false message that may be debunked in hours in political life can cause immediate operational damage during combat. The text identifies several military uses: disrupting enemy command, weakening morale, misleading the adversary about operational intentions, discrediting official orders, provoking escalation through false-flag narratives, and influencing civilian support for war. Deepfakes also raise new problems in machine-to-machine communication, especially identification systems, drone control and signal spoofing. Recent conflicts provide several examples: the fake video of President Zelensky calling for surrender in March 2022, Russian disinformation after the Crocus City Hall attack, Iranian fake television broadcasts in the Gulf, the Russian Doppelgänger operation, forged statements by American officials, and fabricated videos involving Putin or the Philippines. These cases show that deepfakes function as psychological operations within broader information warfare. The central issue is no longer only technical detection, since AI makes falsification increasingly difficult to identify. The decisive question becomes plausibility: how quickly military actors can assess whether a message fits the operational context, the source, and previous discourse. Deepfakes create a new cognitive fog of war. Drones may reduce visual uncertainty on the battlefield, but manipulated narratives increase cognitive uncertainty. In the OODA loop, the "Orient" phase becomes more fragile. Deepfakes therefore belong to cognitive warfare: they seek to disturb perception, trust, decision-making and command cohesion.*

Keywords: *deepfakes, maskirovka, cognitive warfare, deception, command and control.*

Introduction : Les deepfakes, un enjeu tactique et stratégique

Les deepfakes, des contenus audio ou vidéo manipulés grâce à l'intelligence artificielle (IA), sont devenus des outils stratégiques et tactiques dans le domaine militaire.

Leur caractéristique est de mettre en scène des acteurs virtuels ou des avatars d'hommes politiques, responsables militaires ou simples soldats, en usurpant l'identité réelle de personnages existants. Leur utilisation croissante dans les contextes de guerre stricto sensu ou de conflit hybride[1] soulève plusieurs enjeux : les conséquences des deepfakes peuvent revêtir une importance plus ou moins grande suivant les circonstances dans la fabrique de l'opinion. Mais elles peuvent entraîner des répercussions catastrophiques immédiates dans le domaine militaire dans la conduite des opérations. Et ce pour une raison principale que nous détaillerons plus loin, à cause de la temporalité du phénomène guerre qui n'est pas celle des autres domaines de la vie sociale.

C'est l'objectif de cette recherche d'évaluer la façon dont se construit une deep fake dans le discours militaire, de définir son tempo de réalisation et ses conséquences. Il convient tout d'abord de s'interroger sur ce terme de deep fake et de comprendre ce qu'il recouvre et en quoi il constitue une novation parmi les techniques et les méthodes utilisées dans le domaine militaire.

Tromperie et communication militaire : une constante historique

Le domaine militaire comporte, dès l'origine des premiers conflits, une composante de tromperie et de manipulation du jugement de l'adversaire. Dans la dimension mythique avec le cheval de Troie ou historique avec la première bataille de l'Antiquité dont nous avons un récit détaillé, celle de Kadesh en 1274 où le roi Hittite Muwatalli II fait croire au Pharaon Ramsès II que ses troupes sont encore loin du lieu de l'affrontement alors qu'elles sont déjà arrivées pour mieux surprendre les Egyptiens. Cet art de la tromperie sera théorisé par Clausewitz comme une composante du concept de brouillard de guerre.

La manipulation de l'adversaire prend depuis peu une nouvelle dimension avec les progrès de l'intelligence artificielle. Ils permettent aujourd'hui la production de contenus textuels ou iconiques d'une qualité technique de plus en plus avancée. SI l'on ne peut que s'en féliciter dans certains secteurs où ils sont devenus incontournables comme dans le domaine médical ou de la physique, leur impact est plus discutable dans d'autres domaines comme dans la communication politique. Ils permettent en effet la création de textes, de visuels, et de vidéos dans lesquels l'énonciateur n'est pas la personne réelle. Ces faux messages ou discours sont qualifiés de deep fakes et ont pour but d'induire en erreur les destinataires très majoritairement utilisateurs des réseaux sociaux.

Fake news, deepfakes : distinctions conceptuelles

On peut préciser le terme de deep fake à la lumière de la recension effectuée par Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018) sur le terme de fake news, la deep fake en étant une variante plus pernicieuse. La fake news est constituée par une information délibérément fausse destinée à tromper l'opinion publique diffusée sur les réseaux sociaux mais qui peut aussi émaner d'une presse officielle dans des pays où les médias sont étroitement contrôlés par l'Etat. Cette définition permet donc de distinguer la fake news

[1] Des débats médiatiques montrent que pour bon nombre de militaires (dont le colonel Goya très présent sur les plateaux télés en France comme LCI) il vaut mieux réserver le terme de guerre aux conflits armés sur un théâtre d'opérations comme en Ukraine avec leur dimension létale et parler de stratégie hybride pour les opérations de désinformation, manipulation de l'opinion ou actions non létales telles que la rupture volontaire de câbles sous-marins ou d'attaques cyber sur des sites Internet. (Goya, 2014). En l'absence d'un terme alternatif faisant consensus nous garderons celui de guerre dans ses différentes acceptions.

qui est une désinformation, de la mal information, transmission ou relation de faits exacts, mais détachés de leur contexte de façon à tromper les récepteurs de l'information et d'orienter leur jugement et de la mésinformation, transmission de messages faux par un locuteur sans qu'il soit lui-même conscient de la fausseté des messages.

L'utilisation du terme anglophone de fake news apporte un supplément de sens à la notion de désinformation car il inclut généralement le fait qu'elle s'exerce (mais pas nécessairement) sur les réseaux sociaux en utilisant les ressources de plus en plus performantes de l'Intelligence Artificielle

L'article précité établit une typologie sur deux axes, le degré de factualité (facticty) et l'intention de tromper. Le degré de factualité ira du fort (publicité, propagande, satire, basée sur un événement) au faible (mode satirique ou fabrication pure d'un narratif). Le degré d'intention de tromper ira du fort (manipulation, fabrication de fausses nouvelles) au faible (parodie d'information comme dans des émissions de télévision qui ressortent du divertissement).

Nous souhaitons ajouter à ces deux axes un troisième axe basé sur la vraisemblance de l'information. Cette question implique de s'intéresser à la réception de l'information car la vraisemblance n'est pas la vérité en soi d'une information mais le degré de confiance que les récepteurs du discours lui accordent.

Il convient maintenant de voir en quoi les deep fakes se distinguent des simples fake news. Si les fakes news peuvent avoir l'écrit pour support, les deep fakes utilisent les photos, les vidéos ou les enregistrements audio pour diffuser de fausses informations. Tout l'intérêt de la deep fake est le renforcement de la crédibilité du discours par la présence de l'énonciateur. Celui-ci possède nécessairement la légitimité voulue pour que son discours apparaisse crédible. On retrouve ainsi le phénomène bien connu en communication du discours d'autorité accepté par l'auditoire (Joule et Beauvois 2024, Cialdini 2014, Mucchielli 1998).

La cible principale de ces deep fakes est celle des citoyens avec pour intention de renforcer une prise de position politique ou d'orienter un vote lors d'une élection en décrédibilisant les candidats d'un parti adverse.

De très nombreuses études universitaires ont été réalisées depuis plusieurs années dans ce domaine et la lutte contre les deep fakes a été relayée par les médias qui alertent régulièrement sur ces fausses informations, avec sous-jacente l'idée que les journalistes sont là pour éclairer les citoyens en dénonçant le caractère mensonger de ces deep fakes. C'est ainsi que depuis plusieurs années nombre de médias appartenant à des chaînes publiques comme c'est le cas en France avec France 2 ou à des médias indépendants à la réputation établie (Le Monde, Le Figaro) ont créé des services chargés de « débunker » les deep fakes et les fake news. Le mot vient d'ailleurs d'apparaître officiellement dans la langue française dans le Petit Robert avec le sens de « *démystifier, démontrer la fausseté d'une information, une théorie). Débunker des thèses complotistes.* ». Ce travail citoyen des journalistes, destiné à améliorer la crédibilité des médias traditionnels face aux réseaux sociaux peut etre confronté à un manque de moyens pour faire efficacement leur travail face aux flots de fake news émanant de centrales de désinformation ou de fermes à trolls disposant de moyens digitaux d'envergure. Si des délais de quelques heures pour démonter une fausse information sont admissibles dans le domaine du politique, nous verrons qu'ils deviennent plus problématiques dans le domaine militaire qui exige des délais de vérification des informations beaucoup plus brefs.

Spécificité des deepfakes dans le domaine militaire

Il est un domaine qui a été moins exploré, celui de l'impact des deep fakes sur la cible des militaires. Quel peut être leur impact et le progrès des techniques en IA ne va t'i pas apporter une dimension nouvelle à la question de la communication dans la conduite des opérations militaires ?

Les deepfakes dans le domaine militaire s'inscrivent dans une problématique beaucoup plus large qui est celle de la communication dans la conduite des conflits armés.

Qu'il s'agisse de Sun Tzu ou de Clausewitz, les auteurs les plus remarquables dans le domaine de la stratégie militaire ont insisté sur le rôle de la communication dans la conduite de la guerre. L'aphorisme de Sun Tzu (2017) : « Tout l'art de la guerre est basé sur la duperie » montre bien que cette dimension communication fait partie intégrante de la conduite des conflits. Cette conception de la guerre reste toujours présente dans la pensée militaire chinoise comme le développent Qiao Liang et Wang Xiangsui (2006). Clausewitz n'utilise pas tel quel la notion de communication mais deux concepts essentiels de sa pensée s'y réfèrent indirectement.

Tout d'abord la friction (*Reibung*), quand l'intention et le plan d'action d'un chef se grippent à cause d'événements fortuits et non prévus. Ainsi dans un conflit actuel un exemple de friction pourrait être la fourniture de batteries pour des moyens de communication qui ne correspondent pas aux matériels en dotation rendant inopérants les matériels de transmissions utilisés. Ensuite le brouillard de guerre (*Nebel des Krieges*) qui regroupe l'ensemble des facteurs ne permettant pas une compréhension exacte des situations le terrain, qu'il s'agisse de ses propres unités par manque de coordination ou de moyens de renseignement insuffisants ou encore des intentions de l'adversaire qui, volontairement ou non, cache son dispositif et ses intentions de manoeuvre. Soulignons à cet égard que l'utilisation massive des drones sur le champ de bataille comme c'est le cas sur le théâtre d'opérations en Ukraine bouleverse complètement la donne par rapport aux conflits antérieurs. Tous ces éléments contribuent à augmenter l'incertitude dans la conduite des conflits et conduisent à des prises de décision des responsables du commandement en situation d'information incomplète.

La *maskirovka* : une doctrine structurante de la stratégie militaire russe

Cette réflexion conduit à préciser le terme de *maskirovka* présent dans le titre de cette communication. Comme le souligne Christine Dugoin-Clément (2025) Il fait partie des stratégies globales d'influence élaborées comme une véritable doctrine par l'armée russe. Il est l'équivalent du terme d'origine anglo-saxon de déception entendu comme une tromperie, une supercherie, une duperie, utilisé dans le vocabulaire militaire en français alors que des termes équivalents existent dans notre langue (Chekinov et Bogdanov).

Parmi les auteurs s'étant intéressés à cette question de la maskirovska, Dimitri Minic (2023) considère que la pensée militaire soviétique puis russe a théorisé depuis les années 30 cet usage de la dissimulation et de la tromperie comme un outil fondamental de l'art de la guerre. Il est significatif comme le note Lucy Ash (2020) que la ruse du prince Dimitri Donskoi camouflant une partie de ses forces aux armées mongoles à la bataille de Koulikovo en 1380 soit encore enseignée aux élèves officiers russes. Elle est définie dans le règlement de campagne de l'Armée Rouge comme le rappelle Claude Quétel :

> « La maskirovka constitue le moyen le plus important d'acquérir la surprise, condition de base pour le succès dans la bataille (…) en assurant les opérations par des mesures complexes visant à tromper l'ennemi sur la présence et la localisation des forces, des installations, les objectifs, la préparation d'une offensive. » (Quétel, 2022)

Cette stratégie sera particulièrement utilisée lors de l'opération Bagration en août 44 lors de la grande offensive de l'armée russe sur les groupes d'armées centre du dispositif allemand. Si les Russes l'ont théorisé, les Alliés pendant la 2e Guerre Mondiale l'ont aussi utilisé. On peut mentionner à la fois l'usage du camouflage et des leurres avec l'utilisation de faux équipements de structure factice (comme les Américains l'ont fait lors de l'opération Fortitude avant le débarquement en Normandie avec la fausse armée de Patton), des mouvements simulés pour masquer les intentions des forces adverses (mouvements de véhicules légers anglais à la bataille d'El Alamein pour camoufler l'axe principal d'attaque) mais aussi la désinformation comme l'opération Bodyguard des Anglais avec le cadavre d'un faux officier échoué sur une plage avec une mallette comportant des documents précisant que le débarquement allié aurait lieu dans le Pas de Calais.

L'objectif d'utilisation de fake news et de deepfakes est de rendre la prise de décision et les capacités de réactivité de l'adversaire de plus en plus complexes. On peut effectivement envisager la possibilité de contrefaire la voix d'une autorité et de donner de faux ordres préjudiciables à une unité sur le terrain. Les nouvelles architectures de communication impliquées dans le combat collaboratif peuvent permettre à terme le détournement de communications dans un réseau et la question de plus en plus complexe de la reconnaissance ami-ennemi ouvre la porte à des possibilités de manipulations de plus en plus sophistiquées. Les opérations sous faux drapeau, dont l'histoire fournit de nombreux exemples, peuvent aussi bénéficier de l'apport de deepfakes soigneusement préparées.

L'accélération du tempo des opérations militaires, permise par le recours à toujours plus de communication, implique de réfléchir au mode opératoire des deepfakes.

Objectifs militaires des deepfakes

La première question à se poser est celle de l'objectif recherché dans la diffusion d'une deep fake.

- Le premier objectif recherché peut être la désorganisation du commandement adverse. En s'immisçant dans le réseau de communication de l'ennemi il est possible de créer une confusion dans la chaîne de commandement entraînant au pire des erreurs d'appréciation et de mauvaises décisions mais au moins des retards dans les décisions préjudiciables à la manœuvre. Même si les réseaux militaires sont en théorie protégés contre les intrusions, il existe toujours une possibilité qu'une fausse image apparaisse sur les écrans d'ordinateurs de l'ennemi. Cette possibilité est rendue plus probable si le réseau sécurisé est défaillant et que l'on recourt à des réseaux non sécurisés.
- Le deuxième objectif consiste dans la recherche d'un affaiblissement de la volonté de combattre. Durant la guerre du Pacifique les Japonais avaient utilisé cette possibilité en diffusant des émissions de radio imitant les radios américaines en insistant sur des pertes exagérées.
- Le troisième objectif vise à tromper l'adversaire sur les intentions réelles des manœuvres envisagées. En multipliant le trafic radio dans une zone donnée on peut faire croire que l'effort principal va se situer à cet endroit alors que

l'offensive réelle va se porter ailleurs. Cette possibilité a été exploitée par les troupes de la coalition lors de la 2e guerre du Golfe, faisant croire à une offensive sur l'axe Koweit-Bagdad, alors que l'offensive réelle consistait en une manœuvre d'enveloppement sur la droite du dispositif irakien (Hémez, 2022). C'est ce que les militaires qualifient de manœuvre de déception.

- Le quatrième objectif vise à décrédibiliser les informations émanant de la chaine de commandement adverse. En saturant l'espace de communication de messages contradictoires il est possible d'affaiblir l'adhésion aux directives émanant de la chaîne de commandement en créant un doute sur l'information fournie et un retard dans la prise décision, lié au temps de la vérification.
- Le cinquième objectif consiste à provoquer un incident entraînant une escalade dans un conflit. Ce sont généralement des opérations sous faux drapeau qui ont pour but de créer les conditions d'une intervention en réponse. Les Japonais l'ont utilisé avec l'épisode du pont de Moukden en 1931 pour trouver un prétexte à envahir la Mandchourie.
- Le sixième objectif ne concerne pas la cible militaire directement mais la cible civile dont l'adhésion aux buts poursuivis par ses forces armées est indispensable dans la conduite d'un conflit sur le long terme.

Deepfakes et relations machine-machine

Les différents objectifs précités concernent les relations humaines de communication. Un domaine prend une importance croissante, celui des relations machines-machines. C'est toute la problématique en aéronautique militaire de l'identification d'un aéronef adverse avec les systèmes IFF (Identification Friend or Foe). Les différentes aviations militaires ont depuis la guerre de 14 consacré des sommes importantes pour identifier correctement un aéronef entrant dans une zone de détection visuelle d'abord radar à partir de 1939 dans la RAF (un sujet complexe traité rigoureusement en langue française sur le site de la base documentaire de l'artillerie). Là encore, la possibilité d'envoyer un faux signal d'appartenance à une force aérienne amie rend indispensable la sécurisation des informations et des réseaux. Le phishing ou l'usurpation d'identité fait partie de l'arsenal des techniques de manipulation d'identité comme le relève Philippe Boulanger (2025) dont le « débunkage » est crucial pour les attaques d'aéronefs opérant avec de faux codes d'identification.

Dans le même domaine des fausses informations dans le dialogue machine-machine, le conflit en Ukraine montre depuis quelques mois que la transmission d'informations des opérateurs vers les drones peut être brouillée par de fausses instructions transmises par des ondes radio. Un brouillage qui a conduit récemment l'armée russe à développer des transmissions filaires pour la communication avec les drones (Fibermart, 2025). Ce mode de transmission réduit évidemment la portée d'utilisation des drones qui est limitée à quelques kilomètres d'autonomie.

Les différents types de déception militaire ne constituent pas pour autant des fakes news comme le rappelle Philippe Boulanger (2025). Il leur manque l'utilisation des réseaux sociaux comme vecteurs de la diffusion de la désinformation. Soulignons aussi que les deepfakes dans la relation machine-machine ne comportent pas un élément essentiel qui reste du domaine de la relation homme-machine-homme. Si une organisation produit une deep fake par le biais d'une IA à destination d'un public, individu ou organisation, la réception de cette deep fake passe par une interprétation du récepteur qui construit le sens

de cette information. Elle s'insère dans les schémas cognitifs du récepteur, ses cadres narratifs, ses émotions, ses attentes, son idiosyncrasie. L'interprétation du message, élément clé de la communication comme l'avait écrit Paul Watzlawick (1967) est indissociable de l'efficacité d'une fake news. Cette capacité incontournable de l'interprétation ne concerne pas en revanche la communication machine-machine. Un capteur reçoit un signal, calcule des paramètres mais reste en deçà du seuil de l'interprétation… du moins tant qu'un humain reste dans la boucle. La généralisation de l'utilisation des fake news pose un certain nombre de questions qui doivent impérativement trouver des solutions et si possible quasiment instantanément comme c'est le cas d'un système d'armes anti missiles qui doit répondre instantanément à une menace.

Cette première question est évidemment cruciale en aéronautique militaire quand un pilote doit prendre une décision très rapide pour identifier un aéronef. Quelques secondes dans l'identification peuvent faire la différence en situation de combat aérien et les développements à venir du combat en essaim où une plate-forme pilotée dirige des dizaines de drones rend de plus en plus complexe cette question de la sécurité des transmissions.

Comment vérifier dans un contexte militaire la vraisemblance d'une vidéo ou d'un texte dont on soupçonne qu'il puisse être un faux ? A l'inverse, pour l'émetteur d'une deep fake, comment produire un mensonge crédible ? (Naffi et alii, 2024).

Avant que les réseaux sociaux n'envahissent l'espace médiatique, les différents récits pouvaient plus facilement être contrôlés par des instances gouvernementales, même dans des pays démocratiques, par l'usage de la censure comme ce fut le cas en France pendant la Grande Guerre. (Forcade, 2016) Ce contrôle de l'information n'est plus possible efficacement même dans des pays autoritaires. Comment se forme et se déforme l'opinion du combattant dans ces situations ? Un combattant des années 2020 n'est jamais totalement coupé de l'information avec les nouveaux dispositifs du téléphone portable, d'Internet et des réseaux sociaux. Il offre ainsi plus de prise à des discours manipulatoires même si l'encadrement par la hiérarchie limite ce genre de danger.

La deuxième question à envisager est celle de la production de ces deepfakes. la Russie est passée maître dans l'art de produire des deepfakes avec les fermes à trolls qui font partie de la nébuleuse de la cyberguerre dont les fake news et les deep fake ne sont qu'un élément parmi d'autres (sabotage de réseaux et de sites informatiques d'équipements publics tels que les hôpitaux, les transports), Leur rôle consiste à créer des milliers de faux comptes envoyant des messages en grands nombres sur les réseaux sociaux de façon à saturer ces sites et augmenter la viralité des commentaires sur tel ou tel événement. La liberté de parole existant sur des réseaux comme X et le refus des dirigeants d'exercer un contrôle sur ces messages et leurs auteurs a permis de renforcer les opinions de post-vérité. L'arsenal des techniques dans les guerres numériques s'est largement diversifié comme le note Philippe Boulanger (2025).

Des cas pratiques relevés sur l'utilisation de deepfakes

Les conflits récents offrent de nombreux exemples de deepfakes comportant une incidence dans les opérations militaires.

On peut ainsi relever (Twomey and alli, 2023) :

1. Vidéo truquée de Zelensky appelant à la reddition (mars 2022) (Beurnez, 2022)

Une vidéo montrait le président ukrainien Volodymyr Zelensky demandant aux soldats de déposer les armes. Cette vidéo a été diffusée par un piratage de la chaîne Ukraine 24, par un bandeau défilant pendant une émission en direct de la chaîne. Les messages demandaient aux soldats ukrainiens de déposer les armes et affirmaient que Zelenski ne pouvant reprendre le Donbass avait fui Kiev. Le message a été repris par la chaîne Telegram pro-Kremlin et sur le réseau social VKontakte, le réseau social miroir de Facebook appartenant au Kremlin. La vidéo de mauvaise qualité ainsi que l'audio qui imitait mal la voix du Président Zelenski a rapidement été identifiée comme une deepfake et démentie par les autorités ukrainiennes. Indépendamment de la possibilité de debunker cette vidéo par sa médiocrité technique, les conditions de son énonciation ne plaidaient pas pour son authenticité. D'abord parce que la gravité du message aurait mérité une déclaration officielle en plein écran et pas l'insertion d'un bandeau dans une autre émission, ensuite parce que tous les discours précédents du Président Zelenski appelaient au contraire à la résistance face à l'invasion russe et qu'à la date du 16 mars l'Ukraine avait déjà enrayé l'offensive russe au moins dans la direction de Kiev ce qui ôtait une bonne part de crédibilité et de vraisemblance à cette pseudo-intervention télévisée. Ce qui a entraîné une autre intervention télévisée du Président Zelenski : « Si je peux offrir à quelqu'un de déposer les armes, c'est l'armée russe. Rentrez chez vous. ». La vidéo des services russes a ensuite été rapidement supprimée des réseaux Facebook et YouTube.

2. Deepfake d'un responsable ukrainien revendiquant un attentat à Moscou (mars 2024) (Genevrier et Fourt, 2024)

Le 22 mars 2024, une attaque terroriste a visé le Crocus City Hall, une salle de concert située à Krasnogorsk, en périphérie de Moscou. Des assaillants armés ont ouvert le feu sur les spectateurs avant de déclencher un incendie, causant la mort de 145 personnes et blessant 551 autres. Initialement, le président russe Vladimir Poutine a suggéré une implication ukrainienne dans l'attentat, une affirmation démentie par les États-Unis et l'Ukraine. Devant la revendication explicite de l'État Islamique le directeur du FSB, Alexandre Bortnikov, a été obligé de reconnaître que l'attaque avait été planifiée par l'État islamique au Khorassan, sans mentionner de lien dans l'organisation de l'attentat avec l'Ukraine. Une vidéo diffusée par la télévision d'état russe montrait Oleksiy Danilov, chef du Conseil de sécurité ukrainien, revendiquant une attaque terroriste à Moscou. L'analyse a révélé une manipulation par intelligence artificielle. Les images d'une interview du responsable ukrainien ont été manipulées avec un faux discours repris sur les réseaux sociaux pro-russes et qui a engrangé plusieurs centaines de milliers de vues. La propagande du Kremlin a tenté pendant plusieurs jours d'attribuer aux Ukrainiens l'attentat du Crocus City Hall qui avait causé la mort de 145 personnes et 551 blessés. Il a fallu une revendication explicite de l'Etat islamique au Khorassan pour que les autorités russes abandonnent l'hypothèse de la responsabilité ukrainienne.

3. Opération iranienne diffusant un faux journal télévisé aux Émirats arabes unis (décembre 2023).

Des hackers liés aux Gardiens de la Révolution Iranienne ont piraté des services de streaming aux Émirats pour y diffuser un faux journal télévisé animé par un présentateur généré par IA, relayant des images non vérifiées sur la guerre à Gaza. (Naffi et alii, 2024)

4. Utilisation de deepfakes pour l'entraînement militaire américain (avril 2024) (Skove, 2024)

Les forces spéciales de l'armée américaine utilisent des technologies de clonage vocal et de deepfakes, comme l'outil « Ghost Machine », pour simuler des scénarios de guerre informationnelle et former les soldats aux menaces de désinformation. « Ghost Machine », permet de générer des imitations vocales de qualité à partir d'un simple échantillon de voix et d'un ordinateur portable standard. Ce système est utilisé par l'ARSOF (Army Special Operations Forces) pour simuler des communications ennemies, des ordres falsifiés ou des messages de propagande, dans le but d'enseigner aux opérateurs comment ces technologies peuvent être exploitées pour manipuler, désinformer ou inciter à la défection. Cette approche s'inscrit dans une tradition de guerre psychologique, modernisée par l'accessibilité des outils d'intelligence artificielle. Les instructeurs des forces spéciales utilisent « Ghost Machine »» pour démontrer comment des technologies bon marché et largement disponibles peuvent transformer les capacités des gouvernements à cibler et influencer les soldats.

5. Campagne de désinformation « Doppelganger » menée par la Russie (depuis 2022) (Dugoin-Clément, 2023)

Cette opération de désinformation russe a créé de faux sites web imitant des médias occidentaux pour diffuser des contenus pro-Kremlin, incluant des vidéos deepfake visant à saper le soutien à l'Ukraine. L'opération Doppelgänger est une campagne de désinformation russe, initiée en 2022, visant à affaiblir le soutien occidental à l'Ukraine et à promouvoir les intérêts du Kremlin. Elle utilise des techniques sophistiquées de clonage de sites web et de diffusion de contenus falsifiés pour manipuler l'opinion publique dans plusieurs pays, notamment la France, l'Allemagne, les États-Unis et l'Ukraine. La méthodologie a consisté à cloner des sites Web avec la création de copies quasi identiques de sites de médias et d'institutions officielles (pour la France Le Monde, Le Figaro, Le Parisien, le ministère des affaires étrangères français) pour diffuser de fausses informations pro-russes. Une utilisation de faux profils sur les réseaux sociaux comme Facebook et X (anciennement Twitter) a permis d'amplifier la portée des contenus falsifiés. Une autre technique a consisté à acheter des espaces publicitaires sur les réseaux sociaux pour la promotion de messages de propagande, en utilisant des célébrités, pour renforcer la crédibilité des messages par la légitimité réelle ou supposée des intervenants. Cette opération a été conduite par des entités russes telles que la Social Design Agency (2025) et Structura National Technologies[2], en coordination avec les services de renseignement russes. Des réactions et contre-mesures ont fait en sorte de minimiser l'impact de ces offensives cyber comme en France, par l'intermédiaire de VIGINUM (service de vigilance et de protection contre les ingérences numériques étrangères), a identifié et dénoncé l'opération, soulignant son caractère de guerre hybride.[3] L'Union Européenne a imposé des sanctions à plusieurs entités et individus russes impliqués dans l'opération ainsi que le FBI sous l'administration Biden. L'opération Doppelgänger a par la suite étendu ses activités au conflit israélo-palestinien pour diffuser des messages de désinformation visant à diviser l'opinion publique occidentale.

---

[2] Cette organisation fait l'objet de sanctions par le gouvernement britannique : https://www.opensanctions.org/entities/NK-nB5tLveacbaovVHsyrPBd9/.

[3] *Guerre en Ukraine : un bilan de Viginum sur les actions russes de désinformation* https://www.vie-publique.fr/en-bref/297500-guerre-en-ukraine-les-strategies-de-desinformation-russes-par-viginum.

6. Vidéo deep fake d'un responsable américain sur les frappes ukrainiennes (juin 2024)

Une vidéo falsifiée montrait un officiel du Département d'État américain justifiant des frappes ukrainiennes sur une ville russe, dans le but de légitimer les actions militaires ukrainiennes. Cette deepfake mettait en scène Matthew Miller, porte-parole du Département d'État américain, déclarant que la ville russe de Belgorod était une cible légitime pour des frappes ukrainiennes avec des armes fournies par les États-Unis. Cette vidéo a été diffusée sur des plateformes comme Telegram et relayée par des médias d'État russes, a été rapidement identifiée comme une manipulation numérique. Elle correspondait à un besoin de la propagande russe de répliquer aux accusations de crimes de guerre concernant le bombardement d'objectifs civils en Ukraine. Des analyses ont révélé des incohérences visuelles, telles que des changements de couleur de vêtements et une synchronisation défectueuse entre les mouvements des lèvres et l'énonciation du discours. Cette deep fake a été condamnée par les autorités américaines comme tentative de désinformation pour saper le soutien occidental à l'Ukraine.

7. Vidéo deep fake de Vladimir Poutine annonçant une mobilisation générale (juin 2023)

Les Ukrainiens ont aussi recouru à des deepfakes durant le conflit avec la Russie. Une deep fake diffusée sur plusieurs réseaux russes montrait le président Poutine annonçant une invasion et une mobilisation générale, illustrait l'utilisation de cette technologie pour semer la confusion. Cette vidéo avait pour but de démoraliser la population russe en lui conseillant d'évacuer les zones proches de la ligne de front.

8. Deepfake du président philippin Bongbong Marcos donnant des ordres militaires (avril 2024).

Une vidéo falsifiée montrait le président philippin ordonnant à l'armée d'agir contre la Chine, exacerbant les tensions autour du conflit en mer de Chine méridionale.

9. Utilisation de deepfakes dans le conflit Israël-Hamas (octobre 2023)

Des images falsifiées montrant des enfants blessés ont circulé sur les réseaux sociaux, utilisées par les deux camps pour susciter l'émotion et influencer l'opinion publique.

10. Fausses vidéos de soldats ukrainiens démoralisés en novembre 2025

Cette vidéo présente sur Facebook et X prétend montrer des soldats se rendant en masse pendant la bataille de Pokrovsk[4].

Ces exemples montrent l'utilisation croissante des deepfakes dans le domaine de la guerre informationnelle, constituant de véritables opérations psychologiques destinées à annihiler la volonté de l'adversaire et aussi à mobiliser l'opinion publique de son camp ou internationale. Les Russes ont parfaitement compris l'utilisation qui pourrait être faite des images vidéo et de la baisse de leur crédibilité à l'heure des deepfakes. Ils ont ainsi accusé les Ukrainiens de vouloir mobiliser faussement l'opinion internationale après les massacres de Boutcha avec des vidéos trafiquées et de fausses images de cadavres de civils. Un travail

[4] Vidéo générée par l'IA Sora dont le logo apparait sur la vidéo ! https://www.franceinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-de-fausses-videos-generees-par-ia-pretendent-montrer-une-reddition-massive-de-soldats-ukrainiens_7607642.html.

minutieux des médias occidentaux a permis de montrer clairement les exactions des soldats de l'opération militaire spéciale au prix de longues enquêtes de terrain.

Ce recours de plus en plus systématique aux deepfakes pose de nouvelles questions dans le travail des médias mais aussi des gouvernements face à l'envahissement des réseaux sociaux. La crédibilité des médias occidentaux avait été entachée au moment de la Révolution roumaine avec l'affaire du charnier de Timisoara. Elle est confrontée à un défi plus important actuellement avec les progrès de l'Intelligence Artificielle pour démêler le vrai du faux.

La question du temps est une variable primordiale à analyser dans l'impact que peuvent avoir les deepfakes et les fake news. En combien de temps une deep fake se diffuse-t-elle dans l'espace médiatique ? Combien de temps faut-il pour la décrédibiliser ? Combien de temps faut-il pour transmettre aux autorités concernées et aux personnels sous leur commandement la bonne version d'une information ? Combien de temps faut-il pour que les acteurs concernés adhèrent à cette contre information ? Comment éduquer les acteurs concernés à une méfiance légitime face à des informations suspectes ?

Enfin dans quelle perspective plus large s'inscrivent ces deepfakes dans la problématique plus large de la dissimulation des intentions devenue un art dans la pensée militaire russe sous le terme de maskirovka. Autant de questions à résoudre sur l'utilisation de ces informations manipulatrices pour éviter d'en subir les effets négatifs.

Quelles pistes pour aller plus loin dans la lutte contre les deepfakes

Les progrès rapides de l'intelligence artificielle permettent d'envisager des deepfakes de plus en plus sophistiquées. L'enquête menée par Olivier Lascar (2024) montre que le debunkage des vidéos devient de plus en plus difficile voire impossible avec les progrès permanents de l'IA. Pour l'expert spécialiste en Lê Nguyen Hoang, les progrès de l'IA sont devenus tels en cinq ans que le repérage de vidéos ou d'images trafiquées devient pratiquement impossible techniquement. Dans le domaine militaire, la solution consiste évidemment de s'abstenir d'ut iliser les réseaux sociaux et les téléphones portables ce qui est devenu normalement la norme dans toutes les armées. Encore faut-il que les personnels engagés en opérations respectent strictement les consignes de ne pas utiliser leurs téléphones portables pour des motifs personnels comme téléphoner à sa famille. Une imprudence qui avait causé à Makiïvka, dans l'oblast de Donetsk dans la nuit du 31 décembre 2022 la mort de 90 soldats russes, suivant le ministère de la Défense russe ou 400 suivant l'armée ukrainienne. L'armée russe a aussi compté des pertes pour une utilisation tactique de téléphones portables par manque de moyens de communication.

Quelles sont alors les solutions possibles pour ne pas tomber dans le piège des deepfakes ? La réflexion sur la vraisemblance de l'information transmise semble être la meilleure solution.

Face à cette menace les pays occidentaux mettent en place des programmes de contre-mesures pour éviter de voir leurs forces armées paralysées par un brouillard d'information désorganisant les chaînes de commandement et partant, l'efficacité de leurs forces sur les théâtres d'opérations. Dans cette nouvelle forme de lutte entre l'épée et le bouclier investissant le champ de la communication, quelles sont les réponses les mieux adaptées ?

De quels outils théoriques disposons-nous pour contrer ces récits de la post-vérité qui posent un véritable défi aux armées des sociétés démocratiques dans les conflits actuels en Ukraine comme au Moyen Orient ? La théorie de la désinformation développée dans

l'étude de Wardle et Derakhshan (2017) à la demande du Conseil de l'Europe nous fournit un cadre d'analyse sur ces questions.

L'analyse du discours constitue l'outil théorique indispensable pour penser le mode de fonctionnement des récits de la post-vérité et le travail de Patrick Charaudeau (2020) sur la manipulation de la vérité permet de définir un cadre théorique adéquat pour cette réflexion. Il resterait pour poursuivre la pensée de l'auteur à examiner comment les catégories qu'il définit peuvent s'appliquer au contexte particulier de la manipulation dans le domaine militaire. En effet dans le domaine militaire le récepteur n'est pas un usager des réseaux sociaux isolé et conditionné seulement par ses groupes informels de référence. Il s'inscrit dans une organisation avec ses propres contraintes discursives produisant un fort contre-discours aux tentatives de manipulation externes.

Il conviendra aussi de remettre en perspective à la lumière des nouvelles technologies l'analyse classique de Jacques Ellul sur les propagandes pour penser cette nouvelle forme du mensonge d'Etat et des organisations politiques.

Au-delà des questions sur le fonctionnement des deepfakes qui relèvent du domaine des sciences de la communication, se pose l'émergence de nouvelles problématiques dans le domaine de la stratégie et de la tactique où apparaît une nouvelle forme de brouillard de guerre (Dabila, 2025). L'utilisation massive des drones aux performances de plus en plus élevées et dont la diversification des missions ne fait que croitre dans le conflit russo-ukrainien, constitue une révolution au même titre que l'a été l'utilisation de l'arme aérienne et des blindés dans les conflits du XXe siècle. Cette arme nouvelle réduit le brouillard de guerre clausewitzien en donnant à voir précisément sur le champ de bataille ce qui était difficile même pendant la deuxième guerre mondiale (Beevor, 2015)[5]. Mais cette amélioration de ce qu'il est possible de voir s'accompagne avec les deepfakes de difficultés nouvelles dans la compréhension des événements (Maud et Maud, 2021). Ce qui a été gagné sur le plan visuel s'accompagne maintenant de nouvelles difficultés sur le plan cognitif. Dans la boucle OODA (Observe-Oriente-Décide-Agit) la phase d'orientation (ou d'analyse) devient de plus en plus complexe avec une multiplicité de signaux contradictoires.

Le cerveau devient ainsi comme le souligne Clara Petit (2025) un sixième champ de guerre. « La guerre cognitive est une forme de guerre hybride visant à agir directement sur la pensée, la perception, la mémoire ou encore la prise de décision. Elle s'inscrit au cœur d'une stratégie complète d'influence. » Dans cette logique la perturbation du C2 (Command and Control), la confusion décisionnelle, l'érosion de la confiance entre responsables d'unités, les retards à la prise de décision constituent les objectifs majeurs de cette guerre cognitive où les deepfakes jouent le rôle d'élément perturbateur parmi les différentes techniques de déception.

Si les moyens de la duperie ont bien évolué depuis le temps et l'espace d'où Sun Tzu nous parle, l'esprit reste le même : obtenir par le discours un gain dans le conflit en épargnant ses hommes et ses moyens.

[5] La météo exécrable pendant les premiers jours de l'offensive allemande paralyse l'armée américaine incapable de localiser avec ses moyens aériens bloqués au sol les unités de la Wermacht et leurs axes de progression.

BIBLIOGRAPHIE

BAILLARGEON, Normand, (2006), *Petit cours d'autodéfense intellectuelle*, Luxe éditeur.
BEEVOR, Anthony, (2015), *La bataille des Ardennes*, Calmann Levy.
BEURNEZ, Victoria, (2022), *BFM Business*, disponible en ligne : https://www.bfmtv.com/tech/piratee-une-chaine-d-information-ukrainienne-diffuse-un-deepfake-de-volodymyr-zelensky_AN-202203170296.html.
BOULANGER, Philippe, (2025), *Ukraine, géostratégie d'une guerre moderne*, Paris, Armand Colin.
BRETON, Philippe, (2000), *La parole manipulée*, Paris, la Découverte.
BRONNER, Gérald, (2013), *La démocratie des crédules*, PUF.
CAPRON, Alexandre, (2024), *Fake News*, Mardaga.
CERVERA-MARZAL, (2019), *Post-vérité. Pourquoi il faut s'en réjouir*, *Le bord de l'eau*, La bibliothèque du Mauss.
CHARAUDEAU, Patrick, (2020), *La manipulation de la vérité. Du triomphe de la négation aux brouillages de la post-vérité*, Limoges, Lambert-Lucas
CHEKINOV, S.G., et BOGDANOV, S.A., "The Nature and Content of a New-Generation War", dans *Military Thought,* disponible en ligne : https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf.
CIALDINI, Robert, (2014), *Influence et manipulation,* 3e édition, Poche.
CLAUSEWITZ, (2014), *De la guerre,* Rivages, Poches.
COLON, David, (2019), *Propagande. La manipulation de masse dans le monde contemporain*, Belin.
COLON, David, (2023), *La guerre de l'information*, Taillandier.
DABILA, Antony, (2025), *L'échiquier stratégique*, Seuil
DANET DIDIER, Doaré, et RONAN, Malis Christian, (2015), L*'action militaire terrestre de A à Z,* Economica.
DIEGUEZ, Sebastian, (2018), *Total bullshit ! Au coeur de la post-vérité*, PUF.
DUGOIN-CLÉMENT, Christine, (2025), *Géopolitique de l'ingérence russe*, PUF.
DUGOIN-CLÉMENT, Christine, (2023), *L'Opinion*, 3 juillet, disponible en ligne : https://theconversation.com/operation-doppelganger-quand-la-desinformation-russe-vise-la-france-et-dautres-pays-europeens-208071.
ELLUL, Jacques, (1990), *Propagandes,* Ed. Economica.
FIBERMART, Patrick X., (2025), *Qu'est-ce que la fibre optique pour drones UAV/FPV ? Comment l'utiliser ?*, disponible en ligne : https://www.fiber-mart.com/fr/news/what-is-uavfpv-drone-optical-fiber-how-to-use-it-a-6611.html.
FORCADE, Olivier, (2016), *La Censure en France pendant la Grande Guerre*, Fayard.
FOUILLET, Thibault, (2023), *La guerre au XXIe siècle*, Ed du Rocher.
GENEVRIER, Gregory, et FOURT, Olivier, (2024), « Attentat de Moscou : le drame n'échappe pas aux fausses informations », in *RFI*, disponible en ligne : https://www.rfi.fr/fr/europe/20240325-attentat-de-moscou-le-drame-n-%C3%A9chappe-pas-aux-fausses-informations.
GOYA, M., (2014), *Sous le feu. La mort comme hypothèse de travail*, Tallandier.
GUCKERT, Elié, (2023), *Comment Poutine a conquis nos cerveaux*, Plon.
GUÉGUEN, Nicolas. (2002), *Psychologie de la manipulation et de la soumission*, Dunod.
HECKER, Marc, TENENBAUM, Elie, (2022), *La guerre de vingt ans*, Robert Laffont.
HÉMEZ, Rémy, (2022), *Ruses et stratagèmes de guerre in les opérations de déception*, Perrin.
https://en.wikipedia.org/w/index.php?title=Crocus_City_Hall_attack&section=14&oldid=1331055619&action=edit
https://en.wikipedia.org/wiki/Crocus_City_Hall_attack
https://en.wikipedia.org/wiki/Disinformation_in_the_Russian_invasion_of_Ukraine
https://www.franceinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-de-fausses-videos-generees-par-ia-pretendent-montrer-une-reddition-massive-de-soldats-ukrainiens_7607642.html

https://www.opensanctions.org/entities/NK-nB5tLveacbaovVHsyrPBd9/
https://www.vie-publique.fr/en-bref/297500-guerre-en-ukraine-les-strategies-de-desinformation-russes-par-viginum
HUYGHE, François-Bernard, (2016), *La guerre de l'information*, PUF.
JOULE, Robert Vincent, et BEAUVOIS, Jean Léon, (2024), *Petit traité de manipulation à l'usage des honnêtes gens*, Nouvelle édition augmentée et actualisée, PUF.
JOUX, Alexandre, (2023), *Journalisme et post-vérité* CNRS Coll., Les essentiels d'Hermès.
KAHNEMAN, Daniel, (2023), *Noise,* Ed. Odile Jacob.
LAMIZET, Bernard, (2006), *La sémiotique de l'événement*, Eyrolles.
LASCAR, Olivier, (2024), *Deep Fake L'IA au service du faux,* Eyrolles.
LETONTURIER, Eric, (2017), *Guerres armées et communication*, CNRS Coll. Les essentiels d'Hermès.
LIMONIER, Kevin, (2025) "A Social Design Agency, une structure clé de la désinformation russe, avec Kevin Limonier", dans *IFG*, disponible en ligne : https://www.geopolitique.net/la-social-design-agency-une-structure-cle-de-la-desinformation-russe-avec-kevin-limonier/.
LITS, Marc, (2008), *Du récit au récit médiatique*, Bruxelles De Boeck.
LOPEZ, Jean, (2023), *L'Armée Rouge*, Perrin.
MARANGÉ, Céline & QUESSARD, Maud, (2021), *Les guerres de l'information à l'ère numérique*, PUF.
MAUD, Marangé, et MAUD, Quessard, (2021), *Les guerres de l'information à l'ère numérique*, PUF.
MINIC, Dimitri, (2023), *Pensée et culture stratégique russe*, EMSH.
MUCCHIELLI, (1998), *Théorie des processus de la communication*, Armand Colin.
NAFFI, Nadia, et alii, (2024), *Désinformation amplifiée par l'IA : incidents médiatisés, régulations et technologies pour contrer les manipulations par hyper trucages*, Projet de la CLE en collaboration avec l'Obvia, l'Université Laval, disponible en ligne : https://www.obvia.ca/sites/obvia.ca/files/ressources/202411-OBV-Pub-Desinformation_Amplifiee_IA_0.pdf.
PETIT, Clara, (2025), *La guerre cognitive*, DEF Tech.
QIAO Liang, et WANG, Xiangsui, (2006), *La guerre hors limites*, Editions Payot et Rivages Poche.
QUÉTEL, Claude, (2022), *Les opérations les plus extraordinaires de la Seconde Guerre mondiale*, Paris, Perrin.
SKOVE, Sam, (2024), "How Army special operators use deepfakes and drones to train for information warfare. One soldier helped create a voice-cloning program using off-the-shelf AI", dans *Defense One*, April 18, disponible en ligne : https://www.defenseone.com/technology/2024/04/how-army-special-operators-use-deepfakes-and-drones-train-information-warfare/395852/.
TANDOC, E. C. Jr., LIM, Z. W., & LING, R., (2018), "*Defining "Fake News*"", dans *Digital Journalism*, 6(2), pp. 137-153.
TCHAKHOTINE, Serge, (1952), *Le viol des foules par la propagande politique*, Tel Gallimard.
TIERCELIN, Alex, et TIERCELIN, Claudine, (2023), *La post-vérité ou le dégout du vrai*, Intervalles.
TWOMEY, John, and alli, (2023), "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine", dans *PLOS One*, October 25, disponible en ligne : https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0291668.
TZU, Sun, (2017), *L'art de la guerre aphorisme 17*, Champs Flammarion.
WATZLAWICK, Paul, (1988), *L'invention de la réalité*, Essai Points Seuil.