

*Guerre cognitive et guerre cognitive*  
*Analyse intégrée des mécanismes neurobiologiques et informationnels*

Patrice Cardot

Juillet 2026

## Exposé des motifs

Ce document comble un vide doctrinal critique en proposant la première analyse systémique et intégrée des guerres cognitive (neurobiologique) et cognitive (informationnelle) — deux modalités souvent confondues, mais ontologiquement distinctes, dont la synergie redéfinit les conflits modernes.

Il cartographie leurs mécanismes technologiques, psychologiques et scientifiques sous-jacents (neurobiologiques, algorithmiques, physiques), leurs synergies opérationnelles et leurs implications géopolitiques dans le cadre des guerres hybrides, tout en proposant des contre-mesures multidimensionnelles (neuroprotection, éducation cognitive, cybersécurité).

## Résumé exécutif

### Guerre cognitive et cognitive – Les mécanismes d’une révolution conflictuelle irréversible

La guerre moderne a opéré un basculement stratégique : l’esprit humain est devenu le champ de bataille décisif. Ce document établit une distinction ontologique entre guerre cognitive (neurobiologique, *bottom-up*) et guerre cognitive (informationnelle, *top-down*), deux modalités complémentaires dont la synergie crée un effet multiplicateur ( $\times 3-5$  selon l’OTAN-STO). Leur irréversibilité est désormais actée, les grandes puissances ayant sciemment franchi les seuils éthiques et juridiques pour militariser neurosciences et IA.

Mécanismes technologiques : La guerre cognitive exploite l’IA générative (*deepfakes* via Sora 2.0, GANs, *Diffusion Models*), les réseaux de bots (15–20 % des comptes Twitter/X en 2026) et les algorithmes de recommandation (YouTube, TikTok) pour manipuler les flux informationnels. La guerre cognitive déploie des *neuroweapons* (ondes EM 1–10 GHz comme le *Moscow Signal*), des interfaces cerveau-machine (BCI comme Neuralink) et des nanoneurotechnologies (projet NANO de la DARPA).

Mécanismes scientifiques : Ces technologies ciblent les vulnérabilités neurobiologiques : modulation des neurotransmetteurs (dopamine pour la dépendance, sérotonine pour l’humeur, noradrénaline pour la peur), perturbation des ondes cérébrales (thêta 4–8 Hz pour la suggestibilité, bêta 12–30 Hz pour la concentration), et exploitation de la plasticité synaptique (LTP/LTD) pour implanter des faux souvenirs. Le modèle des 3 mondes (physique, informationnel, cognitif) et les 4 stades de dégradation cognitive (exposition → pénétration → ancrage → dégénérescence) structurent cette approche systémique, tandis que l’architecture cérébrale hiérarchisée (niveaux autonome, psycho-affectif, cognitif supérieur) révèle des cibles précises pour chaque vecteur.

Mécanismes psychologiques : La guerre cognitive amplifie les biais cognitifs (confirmation, Dunning-Kruger, négativité) via les plateformes numériques, tandis que la guerre cognitive exploite les vulnérabilités structurelles (limites de la mémoire, de l’attention), fonctionnelles (biais, raccourcis mentaux), dynamiques (fatigue, stress) et contextuelles (polarisation sociétale). Les états modifiés de conscience (méditation, transe, hypnose) offrent des fenêtres de vulnérabilité accrues.

Synergie et irréversibilité : L’intégration de ces deux modalités dans les guerres hybrides crée une menace systémique. Leur synergie permet de contourner les défenses traditionnelles : la guerre cognitive sature l’espace informationnel, réduisant les capacités critiques, tandis que la guerre cognitive altère directement les processus cérébraux. Les études de cas (syndrome de La Havane, projets DARPA, opérations russes en Ukraine) confirment leur déploiement opérationnel. Leur irréversibilité est scellée par cinq dynamiques : avantage stratégique décisif, absence de cadre juridique, militarisation de la société civile, absence de contre-mesures universelles, et absence de volonté politique pour une régulation éthique.

Enjeux stratégiques et contre-mesures : Ces armes, furtives, économiques et accessibles à des acteurs non étatiques, menacent la souveraineté mentale des individus et des nations. Elles créent un risque de déstabilisation des démocraties (érosion de la confiance dans les institutions, polarisation sociale, manipulation des élections) et de contrôle comportemental de masse. Face à cette menace multidimensionnelle, une défense intégrée est indispensable : neuroprotection (blindage EM, détection des ondes, antidotes), éducation cognitive (littératie médiatique, pensée critique), cybersécurité

(détection des *deepfakes*, filtrage des bots), résilience économique et coopération internationale pour encadrer ces technologies. L'UE, en retard, doit accélérer sa souveraineté technologique pour éviter une dépendance stratégique.

Conclusion : L'enjeu n'est plus de savoir *si* ces guerres domineront le XXI<sup>e</sup> siècle, mais *comment* y résister sans sacrifier nos valeurs. La maîtrise de ces mécanismes technologiques, scientifiques et psychologiques sera déterminante pour préserver l'autonomie mentale des individus et la stabilité des sociétés.

Nb : Cette analyse a été réalisée avec l'appui technique du Chat Vibe de *Mistral AI* pour la recherche en sources ouvertes disponibles sur le web sur la base de requêtes précises, permettant l'élaboration méthodique d'une synthèse approfondie et structurée des très nombreux documents analysés.

Les opinions exprimées restent bien évidemment celles de l'auteur et n'engagent que sa responsabilité.

## Sommaire

### Lexique global (pages 4 – 8)

Fondement terminologique.

### Introduction générale (p. 9 – 10)

Contexte historique et urgence doctrinale.

### Chapitre I – Cadre théorique (p. 10 - 34)

Distinction et complémentarité des deux guerres.

- Processus cognitifs et vulnérabilités : cartographie des mécanismes ciblés.
- Guerre cognitive vs. guerre cognitique : cerveau (bottom-up) vs. esprits (top-down).
- Complémentarité et synergie : effet multiplicateur (×3-5).

### Chapitre II – Dynamiques opérationnelles (p. 34 – 41)

Mécanismes concrets et enjeux géopolitiques.

- Mécanismes opérationnels : préparation (cognitive) + amplification (cognitive).
- Enjeux géopolitiques : menace pour la souveraineté mentale.
- Implications stratégiques : défense intégrée.

### Chapitre III – Fondements scientifiques (p. 41 – 67)

Mécanismes et technologies.

- Cerveau comme champ de bataille : architecture vulnérable (3 niveaux).
- Technologies offensives : vecteurs : *neuroweapons*, IA, *deepfakes*, bots, drogues.
- Contre-mesures : détection, neuroprotection, authentification, IA défensive.
- Verrous scientifiques : limites physiques, technologiques, éthiques.

### Chapitre IV – Position dans les guerres hybrides (p. 67 – 79)

Intégration dans les conflits modernes.

- Cartographie stratégique : positionnement dans les 5 dimensions.
- Cartographie géopolitique : capacités par acteur.
- Implications stratégiques : défense intégrée et proactive.
- Scénarios d'avenir : escalade, régulation, domination cognitive.

## Chapitre V – L'irréversibilité des processus de guerre cognitive et cognitive dans un monde sans contraintes éthiques (p. 80 – 102)

Analyse exhaustive des pistes de recherche mondiales et des dynamiques structurelles.

- Les pistes de recherche mondiales en 2026 : état de l'art.
- L'irréversibilité des processus : pourquoi le retour en arrière est impossible.
- L'affranchissement des contraintes éthiques, morales et juridiques : une normalisation en marche.
- Études de cas : l'irréversibilité en action.
- Perspectives : vers une guerre cognitive et cognitive permanente et normalisée.
- Scénarios d'avenir : vers une guerre hybride totale ?

## Chapitre VI – Conclusion : La guerre cognitive et la guerre cognitive comme piliers des conflits modernes (p. 101 - 103)

Synthèse des enseignements et implications stratégiques : cinq enseignements clés ; implications pour la défense et la stratégie.

## Annexe A : Phénomènes électromagnétiques, lumineux et autres vecteurs d'influence cognitive (p. 104 - 118)

Une analyse comparative des mécanismes d'action sur le cerveau et les états de conscience.

## Annexe B : Analyse des ondes électromagnétiques des systèmes de télécommunication à distance : fréquences, applications et risques sanitaires (p. 119 - 138)

Cette analyse complète la précédente bien que ces systèmes de télécommunication à distance ne puissent pas être considérés *a priori* comme présentant des menaces relevant des guerres cognitive et cognitive.

### Lexique global : vers un langage commun et précis

Fondement terminologique indispensable pour éviter les ambiguïtés conceptuelles, ce lexique standardisé établit un langage commun entre experts, militaires et décideurs, tout en démystifiant des termes souvent galvaudés. *Exemple* : La distinction entre *plasticité cérébrale* (cible de la guerre cognitive) et *biais cognitifs* (exploités par la guerre cognitive) illustre la complémentarité des deux approches.

### Termes liés à la guerre cognitive (neurobiologique)

| Terme                     | Définition                                                                                                    | Application en Guerre Cognitive                                                         | Exemple                                                  | Source                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|
| <b>Neuroweapon</b>        | Arme conçue pour cibler directement le cerveau via ondes électromagnétiques, ultrasons ou produits chimiques. | Attaque directe : contrôle des émotions, dégradation des capacités cognitives.          | <i>Moscow Signal</i> (1972–1989).                        | Zaret, M. M. (1979). DOI:10.1080/00222737.1979.11689201. |
| <b>Neurotransmetteurs</b> | Molécules (dopamine, sérotonine, noradrénaline, GABA, glutamate) transmettant les signaux entre neurones.     | Modulation de l'humeur, de la mémoire ou de la prise de décision via neurotechnologies. | Ondes EM stimulant la noradrénaline → induction de peur. | Bear, M. F., et al. (2016). ISBN: 978-1451109551.        |
| <b>BCI</b>                | Interface permettant une communication directe entre le cerveau et un dispositif externe.                     | Lecture des pensées, influence des décisions, contrôle mental.                          | <i>Neuralink</i> (Elon Musk).                            | Nicolelis, M. A. L. (2011). ISBN: 978-0805088910.        |

| Terme                        | Définition                                                                                        | Application en Guerre Cognitive                                                                      | Exemple                                                             | Source                                   |
|------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------|
| <b>Plasticité cérébrale</b>  | Capacité du cerveau à se réorganiser via de nouvelles connexions synaptiques ou neurones.         | Imposition de nouveaux schémas mentaux ou dégradation de la capacité d'apprentissage contradictoire. | Campagne de propagande répétée modifiant durablement les croyances. | Claverie & Prébot (2026).                |
| <b>Ondes cérébrales</b>      | Activité électrique du cerveau, classées par fréquence (delta, thêta, alpha, bêta, gamma).        | Perturbation pour désorganiser les processus cognitifs.                                              | Ondes thêta (4–8 Hz) associées à la relaxation.                     | Bear, M. F., et al. (2016).              |
| <b>Effet Frey</b>            | Phénomène où des ondes EM (1–10 GHz) induisent des sons audibles directement dans le cerveau.     | Communication subliminale ou désorientation.                                                         | Projet <i>Pandora</i> (CIA, 1965–1970).                             | Frey, A. H. (1961).                      |
| <b>Neurostimulation</b>      | Utilisation de stimuli électriques, magnétiques ou optiques pour moduler l'activité neuronale.    | Modulation ciblée des circuits neuronaux (émotions, mémoire, prise de décision).                     | TMS pour traiter la dépression.                                     | George, M. S., & Aston-Jones, G. (2010). |
| <b>BZ</b>                    | 3-Quinuclidinyl Benzilate, antagoniste de l'acétylcholine provoquant hallucinations et amnésie.   | Désorientation des troupes, interrogatoires.                                                         | Projet <i>Operation Third Chance</i> (US Army, 1960–1970).          | Ketchum, J. S. (2006).                   |
| <b>LSD</b>                   | Agoniste de la sérotonine provoquant hallucinations et altération de la perception.               | Manipulation sensorielle, interrogatoires.                                                           | Projet <i>MKUltra</i> (CIA, 1953–1973).                             | Nichols, D. E. (2016).                   |
| <b>Scopolamine</b>           | Antagoniste de l'acétylcholine provoquant amnésie antérograde.                                    | Manipulation des souvenirs, interrogatoires.                                                         | "Droque du violeur" (Colombie).                                     | Ketchum, J. S. (2006).                   |
| <b>Nanoneurotechnologies</b> | Utilisation de nanorobots pour interagir avec les neurones à l'échelle moléculaire.               | Espionnage neuronal, manipulation des émotions/mémoire.                                              | Projet <i>NANO</i> (DARPA, 2020).                                   | Rapports DARPA (2020–2026).              |
| <b>TMS</b>                   | Stimulation magnétique transcrânienne (non invasive).                                             | Modulation de l'humeur, traitement de la dépression.                                                 | Dépression résistante.                                              | George, M. S., & Aston-Jones, G. (2010). |
| <b>LIFU</b>                  | <i>Low-Intensity Focused Ultrasound</i> : ultrasons focalisés pour stimuler des zones cérébrales. | Stimulation cérébrale ciblée (mouvements, hallucinations).                                           | Projet <i>Neural Disruptor</i> (DARPA).                             | Legon, W. (2014).                        |

### Termes liés à la guerre cognitive (informationnelle)

| Terme           | Définition                                                   | Application en Guerre Cognitive                                | Exemple                                      | Source                            |
|-----------------|--------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------|-----------------------------------|
| <b>Deepfake</b> | Contenu audio/vidéo synthétique hyperréaliste généré par IA. | Création de fausses preuves pour manipuler l'opinion publique. | Vidéo <i>deepfake</i> du Président français. | Chesney, R., & Citron, D. (2019). |

| Terme                                | Définition                                                                                        | Application en Guerre Cognitive                                   | Exemple                                           | Source                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------|
| <b>Biais cognitifs</b>               | Distorsions systématiques du jugement humain.                                                     | Amplifiés par les algorithmes pour polariser les opinions.        | YouTube favorise les contenus extrêmes.           | Kahneman, D. (2011). ISBN: 978-0374275631.     |
| <b>Biais de confirmation</b>         | Tendance à privilégier les informations confirmant ses croyances.                                 | Renforcement des bulles idéologiques.                             | Réseaux sociaux.                                  | Kahneman, D. (2011).                           |
| <b>Biais de Dunning-Kruger</b>       | Tendance des individus peu compétents à surestimer leurs capacités.                               | Fausse confiance dans la détection des <i>deepfakes</i> .         | Partage de <i>deepfakes</i> par des utilisateurs. | Dunning, D. (2011).                            |
| <b>Biais de négativité</b>           | Tendance à accorder plus d'importance aux informations négatives.                                 | Amplification des <i>fake news</i> anxiogènes.                    | Campagnes de désinformation russes.               | Rozin, P., & Royzman, E. B. (2001).            |
| <b>Effet de simple exposition</b>    | Tendance à préférer ce qui est familier, même si c'est faux ou nuisible.                          | Répétition de fausses informations pour les ancrer.               | <i>Fake news</i> répétées.                        | Zajonc, R. B. (1968).                          |
| <b>Bulle filtrante</b>               | Phénomène où les algorithmes montrent des informations confirmant les croyances de l'utilisateur. | Enfermement dans des réalités informationnelles personnalisées.   | Facebook, YouTube, TikTok.                        | Pariser, E. (2011). ISBN: 978-1594203008.      |
| <b>IA générative</b>                 | Modèles capables de générer des textes, images ou vidéos de manière autonome.                     | Création massive et personnalisée de contenus manipulés.          | GPT-4, Llama 3, Sora.                             | Ho et al. (2020), Brown et al. (2020).         |
| <b>Réseaux de bots</b>               | Comptes automatisés amplifiant la désinformation.                                                 | Inondation des plateformes de messages coordonnés.                | 15–20 % des comptes Twitter/X (2026).             | Ferrara, E. (2017). DOI:10.5210/fm.v22i5.7854. |
| <b>Algorithmes de recommandation</b> | Systèmes personnalisant les contenus en fonction des préférences des utilisateurs.                | Renforcement des biais cognitifs, polarisation.                   | YouTube, TikTok.                                  | Pariser, E. (2011).                            |
| <b>Métavers</b>                      | Univers virtuels persistants et partagés.                                                         | Création de réalités alternatives pour manipuler des populations. | Opérations psychologiques.                        | Rapports DARPA (2020–2026).                    |
| <b>Réalité virtuelle (VR)</b>        | Environnements numériques immersifs.                                                              | Contrôle intégral de la perception sensorielle.                   | <i>Deepfakes</i> en 3D.                           | Rapports DARPA (2020–2026).                    |
| <b>TTS</b>                           | <i>Text-to-Speech</i> : génération de voix synthétiques hyperréalistes à partir de texte.         | <i>Deepfakes</i> audio, usurpation vocale.                        | ElevenLabs, Murf.ai.                              | Rapports OpenAI (2024).                        |
| <b>STT</b>                           | <i>Speech-to-Text</i> : transcription automatique de la parole en texte.                          | Surveillance de masse, espionnage.                                | Whisper (OpenAI), Wav2Vec (Meta).                 | Rapports OpenAI (2024).                        |

## Termes transversaux

| Terme                       | Définition                                                                         | Application                                        | Exemple                                                          | Source                                                           |
|-----------------------------|------------------------------------------------------------------------------------|----------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Souveraineté mentale</b> | Capacité d'un individu ou d'un groupe à contrôler ses propres processus de pensée. | Enjeu central de la guerre cognitive et cognitive. | Perte de souveraineté via <i>neuroweapons</i> ou désinformation. | EGE (2024). <i>Cadre doctrinal</i> .                             |
| <b>Effet de contagion</b>   | Phénomène où un individu manipulé influence son groupe.                            | Amplification des effets de la guerre cognitive.   | Décideur désorienté affectant son équipe.                        | OTAN-STO (2024). <i>Contagion Effects in Cognitive Warfare</i> . |

| Terme                                     | Définition                                                                                           | Application                                                        | Exemple                                                 | Source                                  |
|-------------------------------------------|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------|
| <b>Conscience</b>                         | État de vigilance et d'éveil permettant de percevoir, ressentir, penser et agir de manière intégrée. | Cible ultime des attaques cognitives combinées.                    | Altération de la perception ou de la prise de décision. | Dehaene, S. (2014), Varela, F. (1991).  |
| <b>Accès conscient</b>                    | Capacité à manipuler l'information de manière délibérée.                                             | Ciblé par la guerre cognitive (désinformation, <i>deepfakes</i> ). | Désorientation informationnelle.                        | Dehaene, S. (2014).                     |
| <b>Expérience consciente</b>              | Sentiment subjectif d'être soi ( <i>qualia</i> ).                                                    | Ciblée par la guerre cognitive ( <i>neuroweapons</i> , drogues).   | Hallucinations, dépersonnalisation.                     | Chalmers, D. (1995).                    |
| <b>Intentionnalité</b>                    | Capacité à avoir des états mentaux dirigés vers des objets.                                          | Cible des attaques visant à contrôler les comportements.           | Manipulation des décisions.                             | Searle, J. (1983).                      |
| <b>États modifiés de conscience (EMC)</b> | États où la conscience s'éloigne de son état d'éveil normal (méditation, transe, hypnose).           | Fenêtres de vulnérabilité accrues aux attaques cognitives.         | Lavage de cerveau, hypnose.                             | Oakley, D. A. (2012), Vaitl, D. (2007). |
| <b>Méditation</b>                         | Pratique réduisant l'activité du réseau du mode par défaut (DMN).                                    | Résilience cognitive ou vulnérabilité accrue.                      | Programme <i>Mind Fitness Training</i> (US Army).       | Tang, Y. Y. (2015).                     |
| <b>Transe</b>                             | État de dissociation et de suggestibilité maximale.                                                  | Manipulation culturelle, lavage de cerveau.                        | Rituels chamaniques, sectes.                            | Vaitl, D. (2007).                       |
| <b>Hypnose</b>                            | État de désactivation partielle du sens critique et d'augmentation de la suggestibilité.             | Implantation de faux souvenirs, contrôle émotionnel.               | Projet <i>MKDelta</i> (CIA).                            | Oakley, D. A. (2012).                   |
| <b>Processus cognitifs</b>                | Opérations mentales (perception, mémoire, raisonnement, émotion, prise de décision).                 | Cibles des attaques cognitives et cognitives.                      | Désorientation, faux souvenirs.                         | Bear, M. F., et al. (2016).             |
| <b>Vulnérabilités structurelles</b>       | Faibles liées à la structure du cerveau (plasticité, connectivité, neurotransmetteurs).              | Exploitées par les <i>neuroweapons</i> ou drogues.                 | Implantation de faux souvenirs.                         | Claverie & Prébot (2026).               |
| <b>Vulnérabilités fonctionnelles</b>      | Faibles liées aux fonctions cognitives (biais, limites de la mémoire, attention).                    | Exploitées par la désinformation et les algorithmes.               | Polarisation sociétale.                                 | Kahneman, D. (2011).                    |
| <b>Vulnérabilités dynamiques</b>          | Faibles liées aux états changeants (fatigue, stress, EMC).                                           | Exploitées pour amplifier les effets des attaques.                 | Panique collective.                                     | Claverie & Prébot (2026).               |
| <b>Vulnérabilités contextuelles</b>       | Faibles liées à l'environnement (polarisation, littératie cognitive, dépendance aux institutions).   | Exploitées pour fragmenter les sociétés.                           | Désintégration de la conscience collective.             | Sunstein, C. (2009).                    |
| <b>Vulnérabilités technologiques</b>      | Faibles liées aux outils numériques (IA, réseaux sociaux, BCI).                                      | Exploitées pour manipuler les processus cognitifs.                 | <i>Deepfakes</i> indétectables.                         | Rapports ANSSI (2023).                  |

### Technologies clés

| Technologie           | Définition                                                                 | Application                                         | Exemple                        | Source                  |
|-----------------------|----------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------|-------------------------|
| <b>Sora (OpenAI)</b>  | Modèle d'IA générative créant des vidéos hyperréalistes à partir de texte. | Création de <i>deepfakes</i> vidéo indétectables.   | Vidéos de 60 secondes.         | Rapports OpenAI (2024). |
| <b>GPT-4 (OpenAI)</b> | Modèle de langage de grande taille (LLM) générant du texte cohérent.       | Désinformation textuelle, <i>phishing</i> cognitif. | <i>Fake news</i> automatisées. | Ho et al. (2020).       |

| Technologie | Définition                                                                                       | Application                                           | Exemple                         | Source                      |
|-------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------|-----------------------------|
| ElevenLabs  | Modèle TTS générant des voix synthétiques hyperréalistes.                                        | Deepfakes audio, usurpation vocale.                   | Appels téléphoniques falsifiés. | Rapports ElevenLabs (2023). |
| Truepic     | Technologie de blockchain pour l'authentification des images et vidéos.                          | Preuve de l'intégrité des contenus médias.            | Certification des photos.       | Rapports C2PA (2023).       |
| Adobe CAI   | Content Authenticity Initiative : standard ouvert pour l'authentification des médias.            | Traçage de l'origine et de l'historique des contenus. | Métadonnées infalsifiables.     | Rapports Adobe (2023).      |
| C2PA        | Coalition for Content Provenance and Authenticity : standard pour l'authentification des médias. | Standardisation de l'authentification.                | Interopérabilité des outils.    | Rapports C2PA (2023).       |

### Concepts stratégiques et doctrinaux

| Concept                                      | Définition                                                                                                                                      | Application                                                                   | Exemple                                      | Source                                           |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------|
| Guerre hybride                               | Stratégie intégrée combinant plusieurs modalités (conventionnelle, irrégulière, cyberguerre, guerre de l'information, guerre économique).       | Cadre doctrinal pour comprendre les conflits modernes.                        | Stratégie russe en Ukraine (2014–2026).      | Rapports OTAN-STO (2024).                        |
| Guerre conventionnelle                       | Affrontements armés classiques entre États.                                                                                                     | Dimension traditionnelle des conflits.                                        | Guerre en Ukraine (2022–2026).               | Doctrines militaires classiques.                 |
| Guerre irrégulière                           | Actions menées par des acteurs non étatiques ou des tactiques non conventionnelles.                                                             | Guerre asymétrique via proxies.                                               | Soutien iranien aux Houthis (Yémen).         | Doctrines militaires modernes.                   |
| Cyberguerre                                  | Ciblage des systèmes informatiques pour perturber, espionner ou neutraliser un adversaire.                                                      | Attaques contre les infrastructures critiques.                                | BlackEnergy (Ukraine, 2015).                 | Rapports ANSSI (2023).                           |
| Guerre de l'information                      | Manipulation des flux d'information pour influencer les perceptions et les décisions.                                                           | Désinformation, propagande, manipulation algorithmique.                       | Campagnes russes (2016–2024).                | Rapports OTAN-STO (2024).                        |
| Guerre économique                            | Utilisation de leviers économiques pour affaiblir un adversaire.                                                                                | Déstabilisation des marchés et des chaînes d'approvisionnement.               | Sanctions contre la Russie (2022).           | Harbulot, C. (2021).                             |
| Effet de résonance cognitive                 | Amplification des effets lorsque guerre cognitive et guerre cognitive sont combinées.                                                           | Désorientation exponentielle des cibles.                                      | Opération Éclipse (scénario OTAN-STO).       | OTAN-STO (2024).                                 |
| Modèle des 4 stades de dégradation cognitive | Modèle décrivant la progression des attaques cognitives (Exposition → Pénétration → Ancrage → Dégénérescence).                                  | Compréhension de la dynamique des attaques et adaptation des contre-mesures.  | Attaques combinées deepfakes + neuroweapons. | Adapté des travaux en neurosciences (2020–2026). |
| Modèle des 3 mondes                          | Cadre proposant que la guerre cognitive opère à l'intersection du monde physique, informationnel et cognitif.                                   | Feuille de route pour la défense intégrée.                                    | Neuroprotection + éducation cognitive.       | Claverie & Prébot (2026).                        |
| Modèle des 5 dimensions des guerres hybrides | Cadre décomposant les guerres hybrides en 5 dimensions : conventionnelle, irrégulière, cyberguerre, guerre de l'information, guerre économique. | Positionnement des guerres cognitive et cognitive dans les conflits modernes. | Synergies entre les dimensions.              | Rapports OTAN-STO (2024).                        |

## Introduction générale

Plaçant la « *guerre cognitive* » comme 6<sup>ème</sup> domaine opérationnel, l'OTAN considère désormais le cerveau humain comme un *champ de bataille stratégique*, avec des tactiques visant à modifier non pas *ce que* pensent les individus, mais *comment* ils pensent. Les neurosciences militarisées et les technologies convergentes de type NBIC (nano, bio, info, cognitif) y jouent un rôle central, comme le souligne le rapport "*Cognitive Warfare*" (2021) de l'*Innovation Hub* de l'OTAN, qui évoque explicitement la manipulation cognitive à grande échelle via les Big Data et l'IA.

En France, l'Etat major des Armées a intégré cette dimension dans sa stratégie interarmées 2021, soulignant que la guerre cognitive est « *la clé de voûte des conflictualités hybrides* ». Le CEMA d'alors, le Général d'Armée Thierry Burkhard soulignant que la guerre cognitive est « *la clé de voûte des conflictualités hybrides* ».

En Chine, l'Armée populaire de libération a fait de la guerre cognitive un pilier de sa doctrine militaire. Selon Paul Charon (chercheur à l'IRSEM), Pékin développe des capacités pour « *contrôler les cerveaux* » de ses adversaires, via des ondes électromagnétiques, des campagnes d'influence ciblées, ou des technologies de manipulation cognitive. Le « *syndrome de La Havane* » (2016), où des diplomates américains ont souffert de symptômes neurologiques après une exposition à des ondes, est souvent cité comme un exemple de concrétisation de cette guerre.

Aux États-Unis, la DARPA (agence de recherche du Pentagone) finance depuis des décennies des programmes visant à développer des BCI haute résolution pour des applications militaires (amélioration des soldats, communication silencieuse, etc.). En 2023, la DARPA a lancé le projet N3 (*Next-Generation Nonsurgical Neurotechnology*), pour des interfaces neuronales non invasives et déployables sur le champ de bataille.

La notion de « *guerre cognitive* » fait encore l'objet de nombreux débats dont rend partiellement compte Bettina Trabelsi Pep dans un article de référence publié sur un site officiel du ministère français des Armées :

*« Le terme « guerre cognitive » a été utilisé pour la première fois en 2017 par Vincent R. Stewart, directeur de la « Defense Intelligence Agency » américaine, lorsqu'il a déclaré que la guerre moderne était devenue une bataille cognitive. Pour lui, la guerre XXI<sup>e</sup> siècle consiste à manipuler l'espace décisionnel à travers une lutte pour l'information. Il n'a cependant jamais articulé de définition claire du concept qu'il a introduit, créant un flou sémantique et conceptuel autour du terme « guerre cognitive ».*

*Les différentes et principales considérations concernant la définition de la guerre cognitive sont les suivantes ; Libicki (1995) affirmait que la guerre de l'information se composait de sept éléments, à savoir : le commandement et le contrôle ; la guerre fondée sur le renseignement ; la guerre électronique ; la guerre psychologique ; la guerre du piratage (hacking) ; la guerre de l'information économique et la cyberguerre. Pour lui, la guerre cognitive se place dans la catégorie de la guerre psychologique.*

*Plusieurs chercheurs ont par la suite attesté que la dimension cognitive est un élément clé de l'espace informationnel. D'autres ont soutenu le fait que la guerre cognitive n'est pas limitée au cyberspace et à la guerre de l'information, mais peut être utilisée à travers des méthodes politiques.*

*Face à ces désaccords, Rogers, en 2021, déclarait que « l'amalgame entre la guerre de l'information opérationnelle et la guerre cognitive est une erreur de catégorie qui doit être traitée en premier lieu ».*

*En effet, la guerre de l'information se concentre sur le contrôle du flux de l'information et la guerre cognitive vise à contrôler les réactions des individus et des groupes à l'information présentée. Chaque type de guerre pourrait contenir l'élément d'influence et d'impact sur la cognition humaine, mais seule la guerre cognitive est spécifiquement dédiée au contrôle du cerveau et du cognitif en incorporant des neurosciences militarisées dans diverses pratiques.*

*Plus récemment, le rapport de l'OTAN sur l'avènement de l'aspect « cognitif » de la conduite de la guerre (2022) définissait la guerre cognitive comme « une forme de guerre non conventionnelle qui utilise des outils informatiques pour modifier le raisonnement cognitif de l'ennemi, exploiter les biais*

*cognitifs ou la pensée réflexive, provoquer des distorsions de la pensée, influencer la prise de décision et entraver les actions, avec des effets négatifs tant au niveau individuel qu'au niveau collectif. » »*

*« Le domaine de la manipulation de l'information à but militaire ou diplomatique n'est pas un nouveau phénomène. L'arme de l'information est un héritage de la guerre froide (on pourrait même remonter aux conflits mondiaux du début du XXe siècle) et depuis les années 1960, la notion de champ des perceptions fait partie du champ doctrinal des forces armées. De plus, les opérations de désinformation, déception et de manipulation à des fins militaires sont également documentées depuis plusieurs siècles, comme par exemple le télégramme d'Ems (1870) ou l'opération Mincemeat (1943), visant à manipuler les perceptions et le raisonnement cognitif de l'ennemi.*

*Ces opérations prouvent que la pensée stratégique est en partie une « science de l'autre » dans le sens où il est nécessaire d'acquérir une compréhension du mode de fonctionnement, raisonnement et contexte socio-politico-culturel de l'ennemi afin d'utiliser les bons outils pour le manipuler efficacement. » (Bettina Trabelsi Pep - *La guerre cognitive* – Note de recherche – Armée de Terre française<sup>1</sup>).*

D'autres chercheurs se sont également penchés sur cette nouvelle modalité de la guerre, notamment en France où notamment Bernard Claverie (École Nationale Supérieure de Cognitique, IMS UMR-5218 CNRS, Institut Polytechnique de Bordeaux) a développé depuis quelques années de nombreuses activités d'analyse et de recherche sur ce sujet novateur<sup>2</sup>.

En France, le concept générique de « *guerre cognitive* » est apparu en réalité au début des années 2000 dans le cadre spécifique de l'intelligence stratégique et économique, Christian Harbulot, directeur de l'Ecole de guerre économique (EGE), Nicolas Moine, Directeur du DESS Intelligence économique et Développement des entreprises de l'Université de Poitiers, et Dider Lucas, responsable du Développement du Laboratoire de recherche de l'EGE, en ayant les trois principaux penseurs et promoteurs<sup>3</sup>, bien avant que les milieux militaires n'y fassent référence.

Depuis lors, des avancées sémantiques, épistémologiques, polémologiques et opérationnelles ont conduit à distinguer la guerre cognitive et la guerre cognitique qui représentent deux facettes d'une même menace émergente, celle d'une manipulation systématique des processus mentaux à une échelle sans précédent.

Alors que le monde entre dans une ère où les technologies numériques et neurobiologiques se développent à un rythme exponentiel, et alors que les méthodes de guerre cognitive (au sens le plus large du terme) restent à ce jour en dehors du cadre légal international de ce que constitue un acte de guerre et permettent donc une utilisation non régularisée et non encadrée, ces deux modalités d'attaque — souvent confondues ou mal distinguées — nécessitent une clarification doctrinale, y compris en regard des autres composantes des guerres hybrides avec lesquelles elles entrent en synergie.

Ce document se propose donc d'éclairer ces concepts en démystifiant leurs mécanismes, de cartographier leurs synergies, et de proposer des contre-mesures adaptées, en s'appuyant sur une compréhension approfondie des vulnérabilités cérébrales qui en font la cible privilégiée des attaques cognitives, qu'elles soient neurobiologiques ou informationnelles.

## **I - Cadre théorique et définitions : Distinction et complémentarité entre guerre cognitive et guerre cognitique**

### **Introduction : Clarifier un champ sémantique complexe**

La guerre cognitive et la guerre cognitique sont deux concepts souvent confondus, mais dont la différence de nature est fondamentale. Alors que la première agit directement sur le cerveau (substrat biologique), la seconde cible les perceptions et les systèmes de pensée (substrat informationnel).

<sup>1</sup> Cf. Bettina Trabelsi Pep - [La guerre cognitive](#) - Ministère des Armées (octobre 2023)

<sup>2</sup> Cf. en particulier - [Guerre cognitive et influence psychologique](#) ou encore [La guerre cognitive de bas niveau : la guerre des cerveaux](#) (2024)

<sup>3</sup> Cf. Christian Harbulot, Nicolas Moinet et Didier Lucas - [La Guerre cognitive : A la recherche de la suprématie stratégique](#)

Cette distinction n'est pas qu'une question de sémantique : elle reflète deux paradigmes opératoires distincts, chacun avec ses mécanismes, ses vecteurs et ses objectifs propres.

Ce premier chapitre a pour ambition de :

1. Établir une distinction nette entre ces deux modalités ;
2. Définir avec précision chaque concept, leurs mécanismes et leurs implications ;
3. Montrer leur complémentarité et la manière dont leur combinaison amplifie les effets ;
4. Proposer un lexique unifié pour éviter toute ambiguïté future.

Avant d'aborder les définitions proprement dites, il est essentiel de comprendre les processus et fonctions en jeu, et en particulier ce qui rend le cerveau humain vulnérable aux attaques cognitives.

## **I-1. Les processus cognitifs et les vulnérabilités cérébrales : fondements des attaques cognitives**

L'absence d'une caractérisation systématique et approfondie des processus cognitifs constitue une lacune majeure dans la plupart des analyses sur la guerre cognitive. Ces processus sont pourtant le substrat même des attaques cognitives et cognitives, et leur compréhension fine est indispensable pour en saisir les mécanismes, les vulnérabilités et les contre-mesures.

### **I-1.1 Les processus cognitifs : fondements et vulnérabilités du champ de bataille mental**

#### **Pourquoi les processus cognitifs sont-ils la clé de la guerre cognitive ?**

La guerre cognitive et la guerre cognitive ne ciblent pas des abstractions, mais des mécanismes concrets : les processus cognitifs, ces opérations mentales qui permettent au cerveau de percevoir, penser, décider et agir pour alimenter à la fois ce qu'Aristote qualifiait d'intellection réceptive et de d'intellection active.

Ces processus, bien que souvent perçus comme immatériels, reposent sur des substrats neurobiologiques précis et des mécanismes physiques mesurables.

Leur manipulation — qu'elle soit informationnelle ou neurobiologique — constitue l'arme ultime des conflits modernes, car elle permet de contrôler l'esprit lui-même.

Pourtant, malgré leur importance stratégique, les processus cognitifs restent mal définis dans la littérature sur la guerre cognitive.

Les documents existants se concentrent souvent sur les vecteurs d'attaque ou les effets observables (désinformation, polarisation), sans toujours remonter à la source : *comment* et *pourquoi* ces attaques fonctionnent.

Cette section comble ce vide en offrant une cartographie aussi exhaustive que possible en l'état actuel des connaissances sur ce sujet des processus cognitifs, de leur nature fondamentale à leurs vulnérabilités exploitables.

Cette analyse s'articule autour de cinq axes :

1. La nature des processus cognitifs (chimique, électrique, informationnelle)
2. Leurs fonctions (perception, mémoire, raisonnement, émotion, décision)
3. Leurs mécanismes sous-jacents (neurobiologie, physique, algorithmique)
4. Leurs vecteurs d'influence (naturels, technologiques, chimiques)
5. Leurs vulnérabilités (biais, plasticité, dépendances, limites physiologiques)

Cette démarche permet de démystifier la guerre cognitive en la ramenant à des réalités tangibles, et de préparer le terrain pour les sections suivantes sur les vulnérabilités cérébrales et les attaques.

#### **I-1.1.1 La nature des processus cognitifs : une architecture multi-dimensionnelle**

De manière schématique, nous pouvons appréhender les processus cognitifs comme des processus qui participent à la construction d'une intelligence et d'une pensée, les véritables cibles de ce que l'on

appelle de manière générique « *la guerre cognitive* » et qui recouvre en réalité plusieurs dimensions spécifiques distinctes.

Les processus cognitifs ne sont pas de simples abstractions philosophiques. Ils reposent sur une architecture physique et biologique complexe, où se croisent la chimie, l'électricité et l'information. Leur compréhension nécessite une approche interdisciplinaire, combinant neurosciences, physique et sciences de l'information.

### **A. Une nature neurobiologique : le cerveau comme machine chimique et électrique**

Au cœur des processus cognitifs se trouve le cerveau, un organe d'une complexité inégalée, composé de 86 milliards de neurones (cellules nerveuses) et de 100 000 milliards de synapses (connexions entre neurones). Chaque processus cognitif — qu'il s'agisse de la perception, de la mémoire ou de la prise de décision — repose sur des mécanismes neurobiologiques concrets :

*La transmission chimique* : Les neurones communiquent entre eux via des neurotransmetteurs, des molécules chimiques (dopamine, sérotonine, noradrénaline, GABA, glutamate) qui traversent les synapses pour transmettre des signaux. Ces molécules jouent un rôle clé dans la régulation des émotions, de la mémoire et de l'attention. *Exemple* : La dopamine est associée à la récompense et à la motivation, tandis que la sérotonine régule l'humeur et l'anxiété. Une modulation artificielle de ces neurotransmetteurs (via des drogues ou des ondes électromagnétiques) peut donc altérer radicalement les processus cognitifs.

*Les signaux électriques* : Les neurones génèrent et propagent des potentiels d'action, des impulsions électriques qui parcourent les axones (fibres nerveuses) à une vitesse pouvant atteindre 120 m/s. Ces signaux électriques sont à la base de la communication neuronale et, in fine, de la pensée. *Exemple* : Une stimulation électrique ciblée (via des électrodes ou des ondes EM) peut activer ou inhiber des zones cérébrales spécifiques, modifiant ainsi les processus cognitifs associés (ex. : induction de la peur via la stimulation de l'amygdale).

*Les ondes cérébrales* : L'activité électrique du cerveau génère des ondes cérébrales, mesurables par électroencéphalographie (EEG). Ces ondes, classées en fonction de leur fréquence (delta, thêta, alpha, bêta, gamma), reflètent différents états de conscience et processus cognitifs. *Exemple* : Les ondes thêta (4–8 Hz) sont associées à la relaxation et à la créativité, tandis que les ondes bêta (12–30 Hz) sont liées à la concentration et à la prise de décision. Une perturbation de ces ondes peut désorganiser les processus cognitifs.

### **B. Une nature informationnelle : le cerveau comme système de traitement de l'information**

Si les processus cognitifs ont une base neurobiologique, ils peuvent aussi être modélisés comme des systèmes de traitement de l'information. Cette approche, inspirée des sciences cognitives et de l'intelligence artificielle, permet de comprendre comment le cerveau acquiert, stocke, traite et transmet des données.

*L'acquisition de l'information* : Les processus cognitifs commencent par la perception, c'est-à-dire la collecte d'informations via les sens (vue, ouïe, toucher, etc.). Ces informations sont ensuite filtrées et interprétées par le cerveau. *Exemple* : La vision implique la détection de la lumière par la rétine, suivie de son traitement par le cortex visuel. Une manipulation de cette perception peut donc tromper le cerveau et altérer les processus cognitifs en aval.

*Le stockage de l'information* : La mémoire permet de conserver les informations perçues. Elle se divise en plusieurs types : mémoire sensorielle (très courte durée, ex. : image résiduelle) ; mémoire à court terme (quelques secondes à minutes, ex. : retenir un numéro de téléphone) ; mémoire à long terme (durable, ex. : souvenirs d'enfance). *Exemple* : La mémoire à long terme repose sur des modifications structurelles des synapses (plasticité synaptique). Une manipulation de ces mécanismes peut donc altérer les souvenirs ou implanter de faux souvenirs.

*Le traitement de l'information* : Le cerveau analyse, compare et combine les informations stockées pour en extraire du sens. Ce traitement repose sur des algorithmes naturels (ex. : reconnaissance de formes, détection de patterns). *Exemple* : Le cortex préfrontal joue un rôle clé dans le raisonnement et la prise

de décision. Une surcharge informationnelle (via la désinformation ou les réseaux sociaux) peut saturer ces capacités, rendant le cerveau moins capable de distinguer le vrai du faux.

*La transmission de l'information* : Les processus cognitifs incluent aussi la communication des informations, que ce soit via le langage, les gestes ou les expressions faciales. Cette transmission peut être manipulée pour influencer les autres. *Exemple* : Les algorithmes de recommandation amplifient sélectivement certaines informations, créant des bulles informationnelles qui limitent la diversité des idées auxquelles un individu est exposé.

### C - Le cerveau : une architecture complexe mais exploitable

Le cerveau humain est un système d'une complexité inégalée, capable de raisonnement abstrait, de créativité et d'adaptation. Pourtant, cette même complexité recèle des vulnérabilités structurelles qui en font une cible idéale pour les attaques cognitives, qu'elles soient neurobiologiques ou informationnelles.

Les mécanismes naturels qui font la force du cerveau (plasticité, biais cognitifs) sont aussi ses principales vulnérabilités.

| Terme                       | Définition                                                                                                                                         | Application en Guerre Cognitive                                                                             | Exemple Concret                                                                                                                   |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Plasticité cérébrale</b> | Capacité du cerveau à se réorganiser via de nouvelles connexions synaptiques ou neurones. Mécanisme à la base de l'apprentissage et de la mémoire. | Exploitée pour imposer de nouveaux schémas mentaux, ou dégrader la capacité d'apprentissage contradictoire. | Campagne de propagande répétée pendant des mois modifiant durablement les croyances politiques d'une population.                  |
| <b>Biais cognitifs</b>      | Distorsions systématiques du jugement humain (confirmation, Dunning-Kruger, négativité).                                                           | Amplifiés par les algorithmes pour polariser les opinions et rendre les individus plus vulnérables.         | Les algorithmes de YouTube ou TikTok favorisent les contenus extrêmes, renforçant les biais tout en maximisant l'engagement.      |
| <b>Neurotransmetteurs</b>   | Molécules (dopamine, sérotonine, noradrénaline, GABA, glutamate) transmettant les signaux entre neurones.                                          | Ciblés par les neurotechnologies pour moduler humeur, mémoire ou prise de décision.                         | <i>Neuroweapons</i> utilisant des ondes électromagnétiques pour stimuler la noradrénaline et induire un état de peur généralisée. |
| <b>Mémoire épisodique</b>   | Mémoire des événements vécus, liée à l'hippocampe. Essentielle pour la construction de l'identité.                                                 | Manipulée via deepfakes + récits répétés pour implanter de faux souvenirs.                                  | <i>Deepfake</i> montrant un politique dans une situation compromettante, diffusé massivement, créant un faux souvenir collectif.  |
| <b>Cognition sociale</b>    | Processus mentaux liés aux interactions sociales (empathie, théorie de l'esprit).                                                                  | Déstabilisée par la désinformation, qui érode la confiance et fragmente la cohésion sociale.                | Campagnes de fake news sapant la confiance dans les médias traditionnels, créant un climat de méfiance généralisée.               |
| <b>État de conscience</b>   | Niveau d'éveil et de réactivité du cerveau (éveil, sommeil, transe).                                                                               | Perturbé par des technologies spécifiques (fréquences sonores, stimuli visuels).                            | Fréquences binaurales induisant un état de relaxation profonde, rendant les individus plus réceptifs à la suggestion.             |

Ce tableau révèle que le cerveau humain n'est pas une forteresse impénétrable. Au contraire, il est naturellement vulnérable à la manipulation, précisément à cause des mécanismes qui font sa force.

*Trois implications majeures :*

1. La guerre cognitive exploite des mécanismes naturels : la plasticité, qui permet l'apprentissage, peut être détournée pour imposer des croyances erronées.
2. Les biais cognitifs sont des failles structurelles : amplifiés par les algorithmes, ils deviennent des leviers de manipulation puissants.
3. Les contre-mesures doivent être multidimensionnelles : il faut protéger le cerveau (éducation, neuroprotection) autant que les infrastructures numériques (détection, blockchain).

Comprendre ces vulnérabilités est la clé pour développer des stratégies de défense efficaces.

## De l'organisation hiérarchique du cerveau aux failles exploitables

Les travaux de Bernard Claverie et Baptiste Prébot ont mis en lumière une architecture cérébrale hiérarchisée, où chaque niveau présente des vulnérabilités spécifiques exploitables par les attaques cognitives.

Cette organisation, bien que source de la plasticité et de l'adaptabilité humaines, offre également des portes d'entrée pour la manipulation.

### Niveaux neurobiologiques et leurs vulnérabilités exploitables

| Niveau                                                   | Fonction principale                                     | Processus cognitifs associés                        | Vulnérabilités exploitables                                                 | Technologies d'attaque associées                                      | Exemple concret                                                                             |
|----------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Niveau 1 :<br/>Système nerveux autonome végétatif</b> | Survie de l'individu (homéostasie, besoins primaires)   | Régulation corporelle, réactions instinctives       | Déséquilibre physiologique (stress chronique, fatigue, dépendance)          | Stimulation électromagnétique (basses fréquences), neurotoxines       | Ondes EM pulsées induisant des maux de tête persistants ( <i>Moscow Signal</i> , 1972–1989) |
| <b>Niveau 2 :<br/>Système psycho-affectif</b>            | Gestion des émotions et des relations interpersonnelles | Peur, empathie, motivation, sentiment de soi        | Manipulation émotionnelle (anxiété, euphorie artificielle, apathie)         | Ondes EM (1–10 GHz), musique répétitive, <i>deepfakes</i> émotionnels | Campagnes de désinformation exploitant la peur pour induire un climat de panique collective |
| <b>Niveau 3 :<br/>Système cognitif supérieur</b>         | Pensée réflexive, raisonnement, mémoire                 | Analyse, synthèse, prise de décision, métacognition | Altération cognitive (biais amplifiés, erreurs de jugement, désorientation) | IA générative, <i>deepfakes</i> , désinformation ciblée               | <i>Deepfakes</i> exploitant le biais de confirmation pour renforcer des croyances erronées  |

On voit ainsi que les mécanismes qui font la force du cerveau humain — sa plasticité, sa capacité à s'adapter, sa sensibilité aux émotions — sont aussi ceux qui le rendent vulnérable. Les attaques cognitives, qu'elles soient neurobiologiques ou informationnelles, exploitent ces failles structurelles pour détourner les processus naturels de la pensée.

Cette organisation hiérarchique montre que les attaques cognitives peuvent cibler plusieurs niveaux simultanément. Par exemple, une campagne de désinformation (niveau 3) peut être amplifiée par des ondes EM (niveau 2) pour induire un état de stress, lui-même exploitant les réactions instinctives (niveau 1) de peur ou de fuite.

## D. Une nature émergente : la conscience comme phénomène systémique

Les processus cognitifs culminent dans la conscience, ce phénomène émergent qui permet à un individu de percevoir, ressentir et agir de manière intégrée. La conscience que l'on définit comme « *état de vigilance et d'éveil permettant à un être (humain, animal, ou potentiellement machine) de percevoir, ressentir, penser et agir de manière intégrée* », n'est pas localisée dans une zone cérébrale spécifique, mais résulte de l'interaction dynamique entre plusieurs systèmes :

- *L'éveil (wakefulness)* : état de vigilance ;
- *La conscience de soi (self-awareness)* : capacité à se reconnaître comme un sujet distinct ;
- *Les qualia* : expériences subjectives (par exemple, la rougeur du rouge, la douleur) ;
- *L'intentionnalité* : capacité à avoir des états mentaux dirigés vers des objets.

Alors que le cerveau en constitue le substrat neurobiologique et les perceptions en forment le contenu informationnel, la conscience représente cette capacité dynamique à intégrer, interpréter et agir sur le monde qui nous entoure. C'est elle qui permet à l'individu de distinguer le réel de l'illusion, le vrai du faux, l'autonomie de la manipulation.

## E. La conscience comme champ de bataille : entre perception et réalité

La guerre cognitive et la guerre cognitive ne se contentent pas de cibler le cerveau ou les flux informationnels : elles visent l'essence même de ce qui fait de nous des êtres pensants — la conscience .

Et c'est précisément cette capacité qui devient la cible ultime des attaques cognitives combinées, la conscience étant devenue le champ de bataille ultime, où se jouent la perception, la décision et l'identité — trois dimensions aussi cruciales que le substrat neurobiologique lui-même.

Comme l'intelligence humaine. Associée à la conscience dont elle procède chez les êtres vivants, l'intelligence est un concept multidimensionnel qui a évolué avec les avancées scientifiques. Historiquement associée à des capacités humaines (raisonnement logique, créativité), elle est aujourd'hui modélisable dans des systèmes artificiels. Elle se définit comme la capacité d'un système (biologique ou artificiel) à acquérir, comprendre, appliquer et adapter des connaissances pour résoudre des problèmes, s'adapter à de nouvelles situations, ou atteindre des objectifs. L'intelligence implique des processus cognitifs tels que le raisonnement, l'apprentissage, la mémoire, la perception et la prise de décision.

Les technologies à visées cognitives agissent sur les différents processus cognitifs à des degrés, selon des modalités et avec des impacts divers comme le montre le tableau ci-dessous.

| Processus cognitif     | Définition                                                    | Impact des technologies                                        | Conséquences                                                    | Exemples concrets                                                                                                                                                                  |
|------------------------|---------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Réfléchir</b>       | Dialogue intérieur (Platon) ou collectif (Yoruba <i>ori</i> ) | Fragmentation (notifications, multitâche)                      | Réduction de la capacité à la réflexion profonde                | Durée moyenne de concentration : 8 secondes (vs. 12 en 2000)                                                                                                                       |
| <b>Comprendre</b>      | Construction de modèles mentaux cohérents                     | Illusion de compréhension (biais d'efficacité perçue)          | Surestimation de sa propre compréhension                        | Étude NUMERICOG (2023) : 78% des utilisateurs de réseaux sociaux pensent comprendre des sujets complexes après une lecture superficielle                                           |
| <b>Analyser</b>        | Décomposition du réel pour en saisir les rouages              | Simplification algorithmique (logique binaire)                 | Perte de la pensée nuancée                                      | Bulles filtrantes (Eli Pariser) : enfermement dans des réalités informationnelles personnalisées                                                                                   |
| <b>Apprendre</b>       | Construction active de savoir                                 | Externalisation cognitive (mémoire transactive)                | Appauvrissement de la mémorisation et de la synthèse            | Étude OCDE (2026) : -22% de capacité à synthétiser chez les étudiants utilisant régulièrement l'IA                                                                                 |
| <b>Critiquer</b>       | Mise à l'épreuve des certitudes                               | Biais de confirmation amplifié (algorithmes de recommandation) | Réduction de l'esprit critique                                  | Étude <i>Wall Street Journal</i> (2016) : Facebook peut manipuler les émotions en modifiant son algorithme                                                                         |
| <b>Contester</b>       | Refus de l'ordre ou de la norme établis                       | Outils de mobilisation (réseaux sociaux)                       | Amplification de la contestation... mais aussi de la répression | Printemps arabe, <i>Black Lives Matter</i>                                                                                                                                         |
| <b>Confronter</b>      | Mise face à face des idées                                    | Chambres d'écho (algorithmes)                                  | Polarisation des débats                                         | Étude <i>American Psychological Association</i> (2023) : -25% de capacité à analyser des situations sociales complexes chez les adolescents utilisant >3h/jour les réseaux sociaux |
| <b>Comparer</b>        | Établissement de liens entre les choses                       | Bulles culturelles (personnalisation algorithmique)            | Réduction de l'exposition à des perspectives divergentes        | Étude <i>Université de Tokyo</i> (2020) : les utilisateurs japonais partagent moins de contenus polarisants que les Occidentaux                                                    |
| <b>Déduire/Induire</b> | Raisonnement logique ou intuitif                              | Délégation à l'IA (outils de décision automatisés)             | Dépendance cognitive                                            | Étude <i>Université de Stanford</i> (2024) : 68% des utilisateurs réguliers d'IA générative ont du mal à distinguer un texte humain d'un texte généré par une machine              |
| <b>Synthétiser</b>     | Intégration de connaissances disparates                       | Surcharge informationnelle                                     | Difficulté à intégrer des informations complexes                | Étude <i>Université du Michigan</i> (2023) : -22% de capacité à synthétiser des informations spatiales chez les utilisateurs de maisons intelligentes                              |
| <b>Évaluer</b>         | Jugement et prise de décision                                 | Délégation aux algorithmes                                     | Perte d'autonomie dans la prise de décision                     | Projet NUMERICOG (2023) : -15% de capacité à évaluer des situations complexes                                                                                                      |

Ces transformations ne sont pas neutres : elles réduisent notre autonomie cognitive tout en augmentant notre dépendance aux outils technologiques.

Il existe une multitude d'états de conscience : états naturels (éveil, rêve non lucide, sommeil), états modifiés (rêve lucide, méditation, hypnose, état de flow<sup>4</sup>), états pathologiques (coma, anesthésie, mort cérébrale).

| État de conscience                        | Niveau d'éveil            | Caractéristiques                                                              | Exemples/Commentaires                                                     |
|-------------------------------------------|---------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Éveil (Conscience ordinaire)</b>       | Élevé                     | Perception claire, pensée logique, interaction avec l'environnement.          | Vie quotidienne, travail, conversations.                                  |
| <b>Rêve lucide</b>                        | Variable (souvent modéré) | Prise de conscience pendant le rêve, contrôle partiel ou total des actions.   | Expérience onirique où l'on sait qu'on rêve.                              |
| <b>Rêve non lucide</b>                    | Faible                    | Activité mentale involontaire, absence de conscience de soi.                  | Rêves classiques pendant le sommeil paradoxal.                            |
| <b>Sommeil profond</b>                    | Très faible               | Récupération physique, absence de rêve, difficile à réveiller.                | Phases 3 et 4 du sommeil (sommeil à ondes lentes).                        |
| <b>Sommeil paradoxal</b>                  | Modéré (cerveau actif)    | Rêves intenses, mouvement oculaire rapide (REM), corps paralysé.              | Phase où la plupart des rêves surviennent.                                |
| <b>Méditation profonde</b>                | Variable (souvent élevé)  | État de calme mental, conscience élargie, parfois accès à des états modifiés. | Pratiques comme le samadhi (yoga) ou la pleine conscience.                |
| <b>État hypnotique</b>                    | Modéré à faible           | Suggestibilité accrue, focalisation intense, conscience restreinte.           | Utilisé en thérapie ou pour l'auto-amélioration.                          |
| <b>Coma</b>                               | Minimal à nul             | Absence de réponse aux stimuli, pas de cycle veille-sommeil.                  | État pathologique (ex. : coma post-traumatique).                          |
| <b>Anesthésie générale</b>                | Nul                       | Inconscience totale et réversible, induite par des substances.                | Utilisée en chirurgie.                                                    |
| <b>État végétatif</b>                     | Minimal                   | Éveil sans conscience de soi ou de l'environnement.                           | Syndrome apallique (ex. : après un traumatisme crânien sévère).           |
| <b>Mort cérébrale</b>                     | Nul                       | Absence totale et irréversible d'activité cérébrale.                          | Critère légal de mort dans de nombreux pays.                              |
| <b>Expérience de mort imminente (EMI)</b> | Variable                  | Sensation de sortie du corps, tunnel lumineux, revue de vie.                  | Rapporté par des personnes en situation de mort clinique.                 |
| <b>Trances chamaniques</b>                | Variable                  | État modifié de conscience, souvent induit par des rituels ou des substances. | Pratiques traditionnelles (ex. : ayahuasca, tambours).                    |
| <b>Flow (Flux)</b>                        | Élevé                     | Concentration totale, perte de la notion du temps, performance optimale.      | Expérimenté par les artistes, sportifs ou travailleurs en état de "zone". |

### I-1.1.2 Les fonctions des processus cognitifs : le cerveau comme système opérationnel

Les processus cognitifs sont donc à la fois neurobiologiques (chimie, électricité, ondes cérébrales), informationnels (acquisition, stockage, traitement, transmission) et émergents (conscience comme phénomène systémique).

Cette multi-dimensionalité explique pourquoi ils peuvent être attaqués de multiples manières : via des *neuroweapons* (ciblant la dimension neurobiologique), des *deepfakes* (ciblant la dimension informationnelle), ou des drogues (ciblant la dimension émergente de la conscience).

Les processus cognitifs ne sont pas de simples mécanismes passifs : ils remplissent des fonctions opérationnelles essentielles à la survie et à l'adaptation. Ces fonctions peuvent être regroupées en cinq

<sup>4</sup> Le concept d'état de flow décrit un état de concentration totale où une personne est complètement absorbée par une activité, perdant la notion du temps. On parle aussi parfois d « expérience optimale »

grandes catégories, chacune associée à des zones cérébrales spécifiques et des mécanismes neurobiologiques distincts.

### **A. La perception : la porte d'entrée des informations**

La perception est le processus par lequel le cerveau acquiert et interprète les informations sensorielles (vue, ouïe, toucher, odorat, goût). Elle repose sur la détection sensorielle (les organes sensoriels (yeux, oreilles, etc.) captent les stimuli externes et les transforment en signaux nerveux), le traitement cortical (ces signaux sont ensuite traités par des zones cérébrales spécialisées (ex. : cortex visuel pour la vue, cortex auditif pour l'ouïe)) ainsi que sur l'intégration multisensorielle (le cerveau combine les informations provenant de différents sens pour créer une représentation cohérente du monde). *Exemple* : la vision implique la détection de la lumière par les cônes et bâtonnets de la rétine, le traitement de cette information par le cortex visuel primaire et son interprétation par les zones associatives (ex. : reconnaissance des visages dans le cortex temporal).

Ses vulnérabilités sont principalement les suivantes : illusions sensorielles (des stimuli trompeurs peuvent fausser la perception) ; surcharge sensorielle (une exposition à trop d'informations peut saturer les capacités perceptives) ; déficiences sensorielles (des lésions cérébrales (ex. : AVC dans le cortex visuel) peuvent altérer la perception).

### **B. La mémoire : le stockage et la récupération des informations**

La mémoire permet de conserver et récupérer les informations perçues. Elle se divise en plusieurs types, chacun associé à des mécanismes neurobiologiques spécifiques :

*Mémoire sensorielle* : Stockage très court (quelques millisecondes à secondes) des informations sensorielles. *Mécanisme* : Activation temporaire des zones sensorielles (ex. : cortex visuel).

*Mémoire à court terme* : Stockage temporaire (quelques secondes à minutes) des informations utiles. *Mécanisme* : Activation du cortex préfrontal et des circuits neuronaux impliquant le cortex pariétal.

*Mémoire à long terme* : Stockage durable (jours à toute une vie) des informations. *Mécanisme* : modifications structurelles des synapses (plasticité synaptique) dans l'hippocampe et le cortex. *Exemple* : la formation d'un souvenir à long terme implique l'encodage de l'information dans l'hippocampe, sa consolidation pendant le sommeil (via les ondes cérébrales) et son stockage dans le cortex pour une récupération future.

Ses vulnérabilités se manifestent principalement par les événements suivants : faux souvenirs (des informations répétées ou des stimulations ciblées peuvent implanter de faux souvenirs) ; amnésie (des lésions de l'hippocampe ou des drogues peuvent effacer la mémoire) ; biais de mémoire (le cerveau reconstruit les souvenirs à chaque rappel, les rendant vulnérables à la distorsion).

### **C. Le raisonnement : la manipulation des idées**

Le raisonnement permet de manipuler les informations pour résoudre des problèmes, prendre des décisions ou générer de nouvelles idées. Il repose sur la logique (application de règles formelles), l'heuristique (utilisation de raccourcis mentaux comme par exemple des biais cognitifs), la créativité (génération de nouvelles combinaisons d'idées). *Exemple* : la résolution d'un problème implique l'analyse des informations disponibles (via le cortex préfrontal), la comparaison avec des connaissances existantes (via la mémoire) et la génération de solutions (via les zones associatives du cortex).

Ses vulnérabilités se traduisent principalement par les événements suivants : biais cognitifs (les raccourcis mentaux (ex. : biais de confirmation, biais de Dunning-Kruger) peuvent fausser le raisonnement) ; surcharge cognitive (une exposition à trop d'informations peut paralyser le raisonnement) ; manipulation algorithmique (les algorithmes de recommandation peuvent amplifier les biais et limiter la diversité des idées et des opinions).

### **D. L'émotion : la coloration affective de la pensée**

Les émotions jouent un rôle clé dans les processus cognitifs en colorant les perceptions, mémoires et décisions. Elles reposent sur l'activation du système limbique (l'amygdale (peur, agressivité), l'hippocampe (mémoire émotionnelle) et le cortex cingulaire (régulation émotionnelle) sont des zones

clés), la libération de neurotransmetteurs (la sérotonine (humeur), la dopamine (récompense) et la noradrénaline (stress) modulent les émotions) ainsi que sur les expressions comportementales (les émotions se manifestent par des réactions physiques (ex. : accélération du rythme cardiaque, sudation)). *Exemple* : la peur implique la détection d'une menace (via les sens), l'activation de l'amygdale, qui déclenche une réaction de combat/fuite et la libération de noradrénaline, qui prépare le corps à l'action.

Ses principales vulnérabilités se manifestent par les événements suivants : manipulation émotionnelle (des stimuli externes (ex. : *deepfakes* émotionnels, ondes EM) peuvent induire des émotions artificielles) ; déséquilibre chimique (des drogues (ex. : LSD, BZ) ou des *neuroweapons* peuvent perturber la régulation émotionnelle) ; contagion émotionnelle (les émotions peuvent se propager dans un groupe (ex. : panique collective)).

### **E. La prise de décision : l'aboutissement des processus cognitifs**

La prise de décision est le processus par lequel le cerveau sélectionne une action parmi plusieurs options. Elle repose sur l'évaluation des options (le cortex préfrontal compare les avantages et inconvénients de chaque choix), la pondération émotionnelle (les émotions influencent la décision) et l'exécution motrice (une fois la décision prise, le cortex moteur déclenche l'action). *Exemple* : la décision d'acheter un produit implique l'évaluation de ses caractéristiques (via le cortex préfrontal), la comparaison avec d'autres options (via la mémoire), l'influence des émotions (ex. : désir, peur de manquer) et l'action (achat ou non).

Ses principales vulnérabilités sont les suivantes : paralysie décisionnelle (une surcharge informationnelle ou un stress extrême peut bloquer la prise de décision) ; manipulation des préférences (des algorithmes ou des drogues peuvent influencer les choix) ; biais de décision (les biais cognitifs peuvent fausser les décisions).

Nous voyons ainsi que les processus cognitifs forment un système intégré où la perception fournit les données brutes, la mémoire les stocke, le raisonnement les traite, les émotions les colorent et la prise de décision les utilise pour agir.

Chaque fonction est interdépendante des autres, et une perturbation dans l'une peut avoir des effets en cascade sur les autres. C'est cette interdépendance qui rend les processus cognitifs si vulnérables aux attaques cognitives et cognitives.

#### **I-1.1.3 Les mécanismes sous-jacents : comment les processus cognitifs fonctionnent-ils ?**

Pour comprendre comment les processus cognitifs peuvent être manipulés, il est essentiel de plonger dans leurs mécanismes sous-jacents. Ces mécanismes peuvent être classés en trois grandes catégories : neurobiologiques, physiques et algorithmiques.

##### **A. Mécanismes neurobiologiques : la chimie et l'électricité du cerveau**

Les processus cognitifs reposent sur des mécanismes neurobiologiques précis, qui peuvent être ciblés directement par des attaques neurobiologiques (guerre cognitive).

###### *1. Les neurotransmetteurs : les messagers chimiques*

Les neurotransmetteurs sont des molécules chimiques qui transmettent les signaux entre les neurones. Chaque neurotransmetteur a un rôle spécifique : dopamine (récompense, motivation, plaisir) ; sérotonine (humeur, anxiété, sommeil) ; noradrénaline (éveil, attention, stress) ; GABA (inhibition neuronale, calme) ; glutamate (excitation neuronale, apprentissage) ; acétylcholine (transmission neuromusculaire, mémoire). *Mécanisme d'action* : un neurone libère un neurotransmetteur dans la synapse ; le neurotransmetteur se lie aux récepteurs du neurone suivant ; cela modifie le potentiel électrique du neurone suivant, déclenchant ou inhibant un potentiel d'action.

Leurs vulnérabilités se manifestent au travers des événements suivants : modulation artificielle (des drogues (ex. : BZ, LSD) ou des *neuroweapons* (ex. : ondes EM) peuvent stimuler ou inhiber la libération de neurotransmetteurs) ; déséquilibre chimique (un excès ou un déficit de neurotransmetteurs (ex. : dépression liée à un manque de sérotonine) peut perturber les processus cognitifs).

###### *2. Les potentiels d'action : les signaux électriques*

Les neurones communiquent via des potentiels d'action, des impulsions électriques qui parcourent les axones. Ces signaux reposent sur l'ouverture des canaux ioniques (les canaux sodiques ( $\text{Na}^+$ ) et potassiques ( $\text{K}^+$ ) s'ouvrent et se ferment pour générer un potentiel d'action) et la propagation du signal (le potentiel d'action se propage le long de l'axone jusqu'à la synapse).

Leurs vulnérabilités se manifestent au travers des événements suivants : stimulation électrique artificielle (des neurostimulateurs (ex. : TMS, DBS) ou des ondes EM peuvent induire des potentiels d'action dans des zones ciblées) ; blocage des canaux ioniques (certaines toxines (ex. : tétrodotoxine) peuvent bloquer les canaux sodiques, empêchant la propagation des potentiels d'action).

### 3. La plasticité synaptique : la base de l'apprentissage et de la mémoire

La plasticité synaptique est la capacité des synapses à se renforcer ou s'affaiblir en fonction de leur activité. Elle est à la base de l'apprentissage (renforcement des synapses entre neurones actifs simultanément (principe de Hebb : *"Les neurones qui s'activent ensemble se lient ensemble"*) et de la mémoire (consolidation des souvenirs via la modification des synapses). *Mécanisme d'action* : potentiation à long terme (LTP) (une stimulation intense des synapses les renforce, facilitant la transmission future) ; dépression à long terme (LTD) (une stimulation faible des synapses les affaiblit, réduisant la transmission future).

Ses vulnérabilités se manifestent au travers des événements suivants : manipulation de la plasticité (des drogues (ex. : MDMA) ou des stimulations électriques (ex. : *neurofeedback*) peuvent altérer la plasticité synaptique, affectant ainsi l'apprentissage et la mémoire) ; faux souvenirs (une stimulation ciblée peut renforcer artificiellement des synapses, implantant ainsi de faux souvenirs).

## B. Mécanismes physiques : l'interaction avec l'environnement

Les processus cognitifs peuvent aussi être influencés par des mécanismes physiques, notamment :

### 1. Les ondes électromagnétiques (EM)

Les ondes EM (micro-ondes, radiofréquences, infrasons) peuvent interagir avec le cerveau de plusieurs manières : effet thermique (un échauffement localisé des tissus cérébraux peut perturber l'activité neuronale) ; effet non-thermique (les ondes EM peuvent moduler les canaux ioniques ou synchroniser les ondes cérébrales) ; effet Frey (certaines fréquences (1–10 GHz) peuvent induire des sons audibles directement dans le cerveau).

Ondes cérébrales et leur modulation par les champs EM

| Onde cérébrale | Fréquence (Hz) | Rôle                                   | Effet des champs EM                                      | Technologies associées             | Applications militaires                         | Risques                     |
|----------------|----------------|----------------------------------------|----------------------------------------------------------|------------------------------------|-------------------------------------------------|-----------------------------|
| <b>Delta</b>   | 0,5–4          | Sommeil profond, régénération          | Synchronisation forcée → fatigue, troubles du sommeil    | Ondes ELF (3–30 Hz)                | Désorientation des troupes (fatigue chronique)  | Insomnie, dépression        |
| <b>Thêta</b>   | 4–8            | Méditation, créativité, suggestibilité | Augmentation → état de transe, hallucinations            | Ondes EM (1–3 GHz), binaural beats | Hypnose à distance, implantation de suggestions | Psychose, dépendance        |
| <b>Alpha</b>   | 8–12           | Relaxation, réduction du stress        | Désynchronisation → anxiété, stress                      | Ondes EM (1–10 GHz)                | Désorientation émotionnelle                     | Anxiété chronique           |
| <b>Bêta</b>    | 12–30          | Concentration, vigilance               | Augmentation excessive → stress, troubles de l'attention | Ondes EM (1–3 GHz), Wi-Fi          | Surcharge cognitive, paralysie décisionnelle    | Burnout, troubles cognitifs |
| <b>Gamma</b>   | 30–100         | Mémoire, traitement de l'information   | Perturbation → troubles cognitifs                        | 5G FR1 (3–6 GHz)                   | Désorientation, troubles de la mémoire          | Démence, Alzheimer          |

### 2. Les ondes sonores (infrasons, ultrasons)

Les ondes sonores peuvent aussi affecter le cerveau : infrasons (0,1–20 Hz) (peuvent faire résonner les organes internes, provoquant des nausées, des vertiges ou des hallucinations) ; ultrasons (20 kHz–1 GHz) (peuvent stimuler mécaniquement les tissus cérébraux (via des transducteurs focalisés) ; *Binaural beats* (des fréquences légèrement différentes jouées dans chaque oreille peuvent synchroniser les ondes cérébrales).

### 3. Les stimuli visuels (lumière, lasers)

La lumière peut influencer les processus cognitifs via la stimulation des photorécepteurs (la lumière bleue (450–495 nm) peut inhiber la mélatonine, perturbant ainsi le sommeil) ; les illusions optiques (des stimuli visuels trompeurs (ex. : *deepfakes*, réalité augmentée) peuvent fausser la perception) ; les lasers stroboscopiques (des flashes lumineux à certaines fréquences (ex. : 12 Hz) peuvent provoquer des crises épileptiques).

### Techniques de synchronisation des ondes cérébrales

| Technique                                          | Description                                                                                                                                                 | Fréquences utilisées      | Effets                                                                            | Applications militaires                                           |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>Entraînement auditif (binaural beats)</b>       | Deux fréquences légèrement différentes (ex. : 300 Hz et 310 Hz) sont jouées dans chaque oreille → le cerveau perçoit une 3e fréquence (10 Hz, ondes alpha). | 0,5–40 Hz (delta à gamma) | Synchronisation des ondes cérébrales → état de transe, relaxation, suggestibilité | Hypnose à distance, manipulation émotionnelle                     |
| <b>Stimulation magnétique transcrânienne (TMS)</b> | Champs magnétiques pulsés (1–10 Hz) stimulent le cortex cérébral.                                                                                           | 1–10 Hz (thêta, alpha)    | Modulation de l'activité neuronale → changement d'humeur, désorientation          | Neutralisation de cibles, contrôle des émotions                   |
| <b>Ondes EM pulsées</b>                            | Impulsions EM courtes (1–10 µs) synchronisent les réseaux neuronaux.                                                                                        | 1–3 GHz                   | Perturbation des ondes bêta/gamma → troubles cognitifs                            | Désorientation des troupes, sabotage des capacités décisionnelles |
| <b>Infrasons</b>                                   | Ondes sonores basses fréquences (0,1–20 Hz) font résonner les organes internes.                                                                             | 7–18 Hz                   | Synchronisation des ondes delta/thêta → fatigue, hallucinations                   | Désorientation collective, panique                                |

## C. Mécanismes algorithmiques : le cerveau comme machine computationnelle

Enfin, les processus cognitifs peuvent être modélisés comme des algorithmes, c'est-à-dire des séquences d'opérations permettant de traiter l'information.

Cette approche, inspirée de l'intelligence artificielle, permet de comprendre comment le cerveau acquiert des informations (perception), stocke des informations (mémoire), traite des informations (raisonnement) et transmet des informations (communication).

Leurs principales vulnérabilités se manifestent au travers des événements suivants : biais algorithmiques (les raccourcis mentaux (biais cognitifs) peuvent être exploités pour fausser le raisonnement) ; la surcharge computationnelle (une exposition à trop d'informations peut saturer les capacités de traitement) ; manipulation des entrées (des fausses informations peuvent corrompre les données en entrée, faussant ainsi les sorties).

Les processus cognitifs reposent donc sur des mécanismes neurobiologiques (neurotransmetteurs, potentiels d'action, plasticité synaptique), des mécanismes physiques (ondes EM, ondes sonores, stimuli visuels) et des mécanismes algorithmiques (traitement de l'information).

Chacun de ces mécanismes peut être ciblé par des attaques spécifiques relevant soit de la *guerre cognitive (neurobiologique)* qui cible les mécanismes neurobiologiques, soit de la *guerre cognitive (informationnelle)* qui cible les mécanismes algorithmiques, soit d'une combinaison des deux approches pour obtenir un effet synergique.

### I-1.1.4 Les vecteurs d'influence : comment les processus cognitifs sont-ils ciblés ?

Les processus cognitifs peuvent être influencés — voire manipulés — par une multiplicité de vecteurs, allant des stimuli naturels aux technologies avancées. Ces vecteurs peuvent être classés en quatre grandes catégories : naturels, technologiques, chimiques et comportementaux.

### **A. Vecteurs naturels : les limites intrinsèques du cerveau**

Le cerveau humain n'est pas une machine parfaite : il présente des limites et des biais naturels qui peuvent être exploités pour influencer les processus cognitifs.

#### *1. Les biais cognitifs*

Les biais cognitifs sont des distorsions systématiques du jugement, souvent utiles pour économiser des ressources mentales, mais qui peuvent aussi fausser la pensée.

Parmi les plus importants figurent le biais de confirmation (tendance à privilégier les informations confirmant ses croyances et à ignorer celles qui les contredisent), le biais de Dunning-Kruger (tendance des individus peu compétents à surestimer leurs capacités), le biais de négativité (tendance à accorder plus d'importance aux informations négatives), ainsi que l'effet de simple exposition (tendance à préférer ce qui est familier, même si c'est faux ou nuisible). *Exemple* : les algorithmes de recommandation (YouTube, Facebook) amplifient les biais de confirmation en montrant principalement des contenus alignés avec les opinions existantes, créant ainsi des bulles informationnelles.

#### *2. Les limites de la mémoire*

La mémoire humaine n'est pas infallible : elle est sélective, reconstructive et vulnérable aux distorsions.

Parmi ses limites figurent l'oubli (les souvenirs s'estompent avec le temps), les faux souvenirs (des informations répétées ou des suggestions peuvent implanter de faux souvenirs) et les biais de mémoire (les souvenirs sont reconstruits à chaque rappel, les rendant vulnérables à la distorsion).

#### *3. Les limites de l'attention*

L'attention est une ressource limitée : le cerveau ne peut traiter qu'un nombre restreint d'informations à la fois.

Parmi ses limites figurent la surcharge attentionnelle (une exposition à trop d'informations peut saturer l'attention), la cécité au changement (le cerveau peut ne pas remarquer des changements importants dans son environnement) ainsi que l'effet *cocktail party* (le cerveau filtre les informations non pertinentes, mais ce filtrage peut être contourné (par exemple par des stimuli émotionnels)). *Exemple* : les réseaux de bots peuvent saturer l'espace informationnel avec des contenus contradictoires, rendant impossible la distinction entre le vrai et le faux.

### **B. Vecteurs technologiques : l'amplification artificielle des failles**

Les technologies modernes offrent des moyens puissants pour influencer les processus cognitifs, en exploitant leurs vulnérabilités naturelles.

#### *1. Technologies informationnelles : ces technologies ciblent les mécanismes algorithmiques des processus cognitifs, en manipulant les flux d'information :*

Les *deepfakes* représentent aujourd'hui l'arme la plus redoutable de la guerre cognitive. Ces contenus audio ou vidéo hyperréalistes, générés par des intelligences artificielles comme *Sora* (OpenAI, 2024) ou *Stable Diffusion*, sont capables de tromper même les observateurs les plus avertis. Leur force réside dans leur capacité à exploiter notre confiance naturelle dans la perception visuelle ou auditive : si nous voyons ou entendons quelque chose, nous avons tendance à le croire vrai. *Exemple marquant* : en 2024, un *deepfake* du président français annonçant une mobilisation générale a circulé massivement sur les réseaux sociaux, provoquant une panique temporaire avant d'être démenti. Pourtant, malgré les démentis, 30 % des personnes exposées ont continué à croire à la véracité du contenu (étude IFOP, 2024).

Les modèles d'*IA générative*, comme *GPT-4* (OpenAI) ou *Llama 3* (Meta), ont révolutionné la guerre cognitive en permettant la création massive et personnalisée de contenus manipulés. Contrairement aux méthodes traditionnelles de propagande, qui nécessitaient des ressources humaines importantes,

l'IA générative permet de produire de manière autonome et personnalisée des textes, images et vidéos sur mesure à une échelle industrielle, adaptés aux vulnérabilités spécifiques de chaque cible. *Exemple* : Sora (OpenAI) peut générer des vidéos réalistes à partir de prompts textuels, facilitant la désinformation.

Les *réseaux de bots*, comptes automatisés, souvent contrôlés par des IA, inondent les plateformes numériques de messages coordonnés qui créent un bruit de fond informationnel, amplifiant ainsi la portée de la désinformation. Leur force réside dans leur nombre et leur coordination : en 2026, on estime que 15 à 20 % des comptes actifs sur Twitter/X sont des bots (Ferrara, 2017). *Mécanisme d'action* : un réseau de bots peut diffuser massivement une *fake news* en quelques minutes, la faire monter en tendance via des likes et retweets automatisés, puis créer l'illusion d'un consensus en simulant des discussions entre faux comptes. *Exemple* : pendant les élections présidentielles françaises de 2022, des réseaux de bots ont amplifié des rumeurs infondées sur des candidats, influençant l'opinion publique de manière significative (rapport ANSSI, 2023).

Les *algorithmes de recommandation*, systèmes qui personnalisent les contenus en fonction des préférences des utilisateurs utilisés par des plateformes comme YouTube, Facebook ou TikTok, jouent un rôle décisif mais souvent sous-estimé dans la guerre cognitive. Ce sont les architectes de nos bulles informationnelles. Leur objectif premier est de maximiser l'engagement des utilisateurs, mais leur effet secondaire est de renforcer les biais cognitifs en enfermant les individus dans des bulles filtrantes. *Mécanisme* : un algorithme identifie les préférences d'un utilisateur (ex. : ses likes, ses recherches, son temps de visionnage) et lui propose prioritairement des contenus similaires ou plus extrêmes. *Conséquence* : les utilisateurs sont exposés à des informations de plus en plus polarisées, ce qui amplifie les divisions sociétales et rend les populations plus vulnérables à la manipulation. Une étude de l'MIT (2018) a montré que les *fake news* se propagent six fois plus vite que les informations vraies sur Twitter, en grande partie grâce à l'amplification algorithmique. *Exemple* : YouTube comme X favorisent les contenus extrêmes, amplifiant ainsi la polarisation.

2. *Neurotechnologies* : ces technologies ciblent les mécanismes neurobiologiques des processus cognitifs, en agissant directement sur le cerveau :

Les *neuroweapons* représentent aujourd'hui l'arme la plus redoutable de la guerre cognitive. Ces dispositifs utilisent des ondes électromagnétiques, des ultrasons ou des produits chimiques pour cibler directement le cerveau, sans contact physique (par exemple en stimulant l'amygdale pour induire la peur). Leur force réside dans leur capacité à agir à distance et à contourner les défenses physiques traditionnelles. *Exemple marquant* : le *Moscow Signal* (1972–1989), où des ondes micro-ondes pulsées (2,5–4 GHz) ont ciblé l'ambassade américaine à Moscou, provoquant chez le personnel diplomatique des maux de tête chroniques, des troubles du sommeil et une altération de la mémoire. *Mécanisme* : ces ondes, en modulant les canaux ioniques des neurones, ont perturbé l'activité synaptique dans le cortex cérébral, illustrant comment une attaque électromagnétique peut désorganiser les fonctions cognitives sans laisser de trace visible.

Les *interfaces cerveau-machine* (BCI) permettent une interaction directe entre le cerveau et un dispositif externe, ouvrant la voie à des applications offensives inédites. Contrairement aux *neuroweapons*, qui agissent à distance, les BCI nécessitent un contact physique (implants, électrodes) mais offrent un contrôle sans précédent sur les processus cérébraux (lecture des pensées, contrôle des mouvements, etc.). *Exemple* : *Neuralink* (Elon Musk) ou *BrainGate* (*Brown University*) démontrent comment des dispositifs peuvent lire les pensées ou influencer les décisions en temps réel.

La *neurostimulation* utilise des stimuli électriques, magnétiques ou optiques pour moduler l'activité neuronale de manière précise. Contrairement aux *neuroweapons*, qui agissent de manière globale, la neurostimulation permet un ciblage millimétrique des zones cérébrales. *Exemple* : la stimulation magnétique transcrânienne (TMS), utilisée en médecine pour traiter la dépression, pourrait être détournée pour induire des états émotionnels contrôlés (peur, euphorie) ou altérer les capacités cognitives (mémoire, attention).

Les *nanoneurotechnologies* utilisent des nanorobots ou nanoparticules pour interagir avec les neurones à l'échelle moléculaire. Leur force réside dans leur précision : elles peuvent cibler des neurotransmetteurs spécifiques ou des canaux ioniques pour moduler les états mentaux avec une exactitude chirurgicale. *Mécanisme* : modulent les neurotransmetteurs ou les canaux ioniques avec une

précision chirurgicale. *Exemple* : le projet *NANO* (DARPA, 2020) explore l'utilisation de nanorobots pour espionner les pensées ou manipuler les émotions en temps réel.

- *Technologies immersives* : ces technologies créent des environnements artificiels où les processus cognitifs peuvent être manipulés de manière totale :

L'émergence des environnements de *réalité virtuelle* et du *métavers* (univers virtuel persistant et partagé) offre des possibilités inédites de manipulation sensorielle, en permettant de contrôler intégralement ce que voit, entend et ressent un individu. *Exemple* : un *deepfake* en 3D, intégré dans un environnement virtuel, peut tromper tous les sens d'une cible, rendant la détection de la manipulation presque impossible.

### C. Vecteurs chimiques : la manipulation via la biochimie

*Drogues psychotropes* : ces substances modulent les neurotransmetteurs pour altérer les états mentaux.

Leur force réside dans leur discrétion : elles peuvent être administrées via des aérosols, des aliments ou des injections, sans que la cible ne s'en rende compte.

Le BZ (3-Quinuclidinyl Benzilate), antagoniste de l'acétylcholine développé par l'US Army dans les années 1960, provoque des hallucinations, une confusion mentale et une amnésie antérograde (incapacité à former de nouveaux souvenirs), rendant les cibles incapables de résister à la manipulation. Le LSD, agoniste de la sérotonine, qui provoque des hallucinations et une altération de la perception, a été utilisé par la CIA dans le projet *MKUltra* pour faciliter l'interrogatoire. La Scopolamine, antagoniste de l'acétylcholine qui provoque une amnésie antérograde a été utilisée par des criminels en Colombie comme "drogue du violeur".

*Application stratégique* : une drogue neuroactive pourrait être utilisée pour désorienter des troupes ennemies ou neutraliser des décideurs pendant une opération critique.

*Neurotoxines* : ces substances endommagent les neurones ou perturbent leur fonctionnement.

Le Sarin, inhibiteur de l'acétylcholinestérase qui provoque une surstimulation des récepteurs de l'acétylcholine, a été utilisé dans l'attaque du métro de Tokyo (1995). La toxine botulique, bloqueur de la libération d'acétylcholine qui provoque une paralysie musculaire, pourrait être potentiellement utilisable pour neutraliser des cibles.

### D. Vecteurs comportementaux : l'exploitation des états modifiés de conscience

La conscience n'est pas un phénomène statique, mais un processus émergent résultant de l'interaction entre plusieurs systèmes cérébraux.

Les neurosciences modernes, notamment les travaux de Francisco Varela (*The Embodied Mind*, 1991) et Stanislas Dehaene (*Consciousness and the Brain*, 2014), ont montré que la conscience repose sur deux mécanismes fondamentaux : l'accès conscient (la capacité à rapporter une information) et l'expérience consciente (le sentiment subjectif d'être soi, le *qualia*). Ces deux dimensions sont exploitables séparément ou conjointement par les guerres cognitive et cognitive.

L'accès conscient — la capacité à manipuler l'information de manière délibérée — est particulièrement vulnérable aux attaques informationnelles. Lorsque la guerre cognitive sature l'espace mental avec des *deepfakes*, des narratifs contradictoires ou des stimuli émotionnels, elle désorganise les mécanismes de filtrage et de hiérarchisation de l'information. Le cortex préfrontal, siège des fonctions exécutives, se trouve alors submergé par un flot de données incompatibles, rendant impossible la distinction entre réalité et fiction. *Exemple* : un décideur politique exposé à une campagne de désinformation massive perd progressivement la capacité à évaluer la crédibilité des sources, son accès conscient aux faits étant brouillé par le bruit informationnel.

L'expérience consciente — le sentiment subjectif d'être soi, de vivre une réalité cohérente — est, elle, vulnérable aux attaques neurobiologiques. Les *neuroweapons*, en modulant les neurotransmetteurs ou en stimulant des zones cérébrales spécifiques, peuvent altérer la perception de soi et du monde. *Exemple* : une stimulation ciblée de l'insula (région cérébrale associée à la conscience de soi) par des ondes électromagnétiques peut induire une dépersonnalisation — ce sentiment troublant d'être détaché de son

propre corps ou de ses pensées. De même, une modulation de la sérotonine ou de la dopamine peut provoquer des états modifiés de conscience où la frontière entre réalité et hallucination s'estompe.

La conscience n'est pas toujours dans un état de vigilance optimale. Les états modifiés de conscience (EMC) — qu'ils soient naturels (sommeil, rêve, méditation) ou induits (transe, hypnose, drogues) — offrent des fenêtres de vulnérabilité accrues aux attaques cognitives.

Ces états se caractérisent par une réduction des défenses critiques (le cerveau en état de transe ou de sommeil profond est moins capable de filtrer les informations), une augmentation de la suggestibilité (les sujets en hypnose ou sous l'effet de drogues sont plus réceptifs aux implants de faux souvenirs ou de croyances) et une altération de la mémoire (les EMC facilitent l'implantation de souvenirs fictifs ou la suppression de souvenirs réels)

Plus la conscience s'éloigne de son état d'éveil normal, plus elle devient vulnérable aux attaques. Les états de fatigue, de stress ou de transe constituent ainsi des moments stratégiques pour les opérateurs de guerre cognitive, qui peuvent exploiter ces fenêtres de vulnérabilité pour implanter des croyances, altérer des souvenirs ou contrôler des comportements.

Au-delà des individus, la conscience collective — cette capacité partagée par un groupe à interpréter le monde de manière cohérente — est elle aussi une cible.

Lorsque la guerre cognitive diffuse des *deepfakes* et des narratifs conflictuels à grande échelle, elle fragmente la conscience collective, créant des réalités parallèles où chaque groupe vit dans sa propre bulle informationnelle. Les études de Cass Sunstein montrent que les réseaux sociaux, en amplifiant les biais de confirmation, ont désintégré la conscience collective américaine, rendant impossible le dialogue entre démocrates et républicains.

*Méditation* : la méditation réduit l'activité du réseau du mode par défaut (DMN), améliorant la concentration mais aussi augmentant la suggestibilité. *Vulnérabilité* : un individu en méditation est 2x plus réceptif aux suggestions (étude de l'Université de Stanford, 2018). *Exemple* : utilisée par l'US Army dans le programme "*Mind Fitness Training*" pour améliorer la résilience des soldats, mais aussi potentiellement exploitable pour implanter des croyances.

*Transe* : la transe désactive le réseau du mode par défaut (DMN) et synchronise les ondes cérébrales, rendant l'individu extrêmement suggestible. *Vulnérabilité* : en transe, un individu peut accepter des suggestions qu'il rejeterait normalement. *Exemple* : utilisée par des sectes ou groupes extrémistes pour lavage de cerveau.

*Hypnose* : l'hypnose désactive partiellement le sens critique et augmente la connectivité entre le cortex préfrontal et les régions sensorielles. *Vulnérabilité* : un individu sous hypnose peut implanter de faux souvenirs ou contrôler des émotions. *Exemple* : utilisée par le KGB dans les années 1950–1980 pour extraire des informations ou manipuler des agents.

#### Vulnérabilités de la conscience selon son état

| État de conscience    | Caractéristiques                                                 | Vulnérabilités exploitables                           | Vecteurs d'attaque                       | Contre-mesures                           |
|-----------------------|------------------------------------------------------------------|-------------------------------------------------------|------------------------------------------|------------------------------------------|
| <b>Éveil normal</b>   | Attention focalisée, mémoire active, esprit critique             | Désinformation, <i>deepfakes</i> , biais cognitifs    | Guerre cognitive (IA, réseaux sociaux)   | Éducation critique, <i>fact-checking</i> |
| <b>Fatigue/Stress</b> | Réduction de l'attention, mémoire altérée, suggestibilité accrue | Désinformation amplifiée, neurostimulation            | Guerre cognitive + cognitive             | Détection précoce, neuroprotection       |
| <b>Méditation</b>     | Réduction du bruit mental, suggestibilité modérée                | Implantation de croyances, désinformation subliminale | Guerre cognitive (messages ciblés)       | Formation à la résilience                |
| <b>Transe</b>         | Dissociation, suggestibilité maximale, perte du sens critique    | Lavage de cerveau, implantation de faux souvenirs     | Hypnose, ondes EM, drogues               | Éviter les stimuli inducteurs            |
| <b>Sommeil</b>        | Inconscience, mémoire désactivée                                 | Manipulation onirique (rêves dirigés)                 | <i>Neuroweapons</i> (ultrasons), drogues | Blindage des chambres                    |

| État de conscience | Caractéristiques                          | Vulnérabilités exploitables                        | Vecteurs d'attaque                      | Contre-mesures         |
|--------------------|-------------------------------------------|----------------------------------------------------|-----------------------------------------|------------------------|
| Hypnose            | Suggestibilité extrême, mémoire altérable | Implantation de souvenirs, contrôle comportemental | Guerre cognitive (suggestions verbales) | Résistance à l'hypnose |

Cette section nous a permis de comprendre que les processus cognitifs peuvent donc être influencés par une multiplicité de vecteurs : naturels (biais cognitifs, limites de la mémoire) ; technologiques (*deepfakes*, *neuroweapons*, VR) ; chimiques (drogues, neurotoxines) ; comportementaux (méditation, transe, hypnose), et que ces vecteurs peuvent être combinés pour un effet synergique. Par exemple, une campagne de désinformation (guerre cognitive) peut être amplifiée par des *neuroweapons* (guerre cognitive) pour induire un état de panique collective.

### I-1.1.5 Les vulnérabilités des processus cognitifs : où et comment les attaques cognitives frappent

Les processus cognitifs, bien que puissants et adaptatifs, présentent des vulnérabilités structurelles qui en font des cibles idéales pour les attaques cognitives et cognitives.

Ces vulnérabilités peuvent être classées en cinq grandes catégories : structurelles, fonctionnelles, dynamiques, contextuelles et technologiques.

#### A. Vulnérabilités structurelles : les failles du *hardware* cérébral

Ces vulnérabilités découlent de la structure même du cerveau, qui présente des limites physiques et biologiques.

*Plasticité cérébrale : une force et une faiblesse* : la plasticité cérébrale — la capacité du cerveau à se réorganiser en fonction de l'expérience — est à la fois une force (apprentissage, adaptation) et une faiblesse (vulnérabilité à la manipulation). *Mécanisme* : la plasticité repose sur la modification des synapses (potentiation à long terme, LTP) et la neurogenèse (création de nouveaux neurones). *Vulnérabilité* : une stimulation artificielle (ex. : *neuroweapons*, drogues) peut détourner la plasticité pour implanter de faux souvenirs ou altérer les croyances. *Exemple* : une campagne de propagande répétée peut renforcer artificiellement des synapses, créant ainsi une adhésion compulsive à des idées fausses.

#### Mécanismes de la plasticité cérébrale et leur exploitation

| Mécanisme                       | Description                                                                          | Technologies de manipulation                           | Effets                                                    | Applications militaires                     |
|---------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------|---------------------------------------------|
| Potentiation à long terme (LTP) | Renforcement des synapses après une stimulation intense → apprentissage, mémoire.    | Neurostimulation (TMS, LIFU), drogues (MDMA, LSD)      | Implantation de faux souvenirs, renforcement de croyances | Lavage de cerveau, propagande subliminale   |
| Dépression à long terme (LTD)   | Affaiblissement des synapses après une stimulation faible → oubli, désapprentissage. | Ondes EM (1–3 GHz), drogues (BZ, scopolamine)          | Effacement de souvenirs, désorientation                   | Interrogatoires, manipulation des mémoires  |
| Neurogenèse                     | Création de nouveaux neurones (hippocampe) → apprentissage, mémoire.                 | Neurostimulation (LIFU), drogues (antidépresseurs)     | Amélioration cognitive, implantation de souvenirs         | Soldats augmentés, espionnage neuronal      |
| Pruning synaptique              | Élimination des synapses inutiles → optimisation des réseaux neuronaux.              | Ondes EM (basses fréquences), drogues (psychédéliques) | Désapprentissage, réorganisation forcée                   | Contrôle mental, manipulation des croyances |

*Limites de la connectivité cérébrale* : le cerveau est un réseau complexe de neurones, mais cette connectivité a des limites. *Mécanisme* : les neurones communiquent via des synapses, mais le nombre de connexions est fini. *Vulnérabilité* : une surcharge informationnelle peut saturer les capacités de traitement, rendant le cerveau moins capable de distinguer le vrai du faux. *Exemple* : Les algorithmes de recommandation (YouTube, Facebook) peuvent saturer l'attention avec des contenus émotionnels, réduisant ainsi la capacité critique.

*Dépendance aux neurotransmetteurs* : les processus cognitifs dépendent de neurotransmetteurs spécifiques, dont les niveaux peuvent être manipulés. *Mécanisme* : chaque neurotransmetteur (dopamine, sérotonine, etc.) a un rôle précis dans la régulation des émotions, de la mémoire et de la prise de décision. *Vulnérabilité* : une modulation artificielle (ex. : drogues, *neuroweapons*) peut déséquilibrer la chimie cérébrale, altérant ainsi les processus cognitifs. *Exemple* : une stimulation de la dopamine (via des ondes EM) peut induire une dépendance artificielle à des narratifs manipulés.

## **B. Vulnérabilités fonctionnelles : les failles du *software* mental**

Ces vulnérabilités découlent des fonctions mêmes des processus cognitifs, qui présentent des limites et des biais intrinsèques.

*Biais cognitifs (les raccourcis mentaux)* : les biais cognitifs sont des distorsions systématiques du jugement, souvent utiles pour économiser des ressources mentales, mais qui peuvent aussi fausser la pensée. *Mécanisme* : le cerveau utilise des raccourcis mentaux (heuristiques) pour traiter rapidement l'information. *Vulnérabilité* : ces raccourcis peuvent être exploités pour manipuler les perceptions et les décisions. *Exemple* : le biais de confirmation pousse les individus à privilégier les informations confirmant leurs croyances, rendant ainsi les fake news plus crédibles.

*Limites de la mémoire* : la mémoire humaine n'est pas infaillible : elle est sélective, reconstructive et vulnérable aux distorsions. *Mécanisme* : les souvenirs sont reconstruits à chaque rappel, ce qui les rend vulnérables à la distorsion. *Vulnérabilité* : des informations répétées ou des suggestions peuvent implanter de faux souvenirs. *Exemple* : un *deepfake* montrant un événement fictif, diffusé de manière répétée, peut créer un faux souvenir collectif.

*Limites de l'attention* : l'attention est une ressource limitée : le cerveau ne peut traiter qu'un nombre restreint d'informations à la fois. *Mécanisme* : le cerveau filtre les informations non pertinentes pour se concentrer sur les plus importantes. *Vulnérabilité* : une surcharge informationnelle peut saturer l'attention, rendant le cerveau moins capable de distinguer le vrai du faux. *Exemple* : les réseaux de bots peuvent saturer l'espace informationnel avec des contenus contradictoires, créant ainsi un bruit de fond où toute information crédible devient indistinguable.

## **C. Vulnérabilités dynamiques : les failles des états changeants**

Ces vulnérabilités découlent des changements d'état des processus cognitifs, qui peuvent altérer temporairement leurs fonctions.

*Fatigue et stress* : la fatigue et le stress réduisent les capacités cognitives. *Mécanisme* : le stress chronique augmente le cortisol, qui peut endommager l'hippocampe (mémoire) et le cortex préfrontal (prise de décision). *Vulnérabilité* : un individu fatigué ou stressé est moins capable de penser de manière critique et plus vulnérable à la manipulation. *Exemple* : une campagne de désinformation ciblant une population stressée (ex. : pendant une crise) peut avoir un impact plus important.

*États modifiés de conscience (EMC)* : les EMC (méditation, transe, hypnose, sommeil) modifient temporairement les processus cognitifs. *Mécanisme* : les EMC réduisent les défenses critiques et augmentent la suggestibilité. *Vulnérabilité* : un individu en EMC est plus vulnérable aux attaques cognitives (par exemple par une implantation de faux souvenirs). *Exemple* : un individu en transe peut être manipulé pour accepter des croyances extrêmes.

*Dépendance aux technologies* (voir ci-dessous)

## **D. Vulnérabilités contextuelles : les failles liées à l'environnement**

Ces vulnérabilités découlent du contexte dans lequel les processus cognitifs opèrent, notamment les influences sociales et culturelles.

*Polarisation sociétale* : la polarisation fragmente la conscience collective, rendant les sociétés plus vulnérables aux attaques cognitives. *Mécanisme* : les algorithmes de recommandation, les réseaux de bots comme les IA génératives amplifient les divisions en enfermant les individus dans des bulles informationnelles. *Vulnérabilité* : une société polarisée est moins capable de coopérer pour résister aux attaques (qu'elles aient pour origine des protagonistes exogènes ou endogènes). *Exemple* : les réseaux

sociaux ont désintégré la conscience collective américaine, rendant le dialogue entre démocrates et républicains presque impossible (Cass Sunstein).

*Manque de littératie cognitive* : le manque de formation à la pensée critique rend les individus plus vulnérables à la manipulation. *Mécanisme* : sans une éducation appropriée aux médias et à la détection des biais, les individus sont moins capables de distinguer le vrai du faux. *Vulnérabilité* : une population peu éduquée est plus vulnérable aux *fake news* et aux *deepfakes*. *Exemple* : les sociétés, les groupes sociaux ou les individus sujets à une faible littératie cognitive sont plus vulnérables aux campagnes de désinformation.

*Dépendance aux institutions* : la confiance dans les institutions (gouvernement, parlement, juridictions, administrations, médias « mainstream », organismes bancaires, ...) peut être exploitée pour manipuler les processus cognitifs. *Mécanisme* : les individus font confiance aux autorités instituées pour leur fournir des informations fiables. *Vulnérabilité* : une perte de confiance dans ces institutions peut déstabiliser une société ;

*Exemple* : Les campagnes de désinformation russes (2016–2024) ont érodé la confiance dans les médias traditionnels, affaiblissant ainsi les démocraties cibles.

**E. Vulnérabilités technologiques : les failles des systèmes artificiels**

Ces vulnérabilités découlent de l'utilisation croissante des technologies pour augmenter ou remplacer les processus cognitifs.

*Dépendance aux outils numériques* : l'utilisation excessive des technologies numériques (services numériques, réseaux sociaux, IA, BCI) peut altérer les processus cognitifs. *Mécanisme* : les algorithmes de recommandation renforcent les biais cognitifs et réduisent la diversité des idées. *Vulnérabilité* : une dépendance aux technologies et services numériques peut réduire l'autonomie cognitive, rendant les individus plus vulnérables à la manipulation (problème clé pour les systèmes éducatifs). *Exemples* : les utilisateurs de TikTok et à X sont exposés à des contenus de plus en plus extrêmes, amplifiant ainsi la polarisation sociétale. De même, les utilisateurs de Google ont perdu la capacité à retenir des informations, car ils savent qu'ils peuvent les retrouver en ligne (effet "*Google Effect*").

*Vulnérabilités des IA* : les systèmes d'IA peuvent être exploités pour manipuler les processus cognitifs. *Mécanisme* : les modèles génératifs sont l'objet de multitudes de biais (algorithmique, technologique, idéologique, méthodologique, ...) qui peuvent créer des contenus trompeurs à grande échelle. *Vulnérabilité* : les *deepfakes* et les *fake news* générées par IA sont de plus en plus difficiles à détecter. *Exemple* : Sora (OpenAI) peut générer des vidéos hyperréalistes en quelques secondes, rendant la détection des *deepfakes* de plus en plus difficile.

*Cybersécurité cognitive* : les systèmes de détection (détection des *deepfakes*, des bots) peuvent être contournés. *Mécanisme* : les attaquants (États, groupes criminels) améliorent en permanence leurs technologies pour contourner les défenses. *Vulnérabilité* : les détecteurs de *deepfakes* (comme les détecteurs de virus numériques) sont toujours en retard sur les générateurs de *deepfakes* (resp. générateurs de virus numériques). *Exemple* : les nouveaux modèles génératifs peuvent tromper tous les détecteurs pendant plusieurs jours, voire semaines.

**I-1.1.6 Une cartographie globale des vulnérabilités pour une défense intégrée**

Les processus cognitifs, bien que complexes et adaptatifs, présentent donc des vulnérabilités multiples et interconnectées, qui peuvent être exploitées par des attaques cognitives et cognitives.

Cette section a permis de cartographier ces vulnérabilités selon cinq axes :

| Catégorie     | Vulnérabilités clés                                                                 | Mécanismes sous-jacents                                                                  | Vecteurs d'exploitation                       | Exemples concrets                                        | Impact stratégique                                  |
|---------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------|-----------------------------------------------------|
| Structurelles | Plasticité cérébrale, limites de la connectivité, dépendance aux neurotransmetteurs | Modification des synapses, saturation des capacités de traitement, déséquilibre chimique | Neuroweapons, drogues, désinformation répétée | Implantation de faux souvenirs, dépendance aux narratifs | Manipulation durable des croyances et comportements |

| Catégorie             | Vulnérabilités clés                                                                 | Mécanismes sous-jacents                                                                                 | Vecteurs d'exploitation                                                        | Exemples concrets                                                           | Impact stratégique                                                        |
|-----------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Fonctionnelles</b> | Biais cognitifs, limites de la mémoire, limites de l'attention                      | Raccourcis mentaux, reconstruction des souvenirs, filtrage attentionnel                                 | Deepfakes, algorithmes de recommandation, surcharge informationnelle           | Fausse nouvelles, bulles informationnelles, paralysie décisionnelle         | Désinformation massive, polarisation sociétale                            |
| <b>Dynamiques</b>     | Fatigue et stress, états modifiés de conscience, dépendance aux technologies        | Augmentation du cortisol, réduction des défenses critiques, altération de la suggestibilité             | Campagnes de désinformation ciblées, <i>neuroweapons</i> , EMC induits         | Panique collective, lavage de cerveau, réduction de l'autonomie cognitive   | Déstabilisation sociale, contrôle mental                                  |
| <b>Contextuelles</b>  | Polarisation sociétale, manque de littératie cognitive, dépendance aux institutions | Amplification des divisions, manque de formation critique, perte de confiance                           | Réseaux de bots, désinformation massive, attaques ciblées sur les institutions | Désintégration de la conscience collective, affaiblissement des démocraties | Fragmentation sociale, perte de cohésion nationale                        |
| <b>Technologiques</b> | Dépendance aux outils numériques, vulnérabilités des IA, cybersécurité cognitive    | Modification du traitement de l'information, création de contenus trompeurs, contournement des défenses | IA générative, deepfakes, attaques sur les systèmes de détection               | Deepfakes indétectables, fake news à grande échelle, paralysie des défenses | Saturation de l'espace informationnel, perte de confiance dans les médias |

Cette cartographie des vulnérabilités permet de comprendre :

1. Pourquoi les attaques cognitives et cognitives sont si efficaces : Elles exploitent des failles structurelles des processus cognitifs ;
2. Comment elles opèrent : En ciblant des mécanismes spécifiques (neurobiologiques, physiques, algorithmiques) ;
3. Où elles frappent : Sur des vulnérabilités multiples (structurelles, fonctionnelles, dynamiques, contextuelles, technologiques) ;
4. Quand elles sont les plus efficaces : Dans des contextes de stress, de fatigue ou de polarisation ;
5. Qui peut en être la cible : Individus, groupes, sociétés, États.

Cette section a établi les fondations nécessaires pour comprendre la guerre cognitive et cognitive en :

1. Définissant la nature des processus cognitifs (neurobiologique, informationnelle, émergente) ;
2. Expliquant leurs fonctions (perception, mémoire, raisonnement, émotion, décision) ;
3. Analysant leurs mécanismes (neurobiologiques, physiques, algorithmiques) ;
4. Cartographiant leurs vecteurs (naturels, technologiques, chimiques, comportementaux) ;
5. Identifiant leurs vulnérabilités (structurelles, fonctionnelles, dynamiques, contextuelles, technologiques).

La section suivante approfondira les vulnérabilités cérébrales en s'appuyant sur cette base, en explorant comment les mécanismes neurobiologiques spécifiques (plasticité, neurotransmetteurs, ondes cérébrales) peuvent être exploités par la guerre cognitive.

## I-2. Distinction fondamentale : guerre cognitive vs. guerre cognitive

Maintenant que nous avons compris comment les systèmes cognitifs peuvent être attaqués, nous pouvons aborder qui mène ces attaques et comment elles se distinguent : la guerre cognitive (neurobiologique) et la guerre cognitive (informationnelle).

### I-2.1. La guerre cognitive : la manipulation directe du cerveau, fondement neurobiologique de la domination mentale

*Définition académique* : La guerre cognitive — au sens neurobiologique du terme — désigne l'ensemble des actions intentionnelles visant à altérer directement les processus neurobiologiques du cerveau humain, en utilisant des moyens scientifiques et techniques pour influencer la perception, la mémoire, le raisonnement, les émotions ou la prise de décision au niveau individuel.

Si la guerre cognitive cible les processus de pensée collectifs par le biais de l'information (voir *infra*), la guerre cognitive, elle, agit directement sur le substrat biologique de la pensée : le cerveau humain.

Contrairement à une attaque informationnelle, qui cherche à convaincre ou à tromper, la guerre cognitive force, altère ou contrôle les mécanismes neurobiologiques eux-mêmes, transformant le cerveau en un champ de bataille direct.

Cette approche *bottom-up* exploite les vulnérabilités les plus intimes de notre système nerveux pour détourner les processus naturels de la cognition — perception, mémoire, émotion, décision — et ainsi neutraliser l'autonomie mentale des individus ciblés.

Son arme principale ? La modulation ciblée des neurotransmetteurs, ces messagers chimiques qui régulent chaque aspect de notre fonctionnement mental.

Mais la guerre cognitive ne se limite pas à la chimie cérébrale. Elle déploie une stratégie multi-dimensionnelle combinant stimulation électromagnétique, interfaces cerveau-machine et substances neuroactives, comme le démontrent les travaux de Bernard Claverie et Baptiste Prébot sur les mécanismes de la manipulation neurobiologique.

### **I-2.1.1 Les mécanismes d'action : une attaque chirurgicale contre l'autonomie mentale**

La guerre cognitive déploie ses effets selon une progression systématique, où chaque mécanisme cible une faille spécifique du cerveau. Dans un premier temps, elle module les neurotransmetteurs, ces molécules qui régulent nos émotions, notre mémoire et notre prise de décision. La dopamine, par exemple, peut être stimulée par des ondes électromagnétiques de fréquences spécifiques (1,5–3 GHz) pour induire des états de dépendance artificielle à des narratifs manipulés. Un individu exposé à une telle stimulation, combinée à une campagne de désinformation ciblée, développe une adhésion compulsive aux informations reçues, même lorsqu'elles contredisent la réalité objective.

*Source : DARPA (2025), Études sur la modulation électromagnétique des circuits de récompense.*

Dans un second temps, la guerre cognitive stimule ou inhibe des zones cérébrales spécifiques. Le cortex préfrontal, siège des fonctions exécutives, peut être ciblé pour altérer la prise de décision, tandis que l'amygdale, centre de la peur, peut être stimulée pour induire des états de panique contrôlée. *Exemple historique* : le projet *Pandora* (CIA, 1965–1970) a démontré que des ondes micro-ondes pulsées pouvaient provoquer des hallucinations auditives et des troubles de l'équilibre chez des sujets humains, illustrant comment une stimulation ciblée peut désorienter une cible sans contact physique.

Enfin, la guerre cognitive altère les ondes cérébrales elles-mêmes. Les ondes thêta (4–8 Hz), associées à la relaxation et à la créativité, peuvent être stimulées pour induire un état de suggestibilité accrue, tandis que les ondes bêta (12–30 Hz), liées à la concentration, peuvent être perturbées pour provoquer une désorientation cognitive.

Ces mécanismes expliquent pourquoi les *neuroweapons* sont capables de contourner les défenses traditionnelles en agissant directement sur le substrat biologique de la pensée.

### **I-2.1.2 Les vecteurs technologiques : une panoplie neurobiologique au service de la manipulation**

Pour mener ces attaques, la guerre cognitive s'appuie sur un arsenal technologique varié, où chaque vecteur exploite une faille spécifique des mécanismes cérébraux : les *neuroweapons* (l'arme invisible par excellence), les interfaces cerveau-machine (BCI), la neurostimulation, les drogues neuroactives et les nanoneurotechnologies

Un soldat équipé d'une BCI pourrait voir ses capacités cognitives améliorées (mémoire, prise de décision), mais aussi contrôlées à distance par un adversaire, transformant ainsi une technologie médicale en arme de guerre cognitive. *Neuralink* pourrait permettre de contrôler des drones par la pensée, mais aussi de manipuler les états mentaux.

Un neurostimulateur portable pourrait être utilisé pour neutraliser temporairement un décideur ennemi lors d'une crise, sans laisser de trace physique.

Des nanoneurotechnologies pourraient être déployées pour contrôler à distance des agents ennemis ou saboter les capacités cognitives de décideurs stratégiques.

L'efficacité maximale de la guerre cognitive est atteinte lorsque ces vecteurs sont combinés de manière stratégique.

*Scénario type :*

Phase 1 (Préparation neurobiologique) : Des *neuroweapons* (ondes EM) altèrent légèrement l'activité cérébrale d'une cible, réduisant ses défenses critiques.

Phase 2 (Manipulation ciblée) : Une BCI ou une drogue neuroactive amplifie les effets en modulant des neurotransmetteurs spécifiques (ex. : dopamine pour la dépendance, sérotonine pour l'anxiété).

Phase 3 (Contrôle comportemental) : La combinaison des deux approches verrouille les effets, rendant la cible incapable de résister à la manipulation.

*Résultat* : Un contrôle effectif des états mentaux et des comportements, avec une efficacité multipliée par rapport à une attaque utilisant un seul vecteur.

### **I-2.1.3 La guerre cognitive comme menace existentielle pour l'autonomie mentale**

Au-delà des applications militaires, la guerre cognitive représente une menace fondamentale pour l'autonomie individuelle. En agissant directement sur le cerveau, elle contourne les défenses traditionnelles (éducation, esprit critique) et altère les mécanismes mêmes de la pensée.

Comme le souligne Bernard Claverie, la guerre cognitive ne vise pas à convaincre, mais à contrôler – et c'est ce qui en fait une menace sans précédent pour la souveraineté mentale des individus et des nations.

La guerre cognitive n'est donc pas seulement une menace pour les soldats ou les décideurs : c'est une menace pour l'essence même de ce qui fait de nous des êtres libres et autonomes.

### **I-2.2. La guerre cognitive : la manipulation des esprits à l'ère du tout-numérique**

*Définition académique* : La guerre cognitive — au sens informationnel du terme — désigne l'ensemble des actions intentionnelles visant à altérer les processus de pensée collectifs, en utilisant des moyens technologiques pour influencer la perception, les croyances et les comportements au niveau groupal ou sociétal.

Si la guerre cognitive agit directement sur le substrat biologique de la pensée, la guerre cognitive, elle, cible les processus de pensée collectifs, en exploitant les failles les plus subtiles de notre psyché et de nos systèmes d'information. Contrairement à une attaque physique, qui détruit ou neutralise, la guerre cognitive détourne, manipule et contrôle les flux informationnels pour façonner les perceptions, les croyances et, in fine, les comportements.

Son arme principale ? La désinformation massive, qui inonde l'espace mental avec des *fake news*, des *deepfakes* et des narratifs contradictoires, rendant impossible la distinction entre réalité et fiction. Mais la guerre cognitive ne se limite pas à la diffusion de fausses informations. Elle repose sur une stratégie multi-dimensionnelle combinant manipulation algorithmique, exploitation des biais cognitifs et saturation de l'espace informationnel, comme le démontrent les travaux de Cass Sunstein sur la polarisation des sociétés modernes.

#### **I-2.2.1 Les mécanismes d'action : une attaque en trois temps contre l'esprit critique**

La guerre cognitive déploie ses effets selon une progression insidieuse, où chaque étape prépare le terrain pour la suivante. Dans un premier temps, elle sature l'espace informationnel avec un volume de contenus tel que les mécanismes de filtrage et de vérification des individus s'effondrent. Le cerveau humain, confronté à une surcharge cognitive, voit ses capacités critiques désactivées, rendant les cibles plus réceptives aux manipulations.

*Exemple concret* : Pendant la guerre en Ukraine, des *deepfakes* du président Zelensky appelant à la reddition ont été diffusés sur les réseaux sociaux, semant la confusion parmi les populations et les troupes. Ces contenus, bien que rapidement démentis, ont créé un doute persistant illustrant comment la désinformation peut éroder la confiance dans les institutions même après sa réfutation.

Dans un second temps, la guerre cognitive exploite les biais cognitifs — ces distorsions systématiques de notre jugement qui font de nous des cibles si vulnérables. Parmi ces biais, certains sont particulièrement redoutables car ils amplifient les effets de la désinformation :

Le *bias de confirmation* pousse les individus à privilégier les informations qui confirment leurs croyances préexistantes, tandis que le biais de Dunning-Kruger les amène à surestimer leurs propres capacités, les rendant ainsi plus vulnérables aux manipulations. *Exemple* : un internaute convaincu de pouvoir détecter un *deepfake* à l'œil nu partagera en réalité un contenu synthétique, amplifiant ainsi sa diffusion et renforçant la désinformation.

Le *bias d'ancrage* fait que la première information reçue sur un sujet influence durablement les jugements ultérieurs, même si elle est fausse. *Application* : les campagnes de désinformation ciblent ce biais en diffusant en premier des informations erronées, qui s'enracinent dans l'esprit des individus malgré les démentis ultérieurs.

Le *bias de négativité* nous pousse à accorder plus d'importance aux informations négatives qu'aux informations positives, ce qui explique pourquoi les *fake news* anxiogènes (crises économiques, menaces sanitaires) se propagent si rapidement.

Enfin, la guerre cognitive sature l'espace informationnel via des réseaux de bots et le spam, créant un bruit de fond où toute information crédible devient indistinguable des fausses. En 2026, 15–20 % des comptes actifs sur Twitter/X sont des bots (Ferrara, 2017), amplifiant ainsi la désinformation de manière exponentielle.

### **I-2.2.2 Les vecteurs technologiques : une panoplie au service de la manipulation**

Pour mener ces attaques, la guerre cognitive s'appuie sur un arsenal technologique varié, où chaque vecteur exploite une faille spécifique des systèmes d'information et de la psyché humaine

Les *deepfakes* représentent aujourd'hui l'arme la plus redoutable de la guerre cognitive.

Les modèles d'IA générative ont révolutionné la guerre cognitive en permettant la création massive et personnalisée de contenus manipulés. *Application stratégique* : un message peut être personnalisé en fonction des biais cognitifs d'un individu (ex. : un conservateur sceptique recevra une *fake news* exploitant sa méfiance envers les médias traditionnels, tandis qu'un progressiste recevra un contenu ciblant sa sensibilité aux injustices sociales).

Les réseaux de bots constituent l'infanterie de la guerre cognitive.

Les algorithmes de recommandation jouent un rôle décisif mais souvent sous-estimé dans la guerre cognitive.

Avec l'émergence du métavers et des environnements de réalité virtuelle, la guerre cognitive entre dans une nouvelle dimension. Des opérations psychologiques pourraient être menées dans le métavers pour influencer des populations entières en créant des réalités alternatives contrôlées.

L'efficacité maximale de la guerre cognitive est atteinte lorsque ces vecteurs sont combinés de manière stratégique.

*Scénario type* :

1. Phase 1 (Préparation) : Une IA générative crée un *deepfake* ciblant un décideur politique.
2. Phase 2 (Amplification) : Un réseau de bots diffuse massivement ce *deepfake* sur les réseaux sociaux.
3. Phase 3 (Ancrage) : Les algorithmes de recommandation amplifient la visibilité du contenu en le proposant aux utilisateurs les plus vulnérables (ex. : ceux ayant déjà partagé des contenus similaires).

4. Phase 4 (Exploitation) : La désinformation, désormais virale, est reprise par des médias traditionnels, légitimant ainsi le faux récit.

Résultat : Une désinformation massive qui s'impose comme une réalité alternative, contre laquelle les contre-mesures traditionnelles (éducation, *fact-checking*) peinent à lutter.

### **I-2.2.3 La guerre cognitive comme menace sociétale**

Au-delà des individus, la guerre cognitive vise à fragmenter les sociétés en exploitant leurs divisions naturelles. En ciblant les biais cognitifs et en saturant l'espace informationnel, elle crée des réalités parallèles où chaque groupe vit dans sa propre bulle, rendant impossible le dialogue et la coopération.

Les travaux de Cass Sunstein montrent que les réseaux sociaux, en amplifiant les biais de confirmation, ont désintégré la conscience collective américaine, rendant le dialogue entre démocrates et républicains presque impossible.

La guerre cognitive n'est donc pas seulement une menace pour les individus : c'est une menace pour la cohésion même des sociétés et, in fine, pour la démocratie. Elle ne vise pas à détruire les corps, mais à corrompre les esprits – et c'est peut-être encore plus dangereux.

### **I-3. Différence de nature, complémentarité et synergie entre guerre cognitive et guerre cognitive**

**La guerre cognitive et la guerre cognitive sont deux concepts radicalement distincts, bien que souvent confondus dans les débats publics.** La distinction entre ces deux concepts ne relève pas d'une simple nuance terminologique, mais bien d'une différence ontologique : elles ne ciblent pas les mêmes substrats mécaniques, et ne produisent pas les mêmes effets., n'utilisent pas les mêmes. Schématiquement, la guerre cognitive est une guerre du cerveau (*bottom-up*), tandis que la guerre cognitive est une guerre des esprits (*top-down*).

Leur confusion conduit à des erreurs stratégiques, éthiques et juridiques majeures.

Pourquoi cette distinction est-elle fondamentale ?

#### *1. Niveaux d'atteinte radicalement différents :*

La guerre cognitive agit sur ce que les individus pensent (croyances, narratifs, décisions).

La guerre cognitive agit sur comment leur cerveau fonctionne (activité neuronale, processus neurobiologiques).

#### *2. Implications stratégiques opposées :*

La guerre cognitive est une arme de masse : elle vise des populations entières via des canaux informationnels (médias, réseaux sociaux).

La guerre cognitive est une arme de précision : elle vise des individus ou groupes spécifiques via des technologies matérielles ciblées (ondes, neurostimulation).

#### *3. Enjeux éthiques et juridiques incommensurables :*

La guerre cognitive peut (théoriquement) être régulée par des extensions du droit international humanitaire (ex. : interdiction de la propagande incitant à la haine ou à la violence).

La guerre cognitive échappe à tout cadre existant : elle traite le cerveau humain comme une cible militaire, sans équivalent dans les traités actuels (aucune convention n'interdit explicitement de cibler le cerveau).

#### *4. Irréversibilité différenciée :*

La guerre cognitive est réversible si des contre-mesures efficaces sont déployées.

La guerre cognitive est potentiellement irréversible si elle entraîne des lésions neurobiologiques permanentes.

#### *5. Acceptabilité sociale distincte :*

La guerre cognitive est déjà normalisée dans les conflits modernes (par exemple. : désinformation russe en Ukraine, campagnes chinoises contre Taïwan).

La guerre cognitive reste taboue mais en cours de banalisation (ex. : brevets militaires classifiés, tests opérationnels non reconnus).

Tableau comparatif : Deux paradigmes, deux niveaux d'atteinte

| Critère               | Guerre cognitive                                                                                                                                              | Guerre cognitive                                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Définition            | Manipulation psychologique et informationnelle des processus de pensée, de perception et de décision.                                                         | Ciblage physiologique et neurobiologique direct du cerveau humain via des technologies matérielles.                                                                                |
| Niveau d'atteinte     | Superstructures mentales (croyances, narratifs, raisonnement).                                                                                                | Infrastructures biologiques (neurones, réseaux cérébraux, activité synaptique).                                                                                                    |
| Mécanismes            | Désinformation, propagande, surcharge informationnelle, manipulation narrative, exploitation des biais cognitifs.                                             | Ondes électromagnétiques, neurostimulation (TMS, TES), nanotechnologies, armes psychotroniques, interférence neuronale directe.                                                    |
| Outils                | Médias sociaux, deepfakes, algorithmes de recommandation, IA générative, cyber-attaques sur les infrastructures informationnelles.                            | Armes à énergie dirigée (micro-ondes, lasers), dispositifs de neurostimulation, nanorobots, systèmes psychotroniques.                                                              |
| Effets                | Altération de la pensée rationnelle, polarisation sociale, érosion de la confiance institutionnelle, désorientation stratégique.                              | Modification directe des états de conscience (hallucinations, paralysie, suggestion forcée), lésions neurobiologiques (syndrome de La Havane), contrôle partiel des comportements. |
| Acteurs principaux    | OTAN (projet SPREADS), Russie (Unit 29155, IRA), Chine (Bureau de la Sécurité Internet), États-Unis (Cyber Command).                                          | États-Unis (DARPA NESD/TMS), Chine (Académie des Sciences Militaires), Russie (Institut Kourchatov), Israël (Rafael).                                                              |
| Cadre juridique       | Partiellement couvert par le droit international humanitaire (DIH) si effets psychologiques avérés (ex. : Convention de Genève sur la protection des civils). | Vide juridique total : Aucune convention ne régit spécifiquement les armes ciblant directement le cerveau.                                                                         |
| Seuil éthique franchi | Années 2010 (ex. : ingérence électorale russe, campagnes de désinformation massives).                                                                         | Années 2020 (ex. : déploiement opérationnel d'armes psychotroniques, syndrome de La Havane).                                                                                       |
| DéTECTABILITÉ         | Difficile (attribution des campagnes de désinformation, mais traces numériques exploitables).                                                                 | Extrêmement difficile (absence de traces physiques, effets retardés, attribution complexe).                                                                                        |
| Réversibilité         | Partielle (via éducation, contre-propagande, résilience cognitive).                                                                                           | Faible à nulle (risque de lésions neurobiologiques irréversibles).                                                                                                                 |
| Statut en 2026        | Déploiement opérationnel à grande échelle (doctrines militaires intégrées).                                                                                   | Phase de militarisation avancée (tests opérationnels documentés, déploiement limité mais croissant).                                                                               |

Bien que distinctes par nature, la guerre cognitive et la guerre cognitive ne sont pas antagonistes : elles sont complémentaires, et c'est précisément leur combinaison qui en fait une menace d'une efficacité sans précédent.

Imaginez un instant que vous êtes un décideur politique, submergé par un flot continu d'informations contradictoires. Votre téléphone vibre sans discontinuer : des alertes urgentes, des messages anonymes, des vidéos virales montrant vos alliés les plus proches en train de comploter contre vous. Les réseaux sociaux bruissent de rumeurs sur une crise imminente — une attaque terroriste ici, un coup d'État là. Votre esprit, déjà sollicité par cette charge cognitive, commence à douter de sa propre capacité à distinguer le vrai du faux. Puis, soudain, une migraine tenace s'installe, brouillant davantage votre jugement. Une pression sourde s'exerce sur vos tempes, comme si une force invisible cherchait à percer votre crâne. Vous ne le savez pas encore, mais vous venez de devenir la cible d'une opération cognitive intégrée — une attaque où la guerre cognitive (informationnelle) et la guerre cognitive (neurobiologique) se combinent pour éroder, pas à pas, votre souveraineté mentale.

Ce scénario n'est pas de la fiction. Il illustre la manière dont les deux modalités que nous avons distinguées peuvent s'articuler pour créer une menace multi-dimensionnelle, bien plus redoutable que la somme de ses parties.

### I-3.1 La synergie opérationnelle

L'OTAN-STO (2024) a démontré que les attaques les plus efficaces combinent les deux approches, en exploitant ce que l'on pourrait appeler un effet de résonance cognitive. La guerre cognitive (informationnelle) prépare le terrain en saturant l'espace informationnel et en désorientant les cibles. La guerre cognitive (neurobiologique) amplifie les effets en agissant directement sur les états mentaux des individus. *Résultat* : une déstabilisation exponentielle, bien supérieure à la somme des effets individuels.

*Exemple concret* (scénario validé par l'OTAN-STO, 2024) :

Phase 1 (Guerre cognitive) : Diffusion massive d'un *deepfake* vidéo ciblant un décideur politique (ex. : faux discours appelant à une crise nationale). *Vecteur* : IA générative (Sora 2.0). *Effet* : désinformation, perte de confiance.

Phase 2 (Guerre cognitive) : Utilisation de *neuroweapons* à ondes EM (1–3 GHz) pour induire un état de stress et d'anxiété chez les populations exposées. *Vecteur* : ondes électromagnétiques pulsées. *Effet* : amplification émotionnelle, désorientation.

Phase 3 (Synergie) : Exploitation des biais de confirmation et de la polarisation algorithmique pour amplifier la désinformation et paralyser la prise de décision.

*Résultat* : Contrôle effectif des comportements collectifs (efficacité multipliée par 3 à 5).

Maintenant que les fondations théoriques sont posées, il est temps d'explorer comment ces deux formes de guerre s'articulent concrètement dans la réalité stratégique. Le chapitre II prolongera ce cadre en analysant les dynamiques opérationnelles, les acteurs en présence, et les enjeux géopolitiques qui en découlent, tout en préparant le terrain pour le chapitre III, dédié aux fondements scientifiques sous-jacents.

## II -Prolongement du cadre théorique : dynamiques opérationnelles, acteurs et enjeux stratégiques

### Introduction : Du concept à la réalité du terrain

Le Chapitre I nous a permis d'établir une distinction claire entre guerre cognitive et guerre cognitive.

Ce Chapitre II prolonge ce cadre théorique en explorant comment ces concepts s'articulent en pratique, quels en sont les mécanismes opérationnels, les dynamiques stratégiques, et les implications concrètes pour les acteurs étatiques et non étatiques.

### II-1. Mécanismes opérationnels : L'articulation concrète des deux guerres

Pour comprendre comment la guerre cognitive et la guerre cognitive interagissent sur le terrain, il est nécessaire d'analyser leurs rôles respectifs dans une opération intégrée. La guerre cognitive agit comme un vecteur de préparation, tandis que la guerre cognitive intervient comme un amplificateur des effets.

#### II-1.1. La guerre cognitive comme vecteur de préparation des esprits

La guerre cognitive ne se contente pas de diffuser de fausses informations : elle prépare activement le terrain pour l'action de la guerre cognitive, en exploitant trois leviers principaux : la saturation de l'espace informationnel, l'exploitation des biais cognitifs, et la polarisation algorithmique.

##### II-1.1.1. La saturation de l'espace informationnel : submerger les défenses critiques

En inondant l'espace informationnel de contenus contradictoires, répétitifs et émotionnellement chargés, les attaquants surchargent les capacités critiques des individus et des groupes. Le cerveau humain, confronté à une surcharge cognitive, voit ses mécanismes de vérification et de filtrage s'affaiblir, voire s'éteindre. Ce phénomène, connu sous le nom de "fatigue informationnelle", réduit la capacité à distinguer le vrai du faux, rendant les cibles plus réceptives aux attaques ultérieures.

*Exemple concret* : l'Opération « *Infektion* » (Russie, 2016–2020) consista en une diffusion massive de *fake news* sur les réseaux sociaux, combinée à des *deepfakes* de personnalités politiques, visant à

désorienter les populations occidentales avant des élections. Elle eut pour résultat une baisse de 40 % de la confiance dans les médias traditionnels (*Reuters Institute for the Study of Journalism*, 2021).

**Impact stratégique** : les populations submergées par un flot d'informations contradictoires, deviennent moins capables de faire preuve d'esprit critique, ouvrant la porte à des manipulations plus profondes.

**Conséquence** : la guerre cognitive crée un bruit de fond informationnel qui rend les cibles plus vulnérables aux attaques neurobiologiques. En saturant l'esprit de stimuli contradictoires, elle réduit la capacité à distinguer le vrai du faux, préparant ainsi le terrain pour une intervention de la guerre cognitive.

### II-1.1.2. L'exploitation systématique des biais cognitifs : détourner les failles naturelles de l'esprit

Les biais cognitifs — ces distorsions systématiques de notre jugement — sont des leviers puissants pour la guerre cognitive. En les amplifiant, les attaquants peuvent orienter les perceptions de manière prédictible et affaiblir les défenses naturelles de l'esprit critique.

Ces biais sont aisément exploitables parce qu'ils sont intrinsèques au fonctionnement humain. Ils ne sont pas des défauts, mais des mécanismes d'économie cognitive qui permettent au cerveau de traiter rapidement l'information.

Cependant, ces mêmes mécanismes deviennent des failles lorsqu'ils sont amplifiés ou manipulés par des acteurs malveillants.

Biais cognitifs exploités en guerre cognitive et leurs implications

| Biais                             | Description                                                                                                                                               | Application en Guerre cognitive                                                                                                                                                                           | Exemple concret                                                                                                                                                                  | Impact stratégique                                                                                                |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Biais de confirmation</b>      | Tendance à privilégier les informations confirmant nos croyances préexistantes, tout en ignorant ou en minimisant les informations contradictoires.       | Les algorithmes de recommandation (YouTube, Facebook, TikTok) amplifient les contenus alignés avec les opinions existantes, créant des bulles idéologiques étanches.                                      | Un utilisateur croyant à une théorie du complot ne voit que des contenus la confirmant, renforçant sa conviction et le rendant moins réceptif aux informations contradictoires.  | Kahneman, D. (2011). <i>Thinking, Fast and Slow</i> . Farrar, Straus and Giroux. ISBN: 978-0374275631.            |
| <b>Effet Dunning-Kruger</b>       | Tendance des individus les moins compétents dans un domaine à surestimer leurs capacités, tandis que les plus compétents ont tendance à les sous-estimer. | Les <i>deepfakes</i> et la désinformation exploitent cette surconfiance pour faire croire à des individus qu'ils peuvent détecter des mensonges ou des manipulations, alors qu'ils en sont incapables.    | Un internaute convaincu de repérer un <i>deepfake</i> partagé en réalité un contenu synthétique, amplifiant sa diffusion et renforçant la désinformation.                        | Dunning, D. (2011). <i>The Dunning-Kruger Effect: On Being Ignorant of One's Own Ignorance</i> .                  |
| <b>Biais de négativité</b>        | Tendance à accorder plus de poids et d'attention aux informations négatives qu'aux informations positives ou neutres.                                     | Les campagnes de désinformation se concentrent sur des messages anxiogènes (crises économiques, menaces sanitaires, conflits imminents) pour capter l'attention et provoquer des réactions émotionnelles. | Diffusion de fausses alertes pandémiques ou de rumeurs de guerre pour créer un climat de peur généralisée et faciliter la manipulation.                                          | Rozin, P., & Royzman, E. B. (2001). <i>Negativity Bias, Negativity Dominance, and Contagion</i> .                 |
| <b>Effet de simple exposition</b> | Tendance à préférer ce qui nous est familier, même si c'est faux ou nuisible.                                                                             | La répétition de fausses informations les rend plus crédibles avec le temps, car le cerveau les associe à une familiarité rassurante.                                                                     | Répétition d'une <i>fake news</i> sur plusieurs plateformes (réseaux sociaux, médias complaisants) jusqu'à ce qu'elle soit acceptée comme vraie par une partie de la population. | Zajonc, R. B. (1968). <i>Attitudinal Effects of Mere Exposure</i> . Journal of Personality and Social Psychology. |

L'exploitation de ces biais permet à la guerre cognitive de préparer les esprits à accepter des informations fausses, voire à douter de la réalité elle-même. En ciblant ces mécanismes naturels, les attaquants peuvent contourner les défenses rationnelles et renforcer l'impact de leurs campagnes de désinformation.

### II-1.1.3 La polarisation algorithmique : fragmenter pour mieux régner

Les algorithmes de recommandation des plateformes numériques (YouTube, TikTok, Facebook, Twitter/X) jouent un rôle décisif dans la guerre cognitive. En amplifiant les contenus extrêmes et

émotionnels, ils fragmentent l'espace informationnel en bulles idéologiques étanches, où chaque individu est enfermé dans une réalité personnalisée.

Cette polarisation algorithmique est efficace car ces algorithmes sont conçus pour maximiser l'engagement — et les contenus polémiques, émotionnels ou conspirationnistes génèrent plus de clics, de likes et de partages que les informations neutres ou nuancées.

#### Impact des algorithmes de recommandation sur la polarisation

| Plateforme       | Mécanisme                                                                   | Effet sur la polarisation                                                                                                                                                      | Données clés                                                                                                             | Source                                                                                           |
|------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>YouTube</b>   | Recommandation de vidéos similaires ou plus extrêmes que celle visionnée.   | Radicalisation progressive : Les utilisateurs sont exposés à des contenus de plus en plus extrêmes, renforçant leurs croyances initiales.                                      | 70 % des vidéos recommandées sont plus extrêmes que celle initialement regardée.                                         | <i>Wall Street Journal</i> (2018). <i>YouTube's Algorithm Change</i> .                           |
| <b>TikTok</b>    | Favorise les contenus émotionnellement chargés (colère, peur, surprise).    | Amplification des émotions : Les utilisateurs sont exposés à des contenus conçus pour provoquer des réactions fortes, réduisant leur capacité à réfléchir de manière critique. | L'algorithme favorise les vidéos qui retiennent l'attention le plus longtemps, même si elles sont fausses ou trompeuses. | <i>The Guardian</i> (2022). <i>How TikTok's Algorithm Fuels Disinformation</i> .                 |
| <b>Twitter/X</b> | Amplification des contenus polémiques via les <i>bots</i> et les tendances. | Saturation de l'espace informationnel : Les messages extrêmes ou conspirationnistes sont 10 fois plus amplifiés que les messages neutres.                                      | 15–20 % des comptes actifs sont des <i>bots</i> (2026).                                                                  | Ferrara, E. (2017). <i>Disinformation and Social Bot Operations</i> . DOI:10.5210/fm.v22i5.7854. |

Cette polarisation algorithmique crée un terrain fertile pour l'intervention de la guerre cognitive. Une société divisée et méfiante est en effet plus vulnérable aux attaques neurobiologiques, car ses membres sont moins capables de coopérer pour y résister.

### II-1.3. La guerre cognitive comme amplificateur des effets

Une fois que la guerre cognitive a préparé le terrain, la guerre cognitive (neurobiologique) peut intervenir pour amplifier les effets de manière exponentielle. Cette amplification s'articule autour de trois mécanismes principaux : l'altération des capacités critiques, l'induction d'états émotionnels contrôlés, et la création de faux souvenirs.

#### II-1.3.1 L'altération des capacités critiques : affaiblir les défenses naturelles

Les *neuroweapons* peuvent dégrader temporairement les capacités cognitives des individus, les rendant moins capables de résister à la désinformation.

Cette altération cible spécifiquement les neurotransmetteurs, ces messagers chimiques qui régulent nos émotions, notre mémoire et notre prise de décision.

Pourquoi est-ce si efficace ? Parce que les neurotransmetteurs sont les leviers chimiques du cerveau. En les modulant, on peut contrôler les états mentaux avec une précision chirurgicale, contournant ainsi les défenses cognitives traditionnelles (éducation, esprit critique).

#### Neurotransmetteurs et leurs rôles dans la cognition

| Neurotransmetteur | Rôle principal                                 | Localisation cérébrale                                             | Fonctions cognitives associées                               | Effet d'une surcharge                                                               | Effet d'un déficit                                                                       |
|-------------------|------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Dopamine</b>   | Récompense, motivation, plaisir, apprentissage | Noyau accumbens, aire tegmentale ventrale (VTA), cortex préfrontal | Motivation, prise de décision, mémoire de travail, addiction | Addiction, comportements impulsifs, prise de décision hâtive, euphorie artificielle | Apathie, dépression, manque de motivation, anhedonie (incapacité à ressentir du plaisir) |

| Neurotransmetteur    | Rôle principal                                                  | Localisation cérébrale                                   | Fonctions cognitives associées                                               | Effet d'une surcharge                                                          | Effet d'un déficit                                                                              |
|----------------------|-----------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Sérotonine</b>    | Régulation de l'humeur, sommeil, appétit, digestion             | Noyaux du raphé, cortex préfrontal, hippocampe, amygdale | Régulation émotionnelle, stabilité de l'humeur, inhibition de l'agressivité  | Euphorie artificielle, sentiment de bien-être non justifié, désinhibition      | Dépression, anxiété, irritabilité, troubles du sommeil, troubles obsessionnels compulsifs (TOC) |
| <b>Noradrénaline</b> | Éveil, attention, réponse au stress (mécanisme de combat/fuite) | Locus coeruleus, cortex préfrontal, amygdale             | Vigilance, attention soutenue, mémoire à court terme, réaction au stress     | Hypervigilance, anxiété, paranoïa, panique, insomnie                           | Fatigue, léthargie, manque de concentration, dépression                                         |
| <b>GABA</b>          | Inhibition neuronale, calme, relaxation                         | Noyaux du thalamus, cortex cérébral, cervelet            | Réduction de l'anxiété, relaxation musculaire, stabilisation de l'humeur     | Sédation, ralentissement cognitif, somnolence, léthargie, confusion            | Anxiété, crises d'angoisse, épilepsie, tremblements                                             |
| <b>Glutamate</b>     | Excitation neuronale, apprentissage, mémoire                    | Cortex cérébral, hippocampe, amygdale                    | Transmission rapide des signaux, plasticité synaptique, mémoire à long terme | Hyperactivité cérébrale, crises épileptiques, neurotoxicité (dégâts neuronaux) | Déficits cognitifs, troubles de la mémoire, dépression, schizophrénie                           |
| <b>Acétylcholine</b> | Transmission neuromusculaire, éveil, mémoire                    | Noyaux basaux de Meynert, cortex cérébral, hippocampe    | Contrôle musculaire, attention, mémoire à court terme, apprentissage         | Hyperactivité motrice, tremblements, sueurs, hallucinations (ex. : BZ)         | Faiblesse musculaire, troubles de la mémoire, démence (ex. : maladie d'Alzheimer)               |

En altérant ces neurotransmetteurs, la guerre cognitive réduit la capacité des individus à résister à la désinformation. Elle affaiblit les défenses naturelles de l'esprit, rendant les cibles plus vulnérables aux attaques informationnelles.

Une personne dont les capacités critiques sont altérées sera par exemple moins susceptible de remettre en question une information fausse, même si elle est manifestement contradictoire.

Ces mécanismes expliquent pourquoi les *neuroweapons* (ondes EM, ultrasons, stimulation cérébrale) sont aussi redoutables : elles agissent directement sur les leviers chimiques du cerveau, contournant ainsi les défenses cognitives traditionnelles (éducation, esprit critique).

Une modulation ciblée de ces neurotransmetteurs permet de contrôler les émotions, d'altérer la mémoire, ou de dégrader la prise de décision — trois piliers de la souveraineté mentale.

### II-1.3.2 L'induction d'états émotionnels contrôlés : jouer sur les cordes sensibles de l'esprit

Les *neuroweapons* peuvent induire des états émotionnels spécifiques (peur, euphorie, apathie) pour renforcer l'impact de la guerre cognitive. Ces états sont particulièrement efficaces car ils contournent la raison et agissent directement sur les mécanismes limbiques du cerveau.

Exemples concrets d'induction émotionnelle

*Induction de peur* : des ondes électromagnétiques à 1–3 GHz peuvent stimuler l'amygdale, la région du cerveau responsable de la peur, provoquant un état de panique collective. *Exemple* : le projet « Pandora » (CIA, 1965–1970) a étudié l'utilisation de micro-ondes pour induire des hallucinations auditives et des états de terreur chez des sujets humains.

*Induction d'euphorie* : des *neuroweapons* ciblant la sérotonine ou la dopamine peuvent créer une fausse sensation de bien-être, rendant les individus plus réceptifs à la propagande ou aux suggestions. *Exemple* : utilisation de drogues psychotropes (comme le MDMA) pour faciliter l'implantation de faux souvenirs ou de croyances lors d'interrogatoires.

*Induction d'apathie* : des drogues ciblant le GABA (comme les benzodiazépines) ou des *neuroweapons* inhibitrices peuvent provoquer une paralysie décisionnelle, empêchant toute réaction efficace face à une

crise. *Exemple* : utilisation de sédatifs pour neutraliser des gardes ou des décideurs pendant une opération spéciale.

Ces états émotionnels amplifient l'impact de la désinformation en réduisant la capacité critique des individus. Une personne en état de peur ou d'euphorie artificielle est en effet moins susceptible de remettre en question les informations qu'elle reçoit, même si elles sont manifestement fausses ou contradictoires.

### **II-1.3.3 La création de faux souvenirs : réécrire le passé pour contrôler le présent**

La combinaison de *deepfakes* (guerre cognitive) et de neurostimulation (guerre cognitive) peut implanter de faux souvenirs dans l'esprit des cibles. Cette technique est particulièrement redoutable car elle altère la mémoire, l'un des piliers de l'identité et de la prise de décision.

Phase 1 (Guerre cognitive) : Diffusion d'un *deepfake* montrant un événement fictif (ex. : un politique dans une situation compromettante).

Phase 2 (Guerre cognitive) : Utilisation de *neuroweapons* (ondes EM ou ultrasons) pour stimuler l'hippocampe, la zone du cerveau responsable de la mémoire.

Le cerveau intègre le faux souvenir comme un souvenir réel, avec tous les détails émotionnels associés.

Des chercheurs de l'Université de Californie ont réussi à implanter de faux souvenirs chez des souris en stimulant l'hippocampe via l'optogénétique (*Nature Neuroscience*, 2013). La Darpa a piloté le Projet « *False Memory* » (2015–2020) dédié à l'exploration des possibilités d'implantation de faux souvenirs chez l'humain, avec des applications potentielles en interrogatoire et manipulation.

*Applications stratégiques* : Cette technique pourrait être utilisée pour discréditer des personnalités (en implantant de faux souvenirs de corruption ou de trahison), manipuler des populations entières (en réécrivant des événements historiques) ou encore, contrôler des agents (en leur faisant croire qu'ils ont commis des actes qu'ils n'ont pas commis).

## **II-2. Enjeux géopolitiques : Une menace pour la souveraineté mentale**

La guerre cognitive et cognitive ne se contente pas de menacer les individus ou les groupes : elle représente une menace systémique pour la souveraineté mentale des nations et des sociétés. Ces enjeux sont multi-dimensionnels, touchant à la fois les institutions civiles et militaires, les groupes sociaux et les individus.

Ces deux nouvelles modalités de la guerre trouvent des analogies puissantes dans les disruptions technologiques et sociétales à finalité (*a priori*) non polémogène qui traversent le XXI<sup>ème</sup> siècle.

Dans un article publié dans le Courrier de l'UNESCO, Nic Newman, chercheur associé à l'Institut Reuters pour l'étude du journalisme de l'université d'Oxford (Royaume-Uni), l'auteur principal du *Digital News Report* de 2012 à 2025 ainsi que d'un rapport annuel sur les tendances du journalisme, des médias et des technologies, a mis en perspective les assauts portés au journalisme et à l'information au cours des quinze dernières années.

*« L'une des tendances les plus marquantes de la dernière décennie est le recul de l'influence des médias traditionnels, notamment auprès des jeunes. Le public des journaux télévisés vieillit, la presse écrite décline et même les sites d'information peinent à fidéliser leurs utilisateurs. De plus en plus, on accède à l'actualité sur les réseaux sociaux, les plateformes vidéo, les applications, les agrégateurs de nouvelles ainsi que des moteurs de réponse alimentés par l'IA. »*

*Selon le [Digital News Report 2025](#) de l'Institut Reuters, les personnes qui s'informent sur les réseaux sociaux sont plus nombreuses que celles qui s'en remettent à la télévision. C'est une première aux États-Unis. Dans le monde entier, près de la moitié des moins de 25 ans déclarent désormais que les réseaux sociaux constituent leur principale source d'information — une tendance particulièrement marquée en Afrique, en Amérique latine et dans certaines régions d'Asie.*

*Près de la moitié des moins de 25 ans déclarent que les réseaux sociaux constituent leur principale source d'information*

*Parallèlement, l'IA générative transforme les usages. Ces nouveaux outils peuvent résumer et synthétiser des contenus sans que l'utilisateur n'ait besoin de consulter les sources originales. Les organes de presse, qui dépendaient depuis longtemps du trafic généré par les moteurs de recherche pour attirer des lecteurs et des revenus publicitaires, s'attendent à perdre près de la moitié de leur trafic dans les prochaines années, selon l'enquête [Digital Trends 2026](#) de l'Institut Reuters.*

*Ces évolutions surviennent alors même que l'industrie de l'information peine déjà à capter l'attention dans un environnement saturé d'informations, de divertissements et de distractions en tous genres. Dans cette « économie de l'attention », la concurrence ne vient pas seulement des autres médias, mais aussi des créateurs de contenu, des influenceurs, des streamers, des podcasteurs et autres fils personnalisés conçus pour capter l'audience.*

*De fait, l'actualité et la politique font de moins en moins recette. Selon le Digital News Report 2025, à l'échelle internationale, 40 % des personnes interrogées déclarent éviter parfois ou souvent les informations — contre 29 % en 2017. Elles expliquent que l'actualité leur donne souvent un sentiment d'impuissance, d'épuisement, d'anxiété ou de surcharge. D'autres jugent la couverture médiatique répétitive, trop négative ou décalée par rapport à leur quotidien. Ce désengagement menace le journalisme, mais aussi la démocratie elle-même. Lorsque les citoyens se détournent de l'information publique, ils sont plus exposés à la manipulation, aux théories complotistes et aux récits polarisants.*

*[...] Aujourd'hui, de nombreux publics — en particulier les jeunes utilisateurs — se fient davantage à des individus qu'à des institutions. Les créateurs de contenu, podcasteurs, youtubeurs, streamers et influenceurs sont devenus des voix puissantes dans l'espace public.*

*Certains de ces créateurs produisent un journalisme de qualité très suivi. D'autres se spécialisent dans le commentaire, le militantisme ou le journalisme d'opinion. Mais contrairement aux journalistes traditionnels, ils sont rarement soumis à des lignes éditoriales, des exigences de transparence ou des obligations d'équilibre et de vérification. Les frontières entre journalisme, divertissement et opinion se brouillent.*

*Cette « économie des créateurs » est accélérée par l'évolution des plateformes. Les réseaux sociaux deviennent moins sociaux et plus algorithmiques. De plus en plus, les utilisateurs voient des contenus qui ne proviennent plus de leurs proches, mais de créateurs sélectionnés par des systèmes de recommandation pilotés par l'IA. Les contenus centrés sur les personnalités fonctionnent souvent mieux que les reportages parce qu'ils sont plus divertissants, mais aussi parce qu'ils paraissent plus authentiques et plus proches du public.*

*[...] Parallèlement, la désinformation et la mésinformation gagnent du terrain. Notre enquête Digital News Report montre que l'inquiétude du public face aux contenus faux ou trompeurs progresse. Plus de la moitié des personnes interrogées (58 %) déclarent avoir du mal à distinguer le vrai du faux dans les actualités en ligne.*

*Désormais, l'IA générative menace d'intensifier ce phénomène en réduisant drastiquement le coût de production de faux textes, d'images, de fichiers audio et vidéo. Les deepfakes, les voix synthétiques et la propagande générée par IA ont déjà fait leur apparition dans des campagnes politiques. Mais le plus grand danger réside peut-être dans le volume. Internet risque d'être submergé par des contenus de faible qualité, sensationnalistes ou trompeurs. Si les citoyens ne savent plus à quelles sources se fier, l'autorité du reportage professionnel pourrait encore s'affaiblir. [...]. »<sup>5</sup>*

## **II-2.1 La souveraineté mentale : un nouvel enjeu stratégique**

La souveraineté mentale — la capacité d'un individu ou d'un groupe à contrôler ses propres processus de pensée — est devenue un enjeu stratégique majeur à l'ère de la guerre cognitive et la guerre cognitive qui ne sont pas des concepts abstraits ou spéculatifs.

Comme nous le verrons au chapitre III, elles reposent sur des mécanismes scientifiques concrets, exploitant les lois de la neuroscience, de la physique des ondes, et de l'informatique avancée pour cibler,

---

<sup>5</sup> Cf. Nic Newman - [Comment le journalisme peut-il se réinventer ?](#) – Le Courrier de l'UNESCO

manipuler et contrôler les processus mentaux humains, soit en sélectionnant des cibles précises, soit en généralisant les attaques à une population élargie.

La manipulation de masse ne date pas de la période contemporaine. Ses mécanismes sont connus :

Cadrage (*framing*) : présenter un même fait selon un angle émotionnel ou moral (victimes/coupables, menace/sauvetage).

Simplification & slogans : réduire des sujets complexes à des formules courtes faciles à répéter.

Charge émotionnelle : susciter peur, colère, humiliation ou espoir intense pour court-circuiter le raisonnement.

Désinformation / rumeur : diffuser des faits faux ou invérifiables, parfois via des “captures” ou extraits

*Cherrypicking* (sélection de données) : n’afficher que les éléments qui vont dans le sens du récit, en omettant le reste.

Faux consensus / autorité : “*tout le monde sait que...*”, “*des experts disent...*”, sans preuves vérifiables.

Polarisation & faux choix : pousser “*soit vous êtes avec nous, soit vous êtes contre*” en excluant les nuances.

Boucles de confirmation : ne montrer que ce qui confirme ce que le public croit déjà (*echo chambers*).

Boucs émissaires : désigner un groupe ou une cause comme responsable de problèmes complexes.

Escalade & urgence : pousser à agir vite (“*immédiatement*”, “*danger maintenant*”) avant vérification.

Pourquoi la souveraineté mentale est-elle cruciale ? Contrairement aux guerres traditionnelles, qui visent les territoires ou les ressources, la guerre cognitive et cognitive cible directement l’esprit humain, le substrat même de la pensée et de la décision. Les dégâts causés par ces attaques peuvent être permanents : troubles psychiatriques (dépression, anxiété chronique) ; faux souvenirs implantés ; altération permanente des capacités cognitives. Les attaques sont souvent invisibles (ondes EM, ultrasons), difficiles à attribuer (désinformation diffuse, réseaux de bots) et silencieuses (pas de trace physique évidente).

La souveraineté mentale est donc aussi importante que la souveraineté territoriale. Elle doit être protégée avec la même rigueur que les frontières nationales ou les infrastructures critiques.

## II-2.2 Les risques pour les démocraties

Les démocraties sont particulièrement vulnérables à la guerre cognitive comme à la guerre cognitive, car elles reposent sur trois piliers fondamentaux : la confiance dans les institutions (gouvernement, parlement, administration, juridictions, experts), l’accès à une information fiable (liberté, éthique, transparence et professionnalisme des médias) et la capacité des citoyens à prendre des décisions éclairées (éducation, esprit critique).

### Risques majeurs pour les démocraties

| Risque                            | Description                                                                                           | Exemple                                                                                           | Impact                                                                                     | Source                                                                |
|-----------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Érosion de la confiance</b>    | Perte de confiance dans les médias, les gouvernements, les experts et les institutions démocratiques. | Campagnes de désinformation russes (2016–2024) ciblant les élections en Europe et aux États-Unis. | Affaiblissement des institutions démocratiques, montée du populisme, polarisation sociale. | OTAN-STO (2023). <i>The Impact of Disinformation on Democracies</i> . |
| <b>Polarisation sociale</b>       | Division de la société en groupes antagonistes et imperméables, incapables de dialoguer.              | Réseaux sociaux (YouTube, Facebook, TikTok) amplifiant les contenus extrêmes.                     | Incapacité à trouver des compromis politiques, paralysie des systèmes démocratiques.       | Pariser, E. (2011). <i>The Filter Bubble</i> .                        |
| <b>Manipulation des élections</b> | Influence sur les résultats électoraux via la désinformation, les                                     | Élection présidentielle américaine (2016, 2020),                                                  | Légitimité des gouvernements remise en cause, instabilité                                  | Rapport du Sénat américain (2020).                                    |

| Risque                         | Description                                                                                          | Exemple                                                                               | Impact                                                                                                      | Source                                                                     |
|--------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
|                                | <i>deepfakes</i> et les réseaux de bots.                                                             | référendum sur le Brexit (2016).                                                      | politique, perte de confiance dans le processus démocratique.                                               | <i>Russian Interference in the 2016 U.S. Election.</i>                     |
| <b>Paralysie décisionnelle</b> | Incapacité des décideurs (politiques, militaires, économiques) à prendre des décisions rationnelles. | <i>Neuroweapons</i> ciblant des dirigeants, désinformation massive pendant une crise. | Crises politiques et économiques, perte de contrôle sur les événements, instabilité nationale.              | OTAN-STO (2024). <i>Cognitive Warfare and Decision-Making.</i>             |
| <b>Perte de souveraineté</b>   | Influence étrangère sur les processus décisionnels nationaux (élections, politiques publiques).      | Campagnes de désinformation chinoises en Afrique, ingérence russe en Europe de l'Est. | Dépendance géopolitique accrue, perte d'autonomie stratégique, alignement forcé sur des intérêts étrangers. | Rapport de l'UE (2023). <i>Foreign Interference in European Elections.</i> |

Ces risques menacent la stabilité même des démocraties. Sans une réponse adaptée, les sociétés ouvertes pourraient devenir vulnérables face à des acteurs autoritaires, qui utilisent ces armes pour saper les fondements de la démocratie : la confiance, le débat rationnel et la prise de décision éclairée.

## II-2.3 Les risques pour les individus

Les individus sont en première ligne face à la guerre cognitive et cognitive. Leurs libertés fondamentales — accès libre à une information fiable, liberté de pensée, autonomie décisionnelle, intégrité mentale — sont directement menacées.

### Risques majeurs pour les individus

| Risque                               | Description                                                                                    | Exemple                                                                                  | Impact                                                                                  | Source                                                                                                         |
|--------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Perte de souveraineté mentale</b> | Incapacité à contrôler ses propres pensées et émotions, manipulation par des acteurs externes. | Manipulation via <i>neuroweapons</i> (ondes EM) ou désinformation massive.               | Dépression, anxiété chronique, troubles psychiatriques, perte d'autonomie.              | Claverie & Prébot (2026). <i>La guerre cognitive de bas niveau : la guerre des cerveaux.</i>                   |
| <b>Désorientation cognitive</b>      | Incapacité à distinguer le vrai du faux, perte de repères.                                     | Exposition à des <i>deepfakes</i> et à des <i>fake news</i> contradictoires.             | Prise de décisions erronées, perte de confiance en soi, isolement social.               | ANSSI (2023). <i>Détection des Cyberattaques Cognitives.</i>                                                   |
| <b>Dépendance technologique</b>      | Dépendance aux outils numériques (réseaux sociaux, IA, BCI).                                   | Algorithmes de recommandation (TikTok, YouTube), neurostimulation addictive.             | Réduction de l'autonomie cognitive, perte de capacité à penser de manière indépendante. | Pariser, E. (2011). <i>The Filter Bubble.</i>                                                                  |
| <b>Manipulation émotionnelle</b>     | Contrôle des émotions par des acteurs externes (États, groupes criminels).                     | <i>Neuroweapons</i> ciblant l'amygdale, réseaux sociaux exploitant la peur ou la colère. | Comportements impulsifs ou irréfléchis, perte de libre arbitre, vulnérabilité accrue.   | George, M. S., & Aston-Jones, G. (2010). <i>Noninvasive Techniques for Probe Brain Function.</i>               |
| <b>Atteintes à la vie privée</b>     | Accès non autorisé aux pensées ou aux souvenirs (via BCI, neuro-espionnage).                   | Piratage de dispositifs BCI, utilisation de <i>neuroweapons</i> pour lire les pensées.   | Violation des droits fondamentaux, perte d'intimité mentale, risque de chantage.        | Nicolelis, M. A. L. (2011). <i>Beyond Boundaries: The New Neuroscience of Connecting Brains with Machines.</i> |

Ces risques menacent le bien-être mental et la liberté individuelle. Ils soulèvent des questions éthiques fondamentales sur les limites de la manipulation mentale et la protection des droits de l'homme à l'ère numérique. La souveraineté mentale individuelle doit donc être protégée au même titre que les autres droits fondamentaux.

On voit donc que la guerre cognitive et cognitive représente une menace multi-dimensionnelle, qui nécessite une réponse stratégique intégrée, combinant défenses technologiques, éducation critique et coopération internationale.

## III - Fondements scientifiques (mécanismes neurobiologiques et technologies de la guerre cognitive et cognitive)

Introduction : La science derrière la manipulation de l’esprit

Ce chapitre explore les vulnérabilités cérébrales (architecture neurobiologique, neurotransmetteurs, plasticité), les technologies offensives (*neuroweapons*, IA générative, *deepfakes*, réseaux de bots) ainsi que les contre-mesures scientifiques (détection, neuroprotection, résilience cognitive).

Parce que la guerre cognitive est une réalité physique et biologique, où la science devient une arme, comprendre ces mécanismes, c’est démystifier la menace et se doter des moyens indispensables pour préparer des défenses adaptées.

III-1. Le cerveau comme champ de bataille : une architecture vulnérable

Le cerveau humain est un système d’une complexité inégalée, capable de raisonnement abstrait, de créativité et d’adaptation. Pourtant, cette même complexité recèle des failles structurelles qui en font une cible idéale pour les attaques cognitives.

III-1.1 L’organisation hiérarchique du cerveau et ses failles exploitables (Claverie & Prébot, 2026)

Les travaux de Bernard Claverie et Baptiste Prébot ont mis en lumière une architecture cérébrale hiérarchisée, où chaque niveau présente des vulnérabilités spécifiques exploitables par les attaques cognitives.

III-1.1.1 Les trois niveaux neurobiologiques

Niveaux neurobiologiques et leurs vulnérabilités exploitables

| Niveau                                           | Fonction principale                                     | Processus cognitifs associés                                            | Vulnérabilités exploitables                                                                      | Technologies d’attaque associées                                                                                       | Exemple concret                                                                                                                                                              | Impact stratégique                                                                                                                    |
|--------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Niveau 1 :<br>Système nerveux autonome végétatif | Survie de l’individu (homéostasie, besoins primaires)   | Régulation corporelle, réactions instinctives (combat/fuite)            | Déséquilibre physiologique (stress chronique, fatigue, dépendance, troubles du sommeil)          | Stimulation électromagnétique (basses fréquences 0,1–100 Hz), neurotoxines (ex. : BZ, sarin), infrasons (7–18 Hz)      | Moscow Signal (1972–1989) : micro-ondes pulsées (2,5–4 GHz) provoquant maux de tête, troubles du sommeil, altération de la mémoire chez le personnel diplomatique américain. | Affaiblissement des capacités physiques et cognitives, rendant les cibles plus vulnérables aux attaques ultérieures.                  |
| Niveau 2 :<br>Système psycho-affectif            | Gestion des émotions et des relations interpersonnelles | Peur, empathie, motivation, sentiment de soi, régulation de l’humeur    | Manipulation émotionnelle (anxiété, euphorie artificielle, apathie, désorientation émotionnelle) | Ondes EM (1–10 GHz), musique répétitive (ex. : binaural beats), <i>deepfakes</i> émotionnels, désinformation anxiogène | Projet Pandora (CIA, 1965–1970) : micro-ondes induisant des hallucinations auditives et des états de terreur.                                                                | Déstabilisation émotionnelle à grande échelle, facilitant la manipulation collective (ex. : panique généralisée, perte de confiance). |
| Niveau 3 :<br>Système cognitif supérieur         | Pensée réflexive, raisonnement, mémoire                 | Analyse, synthèse, prise de décision, métacognition, mémoire épisodique | Altération cognitive (biais amplifiés, erreurs de jugement, désorientation, faux souvenirs)      | IA générative (LLM, VLM), <i>deepfakes</i> historiques, désinformation ciblée, algorithmes de recommandation           | Campagnes de désinformation russes (2016–2024) exploitant le biais de confirmation pour renforcer des croyances erronées.                                                    | Polarisation sociétale, perte de capacité critique, manipulation des comportements collectifs.                                        |

Cette organisation hiérarchique révèle que les attaques cognitives les plus efficaces combinent des actions sur plusieurs niveaux simultanément.

Par exemple : une campagne de désinformation (niveau 3) peut saturer l’espace informationnel et désorienter les cibles ; des ondes EM (niveau 2) peuvent amplifier les effets en induisant un état de stress

ou d'anxiété. Le résultat est une déstabilisation exponentielle, où chaque niveau renforce l'impact des autres.

*Conséquence stratégique* : les attaques cognitives exploitent les failles naturelles du cerveau pour créer des effets multi-dimensionnels, bien plus redoutables que la somme de leurs parties.

### III-1.1.2 Cartographie des zones cérébrales ciblées

Pour comprendre comment les attaques cognitives agissent sur le cerveau, il est essentiel de cartographier les zones cérébrales et leurs vulnérabilités spécifiques.

#### Zones cérébrales ciblées par la guerre cognitive

| Lobe                  | Zone ciblée                | Fonction principale                                                      | Vulnérabilité exploitée                                                                                                | Technologie d'attaque associée                                                                                  | Impact d'une attaque réussie                                                           | Contre-mesures                                                                    |
|-----------------------|----------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Lobe frontal</b>   | Cortex préfrontal (CPF)    | Raisonnement, prise de décision, contrôle inhibiteur, planification      | Biais cognitifs : Surcharge et paralysie décisionnelle sous un flux d'informations contradictoires.                    | Désinformation ciblée, neurostimulation (TMS), ondes EM (1–3 GHz)                                               | Paralysie décisionnelle (ex. : un décideur incapable d'agir face à une crise).         | Éducation critique, formation à la pensée systémique.                             |
| <b>Lobe frontal</b>   | Cortex orbitofrontal (COF) | Émotions, évaluation des récompenses et des risques                      | Manipulation émotionnelle : Déséquilibre de la prise de décision sous l'effet de stimuli émotionnels (peur, euphorie). | <i>Deepfakes</i> émotionnels, propagande ciblée, ondes EM (1–10 GHz)                                            | Décisions impulsives (ex. : achats paniqués, votes émotionnels, réactions de panique). | Neuroprotection (blindage EM), éducation émotionnelle.                            |
| <b>Lobe temporal</b>  | Hippocampe                 | Mémoire épisodique (souvenirs des événements vécus), navigation spatiale | Faux souvenirs : Implantation de souvenirs erronés via des informations répétées ou des <i>deepfakes</i> .             | <i>Deepfakes</i> historiques, répétition systématique de désinformation, neurostimulation (ultrasons focalisés) | Réécriture de la mémoire collective (ex. : croyance en des événements fictifs).        | Preuves irréfutables (blockchain, archives numériques), thérapies cognitives.     |
| <b>Lobe temporal</b>  | Amygdale                   | Traitement des émotions (peur, agressivité), mémoire émotionnelle        | Conditionnement de la peur : Induction d'un état de panique ou d'anxiété généralisée.                                  | <i>Neuroweapons</i> (ondes EM, ultrasons), désinformation anxiogène, musique répétitive                         | Peur généralisée (ex. : panique financière, crise sociale, paralysie des populations). | Neuroprotection (blindage EM, casques Faraday), éducation à la gestion du stress. |
| <b>Lobe pariétal</b>  | Cortex pariétal postérieur | Attention, intégration sensorielle, conscience spatiale                  | Surcharge attentionnelle : Impossibilité de se concentrer sous un flux d'informations saturant.                        | Spam informationnel, réseaux de bots, <i>deepfakes</i> en temps réel                                            | Incapacité à se concentrer (ex. : désorientation des soldats ou des décideurs).        | Filtres automatiques (détection des <i>deepfakes</i> , analyse des métadonnées).  |
| <b>Lobe occipital</b> | Cortex visuel (V1, V2, V3) | Traitement visuel (formes, couleurs, mouvements)                         | Illusions visuelles : Altération de la perception via des images synthétiques ou des stimuli lumineux.                 | <i>Deepfakes</i> vidéo, réalité augmentée malveillante, lasers stroboscopiques                                  | Croyance en des événements fictifs (ex. : confusion entre réalité et fiction).         | Détection automatique (analyse des artefacts visuels), éducation aux médias.      |

*Exemple concret d'attaque multicouche* : une campagne de désinformation moderne ne se contente pas de diffuser une *fake news*. Elle combine un *deepfake* vidéo (ciblant le cortex visuel pour tromper la perception), un récit émotionnel (ciblant l'amygdale pour provoquer la peur ou l'indignation), une diffusion massive via des bots (ciblant le cortex pariétal pour surcharger l'attention) et une répétition systématique (ciblant l'hippocampe pour ancrer un faux souvenir). *Résultat* : une manipulation globale affectant la perception, les émotions, l'attention et la mémoire.

Les contre-mesures doivent par conséquent être multidimensionnelles :

Pour le cortex visuel → Détection automatique des *deepfakes*.

Pour l'amygdale → Neuroprotection (casques anti-ondes).

Pour le cortex pariétal → Filtrage des informations.

Pour l'hippocampe → Vérification systématique (blockchain, archives).

### III-1.2 Les neurotransmetteurs : les leviers chimiques de la manipulation

Les neurotransmetteurs sont les messagers chimiques qui régulent nos émotions, notre mémoire et notre prise de décision. Leur modulation artificielle — qu'elle soit induite par des *neuroweapons*, des drogues ou des stimuli informationnels — permet de contrôler les états mentaux avec une précision chirurgicale.

#### III-1.2.1 Exploitation des neurotransmetteurs en guerre cognitive

##### Neurotransmetteurs et leurs exploitations en guerre cognitive

| Neurotransmetteur    | Technologies de manipulation                                                                                                              | Mécanisme d'action                                                                                              | Effet sur la cognition                                                                                                                                                                           | Impact stratégique                                                                          | Exemple concret                                                                                                                                      |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dopamine</b>      | Algorithmes de recommandation (YouTube, TikTok, Facebook), drogues dopaminergiques (amphétamines, cocaïne)                                | Augmentation de la libération de dopamine dans le noyau accumbens → activation du système de récompense.        | Renforcement des biais cognitifs (ex. : biais de confirmation, Dunning-Kruger) via une boucle de récompense artificielle. Addiction aux réseaux sociaux, réduisant la capacité à se déconnecter. | Polarisation sociétale, radicalisation, dépendance technologique.                           | Réseaux sociaux : 70% des vidéos recommandées par YouTube sont plus extrêmes que celles initialement regardées ( <i>Wall Street Journal</i> , 2018). |
| <b>Sérotonine</b>    | <i>Neuroweapons</i> (ondes EM à 1–10 GHz), désinformation positive (propagande de bonheur), drogues sérotoninergiques (MDMA, LSD)         | Modulation des récepteurs 5-HT <sub>2A</sub> → altération de la régulation de l'humeur et de la perception.     | Déstabilisation émotionnelle à grande échelle, rendant les populations plus suggestibles et moins critiques. Euphorie artificielle → acceptation accrue de la propagande.                        | Manipulation collective, perte de capacité critique, vulnérabilité aux attaques cognitives. | Projet <i>Pandora</i> (CIA, 1965–1970) : ondes micro-ondes induisant des états de bien-être artificiel.                                              |
| <b>Noradrénaline</b> | Neurostimulation (TMS, ultrasons focalisés), désinformation anxiogène (fausses alertes de crise), drogues noradrénergiques (amphétamines) | Augmentation de la libération de noradrénaline dans le locus coeruleus → activation du système de combat/fuite. | Peur généralisée, hypervigilance, paranoïa → paralysie décisionnelle ou réactions de panique collective.                                                                                         | Contrôle des foules, neutralisation de décideurs, déstabilisation politique.                | Campagnes de désinformation russes (2016–2024) : fausses alertes de crise sanitaire ou militaire pour induire un climat de peur.                     |
| <b>GABA</b>          | <i>Neuroweapons</i> inhibitrices (ondes EM basses fréquences, ultrasons), drogues sédatives (benzodiazépines, barbituriques)              | Augmentation de l'activité du GABA → inhibition de l'activité neuronale.                                        | Paralysie cognitive, sédation, ralentissement des réactions → neutralisation temporaire de cibles (décideurs, soldats).                                                                          | Neutralisation stratégique, incapacité à réagir à une crise.                                | Opération <i>Sleeping Beauty</i> (hypothétique) : utilisation de gaz sédatifs pour neutraliser des gardes ou des dirigeants.                         |
| <b>Glutamate</b>     | Stimulation excessive (ultrasons, ondes EM haute fréquence), drogues stimulantes (cocaïne, amphétamines), neurotoxines (acide kaïnique)   | Augmentation de l'activité du glutamate → excitation excessive des neurones → neurotoxicité.                    | Surcharge mentale, <i>burn-out</i> collectif, altération des capacités d'analyse et de prise de décision.                                                                                        | Affaiblissement des institutions, perte de productivité, crises économiques.                | Attaques par ultrasons (DARPA, 2020) : stimulation du cortex préfrontal pour induire une surcharge cognitive.                                        |
| <b>Acétylcholine</b> | <i>Neuroweapons</i> (ondes EM à 1–3 GHz), drogues anticholinergiques (BZ, scopolamine)                                                    | Blocage des récepteurs muscariniques de l'acétylcholine → perturbation de la mémoire et de la perception.       | Confusion mentale, hallucinations, amnésie antérograde (incapacité à former de nouveaux souvenirs).                                                                                              | Désorientation massive, perte de capacité critique, manipulation des comportements.         | Projet <i>MKUltra</i> (CIA, 1953–1973) : utilisation de BZ pour induire des états de confusion et d'amnésie.                                         |

Ces mécanismes expliquent pourquoi les *neuroweapons* (ondes EM, ultrasons, stimulation cérébrale) sont aussi redoutables : elles agissent directement sur les leviers chimiques du cerveau, contournant ainsi les défenses cognitives traditionnelles (éducation, esprit critique).

Une modulation ciblée de ces neurotransmetteurs permet de contrôler les émotions (ex. : noradrénaline → peur ; sérotonine → euphorie), d'altérer la mémoire (ex. : glutamate → surcharge cognitive ; acétylcholine → amnésie) et de dégrader la prise de décision (ex. : dopamine → impulsivité ; GABA → paralysie).

Ces trois piliers (émotions, mémoire, prise de décision) constituent la base de la souveraineté mentale.

### III-1.2.2 Le modèle des "4 stades de dégradation cognitive"

Pour évaluer l'impact des attaques cognitives, nous proposons un modèle en 4 stades, inspiré des travaux en neurosciences cliniques et en psychologie cognitive.

Ce modèle permet de comprendre la dynamique des attaques, d'identifier les mécanismes neurobiologiques en jeu à chaque étape et d'adapter les contre-mesures en fonction du stade atteint.

Modèle des 4 stades de dégradation cognitive

| Stade | Nom                   | Description                                                                                                                                                                                                        | Mécanismes neurobiologiques                                                                                                                                                    | Technologies associées                                                                                                                                   | Exemples concrets                                                                                                                                                         | Contre-mesures recommandées                                                                                                                     |
|-------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | <b>Exposition</b>     | Premier contact avec un stimulus manipulé (information ou signal neurobiologique). Le cerveau perçoit le stimulus, mais celui-ci n'a pas encore été intégré dans les processus cognitifs.                          | Activation des cortex sensoriels (visuel, auditif, somatosensoriel) → traitement initial du stimulus.                                                                          | Désinformation, <i>deepfakes</i> , réseaux de bots, <i>neuroweapons</i> légères (ondes EM de faible intensité, infrasons)                                | Vision d'un <i>deepfake</i> sur les réseaux sociaux, exposition à une onde EM de faible puissance.                                                                        | Filtres automatiques (détection précoce des <i>deepfakes</i> , analyse des métadonnées, détection des ondes EM).                                |
| 2     | <b>Pénétration</b>    | Intégration partielle du stimulus dans les processus cognitifs (mémoire à court terme, émotions, attention). Le cerveau commence à traiter l'information comme crédible, mais de manière temporaire et réversible. | Modification des connexions synaptiques (plasticité synaptique) → libération de neurotransmetteurs (dopamine, noradrénaline) → renforcement temporaire des circuits neuronaux. | Désinformation répétée, algorithmes de recommandation, neurostimulation légère (TMS, ultrasons), ondes EM modérées.                                      | Adoption temporaire d'une croyance fausse après avoir vu une <i>fake news</i> plusieurs fois, sentiment d'anxiété après exposition à une désinformation anxiogène.        | Éducation critique (formation à la pensée critique, diversité des sources, vérification factuelle).                                             |
| 3     | <b>Ancrage</b>        | Intégration complète du stimulus dans les croyances, mémoires ou comportements à long terme. Le cerveau accepte durablement la croyance ou le comportement induit par l'attaque.                                   | Renforcement des circuits neuronaux (plasticité structurelle) → création de nouveaux souvenirs (neurogenèse dans l'hippocampe) → déséquilibre chimique durable.                | Désinformation massive, <i>deepfakes</i> historiques, conditionnement émotionnel, algorithmes de bulles informationnelles, <i>neuroweapons</i> modérées. | Adoption permanente d'une théorie du complot après exposition prolongée à une propagande ciblée, création d'un faux souvenir collectif via un <i>deepfake</i> historique. | Preuves irréfutables (blockchain, archives numériques, témoignages croisés), thérapies cognitives (rééducation, déprogrammation).               |
| 4     | <b>Dégénérescence</b> | Altération permanente des capacités cognitives (raisonnement, mémoire, prise de décision). Le cerveau subit des dégâts structurels irréversibles.                                                                  | Dégâts neuronaux (neurotoxicité due au glutamate) → atrophie cérébrale (réduction du volume de l'hippocampe ou du cortex préfrontal) → déséquilibre chimique chronique.        | <i>Neuroweapons</i> avancées (ondes EM haute intensité, ultrasons focalisés), drogues cognitives (neurotoxines), désinformation à long terme.            | Incapacité à distinguer le vrai du faux, paralysie décisionnelle chronique, troubles psychiatriques (dépression, anxiété, psychose).                                      | Neuroprotection (blindage électromagnétique, casques anti-ondes, antidotes), rééducation cognitive (thérapies comportementales, neurofeedback). |

Ce modèle offre un cadre précis pour comprendre la progression des attaques combinées guerre cognitive/guerre cognitive.

#### Stade 1 : *La désorientation informationnelle*

Au premier stade, la guerre cognitive (informationnelle) sature l'espace mental de l'individu ou du groupe avec des informations contradictoires, des *deepfakes*, et des narratifs conflictuels. *Mécanismes* : surcharge informationnelle du cortex préfrontal, exploitation des biais cognitifs (confirmation, ancrage). *Indicateurs* : augmentation du temps passé à vérifier les informations, réduction de la confiance dans les sources traditionnelles. *Contre-mesures* : filtres informationnels, éducation aux médias, limitation de l'exposition.

#### Stade 2 : *L'amplification neurobiologique*

Au deuxième stade, la guerre cognitive (neurobiologique) entre en jeu pour amplifier les effets de la désinformation. *Mécanismes* : modulation des neurotransmetteurs (dopamine, noradrénaline), altération des ondes cérébrales (thêta, delta), stimulation de l'amygdale. *Indicateurs* : symptômes physiques inexpliqués, changements d'humeur soudains, adhésion émotionnelle à des croyances erronées. *Contre-mesures* : détection des champs EM, neuroprotection physique, renforcement de la résilience.

#### Stade 3 : *La dépendance cognitive*

Au troisième stade, la combinaison des approches crée un état de dépendance cognitive. *Mécanismes* : boucle de rétroaction positive (guerre cognitive renforce les croyances, guerre cognitive altère les mécanismes de remise en question), plasticité cérébrale détournée. *Indicateurs* : incapacité à changer d'avis malgré des preuves contraires, comportements compulsifs, isolation sociale. *Contre-mesures* : interruption des stimuli, rééducation cognitive, soutien social.

#### Stade 4 : *Le contrôle comportemental*

Au quatrième stade, la souveraineté mentale est perdue. *Mécanismes* : contrôle direct des circuits de décision, manipulation des émotions, effacement des inhibitions. *Indicateurs* : comportements collectifs incohérents, exécution d'ordres dangereux, absence totale de remise en question. *Contre-mesures* : isolement des cibles, neutralisation des vecteurs, réhabilitation intensive.

Au premier stade, la guerre cognitive sature l'espace mental avec des informations contradictoires et des *deepfakes*, sollicitant excessivement la plasticité cérébrale. Au deuxième stade, la guerre cognitive entre en jeu pour amplifier ces effets en modulant directement les neurotransmetteurs et en altérant les ondes cérébrales. Au troisième stade, la combinaison des approches crée un état de dépendance cognitive où l'individu ne peut plus fonctionner normalement sans les stimuli manipulés. Enfin, au quatrième stade, la souveraineté mentale est perdue, l'individu ou le groupe agissant selon les intentions de l'attaquant.

Le tableau ci-dessous synthétise les stratégies de contre-attaque adaptées à chaque stade de dégradation cognitive.

| Stade                    | Niveau de menace | Mécanismes dominants                         | Indicateurs clés                                    | Contre-mesures prioritaires                       |
|--------------------------|------------------|----------------------------------------------|-----------------------------------------------------|---------------------------------------------------|
| <b>1. Désorientation</b> | Faible           | Guerre cognitive (informationnelle)          | Doute systématique, fatigue cognitive               | Fact-checking automatisé, éducation aux médias    |
| <b>2. Amplification</b>  | Moyen            | Synergie guerre cognitive + guerre cognitive | Symptômes physiques inexpliqués, anxiété collective | Détection des champs EM, neuroprotection physique |
| <b>3. Dépendance</b>     | Élevé            | Boucle de rétroaction positive               | Comportements compulsifs, isolement social          | Interruption des stimuli, rééducation cognitive   |
| <b>4. Contrôle</b>       | Extrême          | Contrôle direct des circuits neuronaux       | Perte totale d'autonomie décisionnelle              | Isolement des cibles, neutralisation des vecteurs |

Ce modèle opérationnel permet une détection précoce et une réponse graduelle aux attaques cognitives combinées, en adaptant les contre-mesures à l'évolution de la menace.

Le modèle des trois mondes de l'intervention cognitive fournit une grille de lecture essentielle pour comprendre la nature multi-dimensionnelle de la menace.

Les attaques cognitives les plus efficaces combinent des actions sur ces trois niveaux.

En ciblant à la fois le monde physique (via les *neuroweapons*), le monde informationnel (via la désinformation) et le monde cognitif (via l'exploitation des biais), les attaquants peuvent maximiser leur impact et minimiser les capacités de résistance de leurs cibles.

A - *Le monde physique* : la matérialité des attaques neurobiologiques

*Vecteurs* : ondes électromagnétiques (1–10 GHz), ultrasons, nanoneurotechnologies, substances neuroactives (BZ). *Implications* : détectabilité (traces physiques), attribuabilité possible, contre-mesures : blindage, détection, neutralisation.

B - *Le monde informationnel* : l'immatérialité des attaques cognitives

*Vecteurs* : *Deepfakes* (IA générative), réseaux de bots, algorithmes de recommandation, métavers. *Implications* : diffusion virale, déniabilité, effets durables.

C - *Le monde cognitif* : la convergence des deux approches

*Mécanismes* : effet de résonance (la guerre cognitive crée un état de réceptivité, que la guerre cognitive verrouille en altérant les mécanismes neurobiologiques) ; boucle de rétroaction (chaque approche amplifie l'efficacité de l'autre) ; multiplicateur de puissance (amplification par 3 à 5 des effets).

Dans le monde physique, la guerre cognitive déploie ses vecteurs matériels pour agir directement sur le substrat biologique de la pensée.

Dans le monde informationnel, la guerre cognitive agit sur les flux d'information et les systèmes de pensée.

Dans le monde cognitif, les deux approches convergent pour cibler la pensée, la mémoire, l'émotion et la prise de décision.

L'effet de résonance cognitive est particulièrement redoutable : la guerre cognitive prépare le terrain en créant un état de réceptivité, que la guerre cognitive verrouille en altérant les mécanismes neurobiologiques de remise en question. Cette synergie crée une boucle de rétroaction positive où chaque approche amplifie l'efficacité de l'autre, avec un multiplicateur de puissance de 3 à 5 selon les simulations de l'OTAN-STO. (voir le chapitre IV)

### III-1.2.3 Implications stratégiques du modèle des 4 stades

La guerre cognitive est un processus progressif, et non une attaque ponctuelle. Contrairement à une cyberattaque ou à une explosion, qui ont un impact immédiat et visible, les attaques cognitives agissent par étapes, dégradant progressivement les capacités mentales.

Nous pouvons en tirer trois enseignements majeurs :

A - *La guerre cognitive est progressive* :

Stade 1 → Stade 2 : Le stimulus passe de la perception à l'intégration cognitive (mémoire à court terme, émotions).

Stade 2 → Stade 3 : La croyance ou le comportement devient permanent (mémoire à long terme, ancrage des biais).

Stade 3 → Stade 4 : Les dégâts neuronaux deviennent irréversibles (atrophie cérébrale, troubles psychiatriques).

B - *Les contre-mesures doivent être adaptées au stade* : chaque stade nécessite une réponse spécifique :

Stade 1 (Exposition) → Filtres automatiques (détection des *deepfakes*, blocage des bots).

Stade 2 (Pénétration) → Éducation critique (formation à la pensée critique, diversité des sources).

Stade 3 (Ancrage) → Preuves irréfutables (blockchain, archives) + thérapies cognitives.

Stade 4 (Dégénérescence) → Neuroprotection (blindage EM, rééducation cognitive).

Une approche « *one-size-fits-all* » ne fonctionne pas : il faut adapter les défenses en fonction de la gravité de l'attaque.

*C - La prévention est la meilleure défense* : une fois au Stade 4, les dégâts peuvent être irréversibles.

Il est donc essentiel d'agir en amont au moyen de l'éducation (pour renforcer la résistance aux Stades 1 et 2), de la détection précoce (pour bloquer les attaques avant qu'elles n'atteignent le Stade 3), et des technologies défensives (pour protéger le cerveau contre les *neuroweapons* et autres attaques avancées).

Le modèle des 4 stades de la dégradation cognitive est un outil puissant pour comprendre la dynamique des attaques cognitives. En identifiant le stade atteint par une cible (individu ou population), on peut mettre en place les contre-mesures les plus efficaces — et éviter que la dégradation ne devienne permanente.

## III-2. Les technologies offensives : l'arsenal de la manipulation

Comme nous l'avons vu précédemment, les technologies de guerre cognitive et cognitive se divisent en deux grandes catégories : les technologies numériques (IA générative, *deepfakes*, réseaux de bots) et les neurotechnologies (*neuroweapons*, BCI, nanoneurotechnologies). Chacune cible des vulnérabilités spécifiques du cerveau et des systèmes de pensée.

### III-2.1. Les technologies numériques : manipuler les perceptions

Les technologies numériques exploitent les failles des systèmes de pensée pour manipuler les perceptions, les croyances et les comportements. Elles agissent indirectement sur le cerveau, via les sens (vue, ouïe) et les processus cognitifs (mémoire, attention, raisonnement).

#### III-2.1.1. Les *deepfakes* : l'illusion parfaite

##### Quand la réalité devient un produit de consommation

En 2017, créer un *deepfake* coûtait 100 000 dollars et nécessitait des compétences en IA avancée. En 2026, un *deepfake* indétectable à l'œil nu peut être produit en quelques secondes pour moins de 10 euros. Cette révolution technologique a transformé les *deepfakes* en arme de désinformation massive, accessible à tous : États, groupes criminels, voire individus isolés.

Les *deepfakes* sont redoutables parce qu'ils exploitent une faille humaine fondamentale : notre confiance dans ce que nous voyons et entendons. Une vidéo ou un enregistrement audio semble objectif et crédible — mais un *deepfake* peut tromper même les experts.

##### III-2.1.1.1. Évolution technologique : des GANs aux *Diffusion Models*

Chronologie de l'évolution des *deepfakes*

| Année     | Technologie dominante                           | Modèle phare                        | Qualité                                                 | Coût        | Temps de production | Applications principales                                         | Limites                                                               | Contre-mesures                                      |
|-----------|-------------------------------------------------|-------------------------------------|---------------------------------------------------------|-------------|---------------------|------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------|
| 2017      | GANs ( <i>Generative Adversarial Networks</i> ) | CycleGAN, <i>DeepFakes</i> (Reddit) | Faible (artefacts visibles : yeux, dents, mains)        | ~100 000 \$ | Heures à jours      | Échange de visages sur vidéos statiques                          | Nécessite des données d'entraînement massives                         | Analyse des artefacts visuels (ELA)                 |
| 2018–2019 | GANs améliorés                                  | StyleGAN, StyleGAN2                 | Moyenne (visages crédibles, mais artefacts persistants) | ~10 000 \$  | Minutes à heures    | Génération de visages réalistes, <i>deepfakes</i> vidéo basiques | Difficulté avec les mouvements complexes (ex. : clignements des yeux) | Analyse des artefacts temporels (Optical Flow)      |
| 2020–2021 | Hybrides (GANs + Transformers)                  | DFDC (DeepFaceLab), SimSwap         | Élevée (vidéos courtes, 5–10 secondes)                  | ~1 000 \$   | Secondes à minutes  | <i>Deepfakes</i> vidéo avec mouvements réalistes                 | Artefacts dans les mains, les oreilles                                | Détection par modèles de <i>deep learning</i> (CNN) |

| Année     | Technologie dominante  | Modèle phare                        | Qualité                                                  | Coût    | Temps de production | Applications principales                                                    | Limites                                              | Contre-mesures                                          |
|-----------|------------------------|-------------------------------------|----------------------------------------------------------|---------|---------------------|-----------------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------------|
| 2022–2023 | Diffusion Models       | Stable Diffusion, DALL·E 2          | Très élevée (images fixes hyperréalistes)                | ~100 \$ | Secondes            | Génération d'images à partir de texte, <i>deepfakes</i> statiques           | Cohérence temporelle limitée (vidéos)                | Détection par analyse spectrale (Fourier)               |
| 2024–2025 | Diffusion Models Vidéo | Sora (OpenAI), Pika Labs, Runway ML | Excellente (vidéos de 60 secondes, cohérence temporelle) | ~50 \$  | Secondes            | Génération de vidéos réalistes à partir de texte                            | Coût énergétique élevé (nécessite des GPU puissants) | Détection par analyse temporelle (DeepRhythm)           |
| 2026      | Modèles multimodaux    | Sora 2.0 (OpenAI), Google Veo       | Indétectable (à l'œil nu)                                | < 10 €  | Quelques secondes   | Vidéos longues (plusieurs minutes), synchronisation audio/visuelle parfaite | Contournement des détecteurs actuels                 | Combinaison de détection visuelle + audio + métadonnées |

Cette évolution suit une loi exponentielle similaire à la loi de Moore : la qualité des *deepfakes* double tous les 12 à 18 mois ; le coût et le temps de production s'effondrent (division par 10 000 depuis 2017) ; les applications deviennent de plus en plus larges (images → vidéos → multimodal).

On observe trois tendances majeures :

- *l'exponentielle technologique* (en 2026, un *deepfake* peut être indétectable à l'œil nu ; les modèles comme Sora 2.0 (OpenAI) ou Google Veo peuvent générer des vidéos de plusieurs minutes avec une synchronisation audio/visuelle parfaite) ;
- *la démocratisation* (en 2017, les *deepfakes* étaient réservés aux laboratoires et aux États ; en 2026, ils sont accessibles à tous, y compris aux individus isolés. Cette démocratisation a transformé la guerre cognitive en une menace de masse) ;
- *l'automatisation* (la production de *deepfakes* est désormais automatisée et industrielle ; des outils comme Sora ou *Stable Diffusion*) permettent de générer des contenus en temps réel, sans compétences techniques avancées.

### III-2.1.1.2 GANs vs. *Diffusion Models* : Deux approches, deux forces

#### Comparaison technique détaillée

##### A. Les GANs (*Generative Adversarial Networks*) : La compétition créative

Les GANs reposent sur un principe de compétition entre deux réseaux de neurones : le générateur (qui crée des contenus synthétiques (images, vidéos) à partir de bruit aléatoire) et le discriminateur (qui tente de distinguer les contenus réels des contenus générés). *Fonctionnement* : initialisation (le générateur produit des images aléatoires, le discriminateur les classe comme fausses) ; entraînement (le générateur s'améliore pour tromper le discriminateur, tandis que ce dernier s'améliore pour détecter les fautes du générateur) ; équilibre (à la fin, le générateur produit des images indistinguables des vraies pour le discriminateur). *Avantages* : rapidité (génération en temps réel (idéal pour les applications interactives)) ; contrôle (permet de cibler des attributs spécifiques (ex. : changer un visage tout en conservant le reste de l'image)). *Limites* : instabilité (difficile à entraîner (problème de *mode collapse*, où le générateur produit des images peu variées)) ; artefacts (problèmes avec les détails fins (yeux, dents, mains)) ; données (nécessite un grand jeu de données d'entraînement (ex. : 10 000 images d'un visage)). *Exemple* : *DeepFaceLab* (2019) est l'un des outils open-source les plus populaires pour créer des *deepfakes* vidéo. Il utilise des GANs améliorés pour générer des vidéos avec des mouvements de tête réalistes.

##### B. Les *Diffusion Models* : Le débruitage créatif

Contrairement aux GANs, les *Diffusion Models* ne reposent pas sur une compétition, mais sur un processus de débruitage progressif : ajout de bruit (une image réelle est progressivement bruitée sur 1 000 étapes) ; apprentissage (le modèle apprend à inverser ce processus (débruiter)) ; génération (à partir

de bruit pur, le modèle recrée une image réaliste). *Avantages* : stabilité (moins sujet aux artefacts que les GANs (meilleure cohérence globale)) ; qualité (meilleure fidélité aux détails (mains, accessoires, éclairage)) ; flexibilité (peut générer des images à partir de texte). *Limites* : lenteur (génération plus lente que les GANs (mais s’améliore rapidement)) ; coût énergétique (nécessite des GPU très puissants). *Exemple* : Sora (OpenAI, 2024) est le premier modèle grand public capable de générer des vidéos de 60 secondes à partir d’un prompt textuel. Il utilise une variante avancée des *Diffusion Models*, optimisée pour la cohérence temporelle.

Comparaison technique GANs vs. Diffusion Models

| Critère                     | GANs                               | Diffusion Models                   | Vainqueur        | Applications idéales            |
|-----------------------------|------------------------------------|------------------------------------|------------------|---------------------------------|
| Qualité des images          | Bonne (artefacts fréquents)        | Excellente (peu d’artefacts)       | Diffusion Models | Génération d’images fixes       |
| Qualité des vidéos          | Moyenne (mouvements saccadés)      | Excellente (mouvements fluides)    | Diffusion Models | Génération de vidéos            |
| Vitesse de génération       | Très rapide (temps réel)           | Rapide (quelques secondes)         | GANs             | Applications temps réel         |
| Stabilité de l’entraînement | Instable ( <i>mode collapse</i> )  | Stable                             | Diffusion Models | Génération de contenus variés   |
| Flexibilité                 | Limitée (besoin de données cibles) | Élevée (texte → image/vidéo)       | Diffusion Models | Génération à partir de texte    |
| Coût énergétique            | Faible                             | Élevé                              | GANs             | Applications mobiles            |
| Besoins en données          | Élevés (10 000+ images)            | Moyens (peuvent utiliser du texte) | Diffusion Models | Génération de contenus nouveaux |

Les *Diffusion Models* dominent pour la qualité et la flexibilité (ex. : Sora pour la vidéo). Les GANs restent utiles pour des applications temps réel (ex. : *deepfakes* en direct).

À l’avenir, les deux technologies se combineront (ex. : GANs pour la vitesse + *Diffusion Models* pour la qualité).

III-2.1.1.3 Les limites des *deepfakes* en 2026 : des failles exploitables

Bien que les *deepfakes* soient de plus en plus réalistes, ils présentent encore des limites exploitables pour la détection. Ces limites sont importantes parce qu’elles offrent des opportunités de contre-mesures, même si celles-ci diminuent rapidement avec les avancées technologiques.

Limites des *deepfakes* et méthodes de détection associées

| Type de limite      | Description                                                               | Exemples concrets                                                                          | Technologies de détection associées                                                                                            | Efficacité                                | Contournement possible                                   |
|---------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------|
| Artefacts visuels   | Incohérences dans les détails fins (yeux, mains, accessoires, éclairage). | Yeux qui ne clignent pas, mains déformées, ombres incohérentes, reflets anormaux.          | Analyse des pixels ( <i>Error Level Analysis</i> ), réseaux de neurones convolutifs (CNN), analyse de la cohérence des ombres. | 85–95% (pour les <i>deepfakes</i> connus) | <i>Deepfakes</i> de nouvelle génération (ex. : Sora 2.0) |
| Artefacts temporels | Incohérences dans les mouvements (vidéos).                                | Visage qui se déforme légèrement, synchronisation labiale imparfaite, mouvements saccadés. | Analyse de la cohérence temporelle ( <i>Optical Flow</i> ), modèles 3D, analyse des mouvements faciaux.                        | 80–90%                                    | <i>Diffusion Models</i> avancés (ex. : Sora)             |
| Métadonnées         | Traces numériques laissées par les algorithmes de génération.             | Signature du modèle, artefacts de compression, horodatage suspect.                         | Analyse des métadonnées (EXIF, hash perceptuel), détection des artefacts de compression.                                       | 90–95% (si les métadonnées sont intactes) | Suppression des métadonnées ( <i>stripping</i> des EXIF) |

| Type de limite             | Description                                                                  | Exemples concrets                                                                                | Technologies de détection associées                                                                  | Efficacité | Contournement possible                                    |
|----------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------|
| <b>Bruit statistique</b>   | Patterns non naturels dans la distribution des pixels.                       | Bruit de fond anormal, textures répétitives, artefacts de débruitage.                            | Analyse spectrale (Transformation de Fourier), statistiques de pixels, analyse des textures.         | 75–85%     | Amélioration des modèles génératifs                       |
| <b>Limites physiques</b>   | Contraintes du monde réel non respectées (physique des fluides, réflexions). | Larmes qui ne coulent pas naturellement, réflexions de lumière impossibles, ombres incohérentes. | Modèles physiques ( <i>Physics-Based Detection</i> ), analyse 3D.                                    | 70–80%     | Modèles <i>physique-aware</i> (ex. : NeRF pour la 3D)     |
| <b>Limites sémantiques</b> | Incohérences logiques dans le contenu.                                       | <i>Deepfake</i> d'un leader en réunion et en voyage simultanément, incohérences historiques.     | Analyse contextuelle ( <i>fact-checking</i> , bases de données géolocalisées), vérification croisée. | 80–90%     | <i>Deepfakes</i> très ciblés (peu de données disponibles) |

### III-2.1.1.4 La course sans fin entre génération et détection

Nous pouvons posés trois constats clés :

A - Les artefacts visuels disparaîtront avec l’amélioration des modèles (ex. : Sora 3.0 en 2027) ; les métadonnées peuvent être supprimées (ex. : *stripping* des EXIF) ; les limites physiques seront contournées par des modèles *physique-aware* (ex. : NeRF pour la 3D).

B - Les *deepfakes* inédits (nouveaux modèles) peuvent tromper tous les détecteurs pendant quelques jours, voire semaines ; aussi les détecteurs doivent être mis à jour en continu pour suivre l’évolution des modèles génératifs.

C - La combinaison des méthodes est la clé :

Aucune méthode de détection n’est parfaite : analyse visuelle (efficace contre les artefacts, mais inefficace contre les *deepfakes* de haute qualité) ; analyse des métadonnées (précise si les métadonnées sont intactes, mais facile à contourner) ; blockchain (infalsifiable, mais pas rétroactive (ne fonctionne que pour les contenus nouveaux)).

### III-2.1.2 L’IA générative : l’arme ultime de la manipulation cognitive

#### Quand l’IA devient un outil de guerre

L’intelligence artificielle générative a révolutionné la guerre cognitive en offrant des capacités de manipulation sans précédent : création de contenus personnalisés à grande échelle ; adaptation des attaques en temps réel ; ciblage d’individus spécifiques avec une précision chirurgicale<sup>6</sup>.

Contrairement aux outils traditionnels (ex. : propagande papier), l’IA générative automatise ce qui était autrefois manuel : la création de réalités alternatives, à une échelle et avec une précision inégalées.

#### III-2.1.2.1 Les modèles clés de l’IA générative

Modèles clés de l’IA générative et leurs applications offensives

| Type de modèle                     | Exemples                                             | Fonctionnement                                                                                                                                      | Applications offensives                                                                                                                          | Limites                                                                                                                      | Contre-mesures                                                                                                                    | Impact stratégique                                                                                        |
|------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>LLM (Large Language Models)</b> | GPT-4 (OpenAI), Llama 3 (Meta), Mistral (Mistral AI) | Modèles de langage prédictifs, entraînés sur des milliards de mots. Utilisent des <i>transformers</i> pour générer du texte cohérent et contextuel. | Désinformation textuelle ( <i>fake news</i> , <i>deepfakes</i> textuels), chatbots manipulateurs (simulation d’experts, influence des opinions), | Hallucinations (inventions de faits), biais intégrés (reproduction des biais des données d’entraînement), détection possible | Détection automatique (outils comme Originality.ai, Grover), vérification factuelle ( <i>fact-checking</i> ), éducation critique. | Manipulation à grande échelle, saturation de l’espace informationnel, perte de confiance dans les médias. |

<sup>6</sup> Voir en particulier à cet égard : Patrice Cardot - [L’intelligence artificielle face aux guerres secrètes : Enjeux éthiques, limites méthodologiques et risques géopolitiques \(2010-2026\)](#) – academia.edu

| Type de modèle                      | Exemples                                              | Fonctionnement                                                                                                                                                     | Applications offensives                                                                                                                                  | Limites                                                                                           | Contre-mesures                                                                                     | Impact stratégique                                                                              |
|-------------------------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|                                     |                                                       |                                                                                                                                                                    | phishing cognitif (arnaques personnalisées).                                                                                                             | via analyse stylistique.                                                                          |                                                                                                    |                                                                                                 |
| <b>VLM (Vision-Language Models)</b> | CLIP (OpenAI), BLIP (Salesforce), Flamingo (DeepMind) | Modèles multimodaux combinant texte et image. Utilisent des Transformers pour comprendre et générer des contenus visuels et textuels.                              | <i>Deepfakes</i> avancés (génération d'images à partir de texte), manipulation visuelle ciblée (création de contenus adaptés à des groupes spécifiques). | Coût énergétique élevé, besoin de données massives, artefacts visuels (pour les modèles actuels). | Détection des artefacts (analyse visuelle, métadonnées), blockchain (authentification des médias). | Manipulation visuelle à une échelle industrielle, perte de confiance dans les images et vidéos. |
| <b>TTS (Text-to-Speech)</b>         | ElevenLabs, Murf.ai, Descript                         | Génération de voix synthétiques hyperréalistes à partir de texte. Utilisent des réseaux de neurones pour cloner des voix avec seulement quelques secondes d'audio. | <i>Deepfakes</i> audio (fausses interviews, discours falsifiés), usurpation vocale (arnaques téléphoniques, ordres falsifiés).                           | Artefacts sonores (respiration, intonations), détection via analyse spectrale.                    | Analyse audio authentification biométrique.                                                        | Manipulation audio à grande échelle, perte de confiance dans les communications vocales.        |
| <b>STT (Speech-to-Text)</b>         | Whisper (OpenAI), Wav2Vec (Meta)                      | Transcription automatique de la parole en texte. Utilisent des réseaux de neurones pour une transcription précise et contextuelle.                                 | Surveillance de masse (analyse des conversations pour identifier des cibles), espionnage (transcription de réunions privées).                            | Erreurs de transcription, besoin de qualité audio élevée.                                         | Brouillage audio, chiffrement des communications.                                                  | Perte de vie privée, risque de chantage ou de manipulation.                                     |

Trois applications offensives majeures de l'IA générative

*Désinformation textuelle* : les LLM permettent de générer des *fake news* crédibles à grande échelle. *Exemple* : Un article de presse entièrement généré par IA, diffusant une fausse information sur un conflit géopolitique. *Risque* : saturation de l'espace informationnel avec des contenus indistinguables des vrais.

*Deepfakes multimodaux* : les VLM permettent de générer des images et vidéos à partir de prompts textuels. *Exemple* : Sora (OpenAI, 2024) peut créer une vidéo d'un événement fictif en quelques secondes. *Risque* : manipulation visuelle à une échelle industrielle.

*Usurpation vocale* : les TTS permettent de cloner une voix avec seulement quelques secondes d'audio. *Exemple* : un faux appel téléphonique du président, ordonnant une action militaire. *Risque* : compromission des chaînes de commandement via des ordres falsifiés.

L'IA générative est l'arme la plus puissante de la guerre cognitive moderne. Sa capacité à générer des contenus crédibles à grande échelle en fait une menace majeure pour la stabilité informationnelle et la sécurité nationale.

### III-2.1.3 Les réseaux de bots : l'amplification automatique de la désinformation

#### Les armées numériques invisibles

Les réseaux de bots sont les soldats anonymes de la guerre cognitive. Invisibles, nombreux et coordonnés, ils permettent d'amplifier, diffuser et légitimer la désinformation à une échelle industrielle. En 2026, on estime que 15 à 20 % des comptes actifs sur Twitter/X sont des bots. Leur impact est décuplé par l'IA générative, qui leur permet de créer des contenus crédibles en temps réel.

Pourquoi sont-ils si redoutables ? Parce qu'ils transforment une simple *fake news* en un phénomène viral, capable de saturer l'espace informationnel et de manipuler l'opinion publique.

#### III-2.1.3.1 Architectures des réseaux de bots

Typologies des réseaux de bots et leurs caractéristiques

| Type de bot                          | Description                                                                          | Fonctionnalités                                                                           | Niveau de sophistication | Impact potentiel                                                   | Exemple concret                                                                       | Détection                                                                          | Contre-mesures                                                     |
|--------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Bots simples</b>                  | Comptes automatisés basiques, répétant des messages préprogrammés.                   | Diffusion de messages identiques, likes/retweets automatiques, suivi de comptes cibles.   | Faible                   | Amplification basique de la désinformation.                        | Bots relayant une <i>fake news</i> en boucle sur Twitter.                             | Facile (analyse des patterns : messages identiques, horaires réguliers).           | Filtres automatiques (blocage des comptes suspects).               |
| <b>Bots socialement intelligents</b> | Bots simulant un comportement humain (réponses contextuelles, interactions).         | Conversations crédibles, adaptation aux tendances, réponses aux mentions.                 | Moyen                    | Légitimation de la désinformation (les bots semblent réels).       | Bots commentant des posts avec des réponses pertinentes et personnalisées.            | Moyenne (analyse comportementale : délais de réponse, cohérence des messages).     | Analyse comportementale (détection des anomalies).                 |
| <b>Bots hybrides</b>                 | Combinaison de bots et de comptes humains (ex. : comptes volés, <i>honey pots</i> ). | Diffusion massive + crédibilité accrue (mélange de comportements humains et automatisés). | Élevé                    | Impact maximal (diffusion + légitimité).                           | Réseau utilisant des comptes piratés pour amplifier une <i>fake news</i> .            | Difficile (détection des anomalies : changement brutal de comportement).           | Détection des anomalies (analyse des changements de comportement). |
| <b>Bots à IA générative</b>          | Bots utilisant des LLM pour générer des contenus uniques et adaptatifs.              | Messages personnalisés, réponses adaptatives, création de <i>fake news</i> en temps réel. | Très élevé               | Désinformation à grande échelle avec peu de répétitions.           | Bots créant des <i>fake news</i> en temps réel via GPT-4.                             | Très difficile (analyse stylistique : détection des contenus générés par IA).      | Analyse stylistique (outils comme Originality.ai, Grover).         |
| <b>Botnets</b>                       | Réseaux de milliers de bots coordonnés par une IA centrale.                          | Attaques coordonnées, adaptation dynamique, ciblage multi-plateformes.                    | Extrême                  | Saturation de l'espace informationnel, manipulation des tendances. | Botnet inondant Twitter, Facebook et TikTok simultanément avec des <i>deepfakes</i> . | Extrêmement difficile (analyse des réseaux : détection des connexions entre bots). | Analyse des réseaux (cartographie des connexions).                 |

Trois évolutions majeures des réseaux de bots :

*De la quantité à la qualité* : 2016 : Bots simples répétant des messages identiques ; 2026 : Bots intelligents générant des contenus uniques et interagissant de manière crédible. *Impact* : La désinformation devient plus difficile à détecter.

*L'intégration de l'IA générative* : les bots modernes utilisent des LLM pour créer des *fake news* en temps réel, adapter leurs messages au contexte et simuler des conversations humaines. *Impact* : la désinformation devient plus crédible et plus personnalisée.

*La coordination à grande échelle* : les botnets permettent des attaques coordonnées sur plusieurs plateformes. *Exemple* : un botnet peut inonder Twitter/X, Facebook et TikTok simultanément avec la même désinformation. *Impact* : saturation de l'espace informationnel, rendant impossible la distinction entre vrai et faux.

### III-2.1.3.2 Stratégies de détection et de contre-mesures

#### Méthodes de détection des réseaux de bots

| Méthode                     | Principe                                                                                | Avantages                                                | Limites                                             | Exemples d'outils                          | Efficacité |
|-----------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------|--------------------------------------------|------------|
| <b>Analyse des patterns</b> | Détection des comportements répétitifs (ex. : messages identiques, horaires réguliers). | Simple à implémenter, efficace contre les bots basiques. | Inefficace contre les bots avancés (IA générative). | Botometer (Indiana University), BotSlayer. | 70–80%     |

| Méthode                        | Principe                                                                                        | Avantages                                          | Limites                                        | Exemples d'outils                 | Efficacité |
|--------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------|------------------------------------------------|-----------------------------------|------------|
| <b>Analyse comportementale</b> | Identification des anomalies (ex. : délais de réponse trop courts, cohérence des messages).     | Efficace contre les bots socialement intelligents. | Nécessite des données massives, faux positifs. | BotSentinel, FakeSpot.            | 80–85%     |
| <b>Analyse des réseaux</b>     | Cartographie des connexions entre bots (ex. : comptes créés depuis la même IP).                 | Détection des botnets, identification des sources. | Complexe, nécessite une infrastructure dédiée. | Graphika, First Draft News.       | 85–90%     |
| <b>Analyse stylistique</b>     | Détection des contenus générés par IA (ex. : utilisation de mots ou de structures spécifiques). | Efficace contre les bots à IA générative.          | Contournable par de nouveaux modèles.          | Originality.ai, Grover (AllenAI). | 80–85%     |

Les réseaux de bots sont l'arme d'amplification de la guerre cognitive. Leur évolution (IA générative, coordination) en fait une menace toujours plus difficile à contrer. Les stratégies de détection doivent donc être multidimensionnelles et adaptatives.

### III-2.2 Les neurotechnologies : l'attaque directe sur le cerveau

Les neurotechnologies représentent la frontière ultime de la guerre cognitive. Contrairement aux technologies numériques, qui agissent indirectement sur le cerveau via les sens, les neurotechnologies ciblent directement les processus neurobiologiques, offrant un contrôle sans précédent sur les états mentaux. Elles sont-elles redoutables parce qu'elles contournent les défenses traditionnelles (éducation, esprit critique) en agissant directement sur le cerveau.

#### III-2.2.1 Les *neuroweapons* : l'arme invisible

##### Quand la physique rencontre la neuroscience

Comme nous l'avons vu, les *neuroweapons* sont des armes conçues pour cibler directement le cerveau humain, en utilisant des technologies physiques (ondes électromagnétiques, ultrasons) ou chimiques (neurotoxines). Leur objectif : altérer les états mentaux, contrôler les émotions, ou dégrader les capacités cognitives.

##### III-2.2.1.1 Typologies des *neuroweapons*

Classification des *neuroweapons* par technologie

| Type                                 | Technologie                                              | Mécanisme d'action                                                                                                                  | Effets sur le cerveau                                                                                            | Portée                                 | Précision                      | Exemple concret                                                           | Contre-mesures                                                            | Limites                                                       |
|--------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Ondes électromagnétiques (EM)</b> | Micro-ondes (1–300 GHz), radiofréquences (300 MHz–3 GHz) | Stimulation des neurones via des champs EM → modulation des canaux ioniques (Na <sup>+</sup> , K <sup>+</sup> , Ca <sup>2+</sup> ). | Douleur, hallucinations (auditives/visuelles), altération de la mémoire, contrôle des émotions (peur, euphorie). | 1–5 km (selon la puissance)            | Faible (zones larges)          | <i>Moscow Signal</i> (1972–1989), Projet <i>Pandora</i> (CIA, 1965–1970). | Blindage EM (casques Faraday, cages de Faraday), détection des champs EM. | Atténuation par l'atmosphère, risque de dommages collatéraux. |
| <b>Ultrasons</b>                     | Ondes sonores à haute fréquence (20 kHz–1 GHz)           | Stimulation mécanique des tissus cérébraux → modulation de l'activité neuronale.                                                    | Maux de tête, nausées, désorientation, hallucinations, paralysie temporaire.                                     | 1–10 m (portée limitée)                | Élevée (ciblage millimétrique) | Projet <i>Neural Disruptor</i> (DARPA, 2015–2020).                        | Protection auditive, brouillage ultrasonique.                             | Atténuation par l'air, portée courte.                         |
| <b>Neurotoxines</b>                  | Produits chimiques (BZ, sarin, VX, acide kaïnique)       | Altération de la chimie cérébrale → blocage ou surstimulation des neurotransmetteurs.                                               | Hallucinations, paralysie, perte de conscience, amnésie, troubles psychiatriques.                                | Dépend du vecteur (aérosol, injection) | Moyenne (dépend de la dose)    | Gaz BZ (armée américaine, années 1960–1970), Projet <i>MKUltra</i> .      | Masques à gaz, antidotes (atropine, pralidoxime).                         | Diffusion difficile, risque de contamination.                 |

| Type                  | Technologie                                                              | Mécanisme d'action                                                                                                | Effets sur le cerveau                                                                                  | Portée                                    | Précision                                | Exemple concret                                                                    | Contre-mesures                                  | Limites                                                |
|-----------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------|--------------------------------------------------------|
|                       |                                                                          |                                                                                                                   |                                                                                                        |                                           |                                          | (CIA, 1953–1973).                                                                  |                                                 |                                                        |
| Neurostimulateurs     | Stimulation électrique (TMS), magnétique (rTMS), optique (optogénétique) | Modulation de l'activité neuronale → excitation ou inhibition des zones cérébrales.                               | Contrôle des émotions, altération de la mémoire, induction de faux souvenirs, paralysie décisionnelle. | Contact proche (quelques cm)              | Élevée (ciblage précis)                  | TMS (stimulation magnétique transcrânienne), DBS (stimulation cérébrale profonde). | Blindage, détection des champs magnétiques      | Nécessite un contact physique, effets temporaires.     |
| Nanoneurotechnologies | Nanorobots, nanoparticules                                               | Interaction à l'échelle moléculaire avec les neurones → modulation des neurotransmetteurs ou des canaux ioniques. | Espionnage neuronal, manipulation des émotions/mémoire, sabotage des capacités cognitives.             | Dépend du vecteur (injection, inhalation) | Extrêmement élevée (ciblage moléculaire) | Projet <i>NANO</i> (DARPA, 2020).                                                  | Filtrage sanguin, détection des nanoparticules. | Difficulté de déploiement, risque de rejet immunitaire |

Le projet *Pandora* (voir l'annexe A) a montré que les ondes EM pouvaient avoir des effets psychologiques et neurobiologiques, mais leur déploiement opérationnel reste limité par des contraintes techniques.

### III-2.2.1.2 Mécanismes d'action des ondes électromagnétiques

L'annexe A développe de manière plus approfondie la plupart de ces mécanismes.

Nous nous limiterons ici à n'en donner que des éléments suffisamment significatifs pour les illustrer.

#### Gammes de fréquences EM et leurs effets sur le cerveau

| Gamme de fréquences | Type d'ondes                        | Profondeur de pénétration | Zones cérébrales accessibles  | Mécanisme d'action                                                                              | Effets observés                                                                    | Applications potentielles                                                                     | Contre-mesures                          |
|---------------------|-------------------------------------|---------------------------|-------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------|
| 0,1–100 Hz (ELF)    | Ondes extrêmement basses fréquences | Plusieurs mètres          | Tout le cerveau               | Modulation des champs électriques naturels du cerveau (ondes delta, thêta).                     | Synchronisation des ondes cérébrales, altération de l'humeur, troubles du sommeil. | Manipulation émotionnelle à grande échelle (ex. : induction de fatigue ou de désorientation). | Blindage EM, détection des champs ELF.  |
| 300 MHz–1 GHz       | Radiofréquences (RF)                | 1–3 cm                    | Cortex cérébral (superficiel) | Effet thermique (échauffement localisé) + effet non-thermique (modulation des canaux ioniques). | Douleur, maux de tête, altération de la mémoire à court terme.                     | Désorientation de troupes (ex. : neutralisation temporaire de soldats).                       | Blindage EM, casques Faraday.           |
| 1–3 GHz             | Micro-ondes                         | 0,5–2 cm                  | Cortex cérébral (superficiel) | Effet Frey (audition directe via expansion thermoacoustique).                                   | Hallucinations auditives, désorientation, altération de la mémoire.                | Communication subliminale, désorientation de cibles.                                          | Blindage EM, détection des micro-ondes. |
| 3–10 GHz            | Micro-ondes                         | < 1 cm                    | Peau, méninges                | Effet thermique (brûlures, douleur).                                                            | Douleur intense, brûlures cutanées.                                                | Armes à énergie dirigée (ex. : Active Denial System, ADS).                                    | Blindage EM, protection thermique.      |
| 10–300 GHz          | Ondes millimétriques                | < 0,1 cm                  | Surface de la peau            | Effet thermique (brûlures superficielles).                                                      | Douleur, brûlures.                                                                 | Armes non létales (ex. : contrôle des foules).                                                | Blindage EM, protection thermique.      |

L'effet Frey est un exemple concret de la manière dont les ondes EM peuvent être utilisées comme armes cognitives. Cependant, son déploiement opérationnel reste limité par des contraintes techniques.

L'annexe B pose une analyse extrêmement précise et documentée sur les ondes électromagnétiques utilisées par les systèmes de télécommunication à distance et les risques pour les utilisateurs.

### III-2.2.2 Les interfaces cerveau-machine (BCI) : le contrôle direct

#### La fusion entre l'humain et la machine

Les interfaces cerveau-machine (BCI) permettent une communication directe entre le cerveau et un dispositif externe. Leur potentiel militaire est énorme quand bien même il n'est pas encore 'officiellement - totalement exploité : lecture des pensées (espionnage) ; capacité d'influence des décisions (manipulation) ; contrôle des fonctions motrices (soldats augmentés). Elles sont redoutables parce qu'elles contournent toutes les défenses traditionnelles (éducation, esprit critique) en agissant directement sur le cerveau.

#### III-2.2.2.1 Typologies des BCI

Classification des BCI par niveau d'invasivité

| Type                          | Description                                                                       | Niveau d'invasivité             | Applications offensives                                                              | Exemple concret                                                    | Limites                                                         | Contre-mesures                                                         |
|-------------------------------|-----------------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------------|
| <b>BCI invasives</b>          | Implants cérébraux (électrodes directement dans le cerveau).                      | Élevé (nécessite une chirurgie) | Lecture/écriture des pensées, contrôle des fonctions motrices, espionnage neuronal.  | <i>Neuralink</i> (Elon Musk), <i>BrainGate</i> (Brown University). | Risque d'infection, nécessite une chirurgie, rejet immunitaire. | Blindage des implants, détection des intrusions, cryptage des données. |
| <b>BCI semi-invasives</b>     | Implants sous-cutanés ou électrodes intracrâniennes (sans pénétrer le cerveau).   | Moyen                           | Détection des états mentaux, neurofeedback, contrôle partiel des fonctions motrices. | Électrodes ECoG (électrocorticographie).                           | Précision limitée, risque d'infection.                          | Brouillage EM, blindage.                                               |
| <b>BCI non invasives</b>      | Casques ou électrodes externes (EEG, IRMf, fNIRS).                                | Faible                          | Détection des états mentaux, neurofeedback, contrôle limité des fonctions motrices.  | Casques EEG (ex. : <i>Emotiv</i> , <i>Muse</i> ).                  | Précision limitée, sensible aux interférences.                  | Brouillage EM, blindage.                                               |
| <b>BCI à retour sensoriel</b> | BCI stimulant le cerveau en retour (ex. : neurofeedback, stimulation électrique). | Variable                        | Manipulation des émotions, contrôle des décisions, induction de faux souvenirs.      | Neurostimulateurs (ex. : TMS, DBS).                                | Effets imprévisibles, risque de dépendance.                     | Détection des stimulations, régulation éthique.                        |

#### Étude de cas – Neuralink et ses implications militaires

Neuralink, fondée par Elon Musk en 2016, développe des BCI invasives pour des applications médicales et potentielles applications militaires. *Technologie* : implants cérébraux (électrodes de 4–6 µm de diamètre) ; communication sans fil avec un dispositif externe ; stimulation électrique pour contrôler les fonctions motrices ou cognitives.

*Applications potentielles* :

A - *Soldats augmentés* (contrôle d'armes ou de drones par la pensée ; amélioration des capacités cognitives (mémoire, prise de décision). *Exemple* : Un soldat pourrait contrôler un drone de combat via une BCI.

B - *Espionnage neuronal* : lecture des pensées d'un ennemi ou d'un décideur. *Exemple* : une BCI pourrait être utilisée pour extraire des informations sensibles lors d'un interrogatoire.

*C - Manipulation comportementale* : influence des décisions via une stimulation ciblée. *Exemple* : une BCI pourrait être utilisée pour contrôler les émotions d'un prisonnier ou d'un espion.

*Limites* : risque d'infection (les implants cérébraux sont vulnérables aux infections) ; rejet immunitaire (le corps peut rejeter les implants étrangers) ; effets secondaires (stimulation excessive → crises épileptiques, troubles psychiatriques).

Si Neuralink représente une avancée majeure dans les BCI, son déploiement militaire pose des questions éthiques et techniques majeures.

### III-2.2.3 Les nanoneurotechnologies : l'attaque invisible

#### La menace à l'échelle moléculaire

Les nanoneurotechnologies utilisent des nanorobots (robots de taille nanométrique, 1–100 nm) pour interagir avec les neurones à l'échelle moléculaire.

Leur potentiel offensif est énorme : Espionnage (lecture des pensées) ; manipulation (contrôle des émotions, mémoire) ; sabotage (dégâts neuronaux ciblés).

Pourquoi sont-elles si redoutables ? Parce qu'elles sont invisibles (les nanorobots sont trop petits pour être détectés par les méthodes traditionnelles), précises (elles peuvent cibler des neurones spécifiques ou des neurotransmetteurs particuliers) et furtives (elles peuvent agir sans laisser de trace).

#### III-2.2.3.1 Mécanismes et applications des nanoneurotechnologies

##### Applications offensives des nanoneurotechnologies

| Mécanisme                      | Description                                                                                                            | Applications offensives                                                                                                                                                      | Exemple concret                                                                                    | Limites                                                                                    | Contre-mesures                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Injection de nanorobots</b> | Injection dans le sang ou les tissus cérébraux via des vecteurs (aérosols, injections).                                | Espionnage neuronal (lecture des pensées, surveillance des états mentaux), manipulation des émotions (contrôle de la peur, de l'euphorie).                                   | Projet <i>NANO</i> (DARPA, 2020) : nanorobots pour la surveillance cérébrale.                      | Difficulté de déploiement (nécessite un vecteur efficace), risque de rejet immunitaire.    | Filtrage sanguin, détection des nanoparticules (nanocapteurs).              |
| <b>Nanocapteurs</b>            | Capteurs nanométriques pour mesurer l'activité neuronale ou les niveaux de neurotransmetteurs.                         | Surveillance à distance (transmission des données cérébrales en temps réel), détection des états mentaux (stress, fatigue).                                                  | Nanocapteurs implantés chez des soldats pour surveiller leur état mental.                          | Portée limitée (nécessite une infrastructure de transmission), risque de détection.        | Brouillage des signaux, blindage EM.                                        |
| <b>Nanostimulateurs</b>        | Stimulation ciblée des neurones via des nanorobots (libération de neurotransmetteurs, modulation des canaux ioniques). | Contrôle des émotions (induction de peur, euphorie), altération de la mémoire (implantation de faux souvenirs), sabotage des capacités cognitives (dégâts neuronaux ciblés). | Projet <i>Neural Dust</i> (UC Berkeley, 2016) : nanocapteurs pour la stimulation cérébrale.        | Précision limitée (difficile de cibler des neurones spécifiques), effets imprévisibles.    | Détection des stimulations, neutralisation (champs magnétiques, antidotes). |
| <b>Nanodrugs</b>               | Libération ciblée de drogues via des nanoparticules (ex. : liposomes, dendrimères).                                    | Manipulation pharmacologique (contrôle des émotions, mémoire), sabotage des capacités cognitives (dégâts neuronaux).                                                         | Nanoparticules libérant du BZ ou de la scopolamine pour induire des hallucinations ou une amnésie. | Difficulté de ciblage (risque d'effets secondaires), détection par le système immunitaire. | Filtrage sanguin, antidotes spécifiques.                                    |

#### Étude de cas – Le projet *Neural Dust* (UC Berkeley, 2016)

En 2016, des chercheurs de l'Université de Californie à Berkeley ont développé le projet *Neural Dust*, une technologie de nanocapteurs capables de mesurer l'activité neuronale à l'échelle micrométrique.

*Technologie* : nanocapteurs (10–100 µm) en graphène ou en matériaux piézoélectriques ; alimentation sans fil via des ondes ultrasonores ; transmission des données via des signaux ultrasonores ou électromagnétiques.

### Applications potentielles :

A - *Surveillance cérébrale* : mesure de l'activité neuronale en temps réel. *Exemple* : surveillance des soldats pour détecter la fatigue ou le stress.

B - *Stimulation cérébrale* : modulation de l'activité neuronale via des ultrasons. *Exemple* : induction de la peur ou de l'euphorie chez une cible.

C - *Espionnage neuronal* : lecture des pensées via l'analyse des signaux neuronaux. *Exemple* : extraction d'informations sensibles lors d'un interrogatoire.

*Limites* : Portée limitée (les nanocapteurs nécessitent une source d'alimentation externe) ; précision limitée (difficile de cibler des neurones spécifiques) ; risque de détection (les signaux ultrasonores peuvent être détectés).

Là encore, si *Neural Dust* représente une avancée majeure dans les nanoneurotechnologies, son déploiement militaire reste limité par des défis techniques.

### III-2.2.4 La manipulation pharmacologique : la chimie au service du contrôle

#### Introduction : Quand les drogues deviennent des armes

La manipulation pharmacologique utilise des substances chimiques pour altérer les états mentaux, contrôler les émotions ou dégrader les capacités cognitives.

Contrairement aux *neuroweapons*, qui agissent via des stimuli externes, les drogues agissent directement sur la chimie du cerveau, offrant un contrôle puissant mais souvent imprévisible.

Cette manipulation pharmacologique est redoutable parce qu'elle contourne toutes les défenses physiques (blindage, détection) en agissant directement sur les neurotransmetteurs.

#### III-2.2.4.1 Substances et mécanismes d'action

##### Drogues et leurs applications en guerre cognitive

| Substance                                       | Mécanisme d'action                                                                                                                              | Effets sur le cerveau                                                                                                                                         | Applications offensives                                           | Exemple concret                                                    | Durée des effets | Contre-mesures                            | Limites                                                  |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------|------------------|-------------------------------------------|----------------------------------------------------------|
| <b>BZ (3-Quinuclidinyl Benzilate)</b>           | Antagoniste des récepteurs muscariniques de l'acétylcholine → perturbation des voies cholinergiques (mémoire, perception).                      | Hallucinations (visuelles/auditives), confusion mentale, désorientation, amnésie antérograde (incapacité à former de nouveaux souvenirs).                     | Désorientation des troupes, contrôle des foules, interrogatoires. | Projet <i>Operation Third Chance</i> (US Army, 1960–1970).         | 24–72 heures     | Masques à gaz, antidotes (physostigmine). | Effets imprévisibles, diffusion difficile.               |
| <b>LSD (Diéthylamide de l'acide lysergique)</b> | Agoniste des récepteurs 5-HT <sub>2A</sub> de la sérotonine → augmentation de la connectivité cérébrale, désorganisation des réseaux neuronaux. | Hallucinations (visuelles/auditives), altération de la perception du temps et de l'espace, dissolution de l'ego, émotions intenses (euphorie, peur, anxiété). | Manipulation sensorielle, interrogatoires, contrôle mental.       | Projet <i>MKUltra</i> (CIA, 1953–1973).                            | 6–12 heures      | Benzodiazépines, environnement calme.     | Effets variables, risque de <i>bad trip</i> .            |
| <b>Scopolamine</b>                              | Antagoniste des récepteurs muscariniques de l'acétylcholine → perturbation de la mémoire et de la perception.                                   | Amnésie antérograde, suggestibilité accrue, désorientation.                                                                                                   | Manipulation des souvenirs, interrogatoires, contrôle mental.     | Utilisation par des criminels en Colombie (« drogue du violeur »). | 2–6 heures       | Surveillance des boissons, éducation.     | Effets temporaires, nécessite une administration proche. |

| Substance             | Mécanisme d'action                                                                                                                 | Effets sur le cerveau                                                                 | Applications offensives                                                     | Exemple concret                                                       | Durée des effets | Contre-mesures                                    | Limites                                                 |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------|------------------|---------------------------------------------------|---------------------------------------------------------|
| <b>MDMA (Ecstasy)</b> | Stimulant de la sérotonine et de la dopamine → augmentation de l'empathie et de l'euphorie.                                        | Empathie artificielle, euphorie, désinhibition, altération de la perception.          | Manipulation émotionnelle, création de liens de confiance, contrôle mental. | Utilisation par des espions pour gagner la confiance de leurs cibles. | 4–6 heures       | Détection des comportements suspects.             | Effets à court terme, risque de dépendance.             |
| <b>Sarin</b>          | Inhibiteur de l'acétylcholinestérase → accumulation d'acétylcholine → surstimulation des récepteurs muscariniques et nicotiniques. | Convulsions, paralysie, perte de conscience, décès (à haute dose).                    | Neutralisation massive, contrôle des foules.                                | Attaque au gaz sarin dans le métro de Tokyo (1995).                   | Minutes à heures | Masques à gaz, antidotes (atropine, pralidoxime). | Diffusion difficile, risque de contamination.           |
| <b>Modafinil</b>      | Inhibiteur de la recapture de la dopamine + augmentation de l'orexine → augmentation de la vigilance et de la concentration.       | Amélioration cognitive (mémoire, prise de décision), réduction de la fatigue mentale. | Amélioration des soldats, manipulation cognitive forcée.                    | Utilisation par l'US Air Force pour les pilotes de drone.             | 6–12 heures      | Régulation de l'usage, éducation aux risques.     | Effets à long terme inconnus, dépendance psychologique. |

Le projet *MKUltra* a montré que les drogues psychotropes pouvaient avoir des effets puissants sur le cerveau, mais leur utilisation comme arme reste limitée par des contraintes techniques et éthiques.

### III-3. Les contre-mesures scientifiques : protéger l'esprit et les systèmes

Face à la montée en puissance des attaques cognitives, les technologies défensives deviennent indispensables. Ces solutions — technologiques, cognitives ou organisationnelles — visent à protéger les individus, les institutions et les sociétés.

#### III-3.1 Détection automatique : la première ligne de défense

##### L'IA contre l'IA

La détection automatique est la première ligne de défense contre les attaques cognitives. Elle repose sur des algorithmes d'IA capables d'identifier les *deepfakes* (images, vidéos, audio), les réseaux de bots et les contenus générés par IA.

Pourquoi est-ce indispensable ? Parce que les attaques cognitives évoluent trop vite pour une détection manuelle. Seule l'automatisation permet de suivre le rythme.

##### III-3.1.1 Technologies de détection des *deepfakes*

Méthodes de détection des *deepfakes* et leur efficacité

| Méthode                              | Principe                                                                       | Avantages                                            | Limites                                                                   | Exemples d'outils                             | Efficacité | Contournement possible                   |
|--------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------|------------|------------------------------------------|
| <b>Analyse des artefacts visuels</b> | Détection des incohérences dans les pixels (yeux, mains, éclairage, ombres).   | Rapide, efficace sur les images statiques.           | Inefficace contre les <i>deepfakes</i> de haute qualité (ex. : Sora 2.0). | Error Level Analysis (ELA), F3Net (Facebook). | 85–95%     | <i>Deepfakes</i> de nouvelle génération. |
| <b>Analyse temporelle</b>            | Détection des mouvements non naturels dans les vidéos (visage, lèvres, corps). | Efficace contre les <i>deepfakes</i> vidéo basiques. | Contournable par les <i>Diffusion Models</i> (ex. : Sora).                | Optical Flow, DeepRhythm (Microsoft).         | 80–90%     | <i>Diffusion Models</i> avancés.         |

| Méthode                  | Principe                                                                                                                   | Avantages                                                            | Limites                                                        | Exemples d'outils                                     | Efficacité | Contournement possible                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------|------------|---------------------------------------------|
| Analyse des métadonnées  | Recherche de traces numériques laissées par les algorithmes de génération (signature du modèle, artefacts de compression). | Précis si les métadonnées sont intactes.                             | Facile à contourner (suppression des métadonnées).             | ExifTool, FotoForensics.                              | 90–95%     | Stripping des EXIF.                         |
| Modèles de deep learning | Utilisation d'IA pour détecter d'autres IA (réseaux de neurones convolutifs, Transformers).                                | Adaptatif, peut évoluer avec les nouvelles menaces.                  | Besoins en données, faux négatifs.                             | Deepware Scanner, Microsoft Video Authenticator.      | 85–90%     | Nouveaux modèles génératifs.                |
| Blockchain               | Registre distribué et infalsifiable pour tracer l'origine et l'historique des contenus.                                    | Infalsifiable, impossible à contourner sans accéder à la blockchain. | Pas rétroactif (ne fonctionne que pour les contenus nouveaux). | Truepic, Adobe CAI (Content Authenticity Initiative). | 95–99%     | Contenus non certifiés.                     |
| Analyse physique         | Détection des incohérences avec les lois de la physique (réflexions, ombres, mouvements).                                  | Robuste contre les deepfakes avancés.                                | Complexe, nécessite des modèles 3D.                            | Physics-Based Detection (PBD).                        | 80–85%     | Modèles <i>physique-aware</i> (ex. : NeRF). |

Nous pouvons poser les trois constats clés suivants :

A - Les artefacts visuels disparaîtront avec l'amélioration des modèles (ex. : Sora 3.0 en 2027) ; les métadonnées peuvent être supprimées (*stripping* des EXIF) ; les limites physiques seront contournées par des modèles *physique-aware* (ex. : NeRF pour la 3D).

B - Les *deepfakes* inédits (nouveaux modèles) peuvent tromper tous les détecteurs pendant quelques jours, voire semaines. Les détecteurs doivent être mis à jour en continu pour suivre l'évolution des modèles génératifs.

C - La combinaison des méthodes est la clé :

Aucune méthode de détection n'est parfaite : analyse visuelle (efficace contre les artefacts, mais inefficace contre les *deepfakes* de haute qualité) ; analyse des métadonnées (précise si les métadonnées sont intactes, mais facile à contourner) ; blockchain (infalsifiable, mais pas rétroactive).

La détection des *deepfakes* est un problème d'IA contre IA. C'est une course aux armements algorithmique, où les attaquants (modèles génératifs) et les défenseurs (modèles de détection) s'améliorent en permanence.

### III-3.1.2 Détection des réseaux de bots

#### Méthodes de détection des réseaux de bots

| Méthode                 | Principe                                                                                  | Avantages                                                | Limites                                             | Exemples d'outils                          | Efficacité |
|-------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------|--------------------------------------------|------------|
| Analyse des patterns    | Détection des comportements répétitifs (messages identiques, horaires réguliers).         | Simple à implémenter, efficace contre les bots basiques. | Inefficace contre les bots avancés (IA générative). | Botometer (Indiana University), BotSlayer. | 70–80%     |
| Analyse comportementale | Identification des anomalies (délais de réponse trop courts, cohérence des messages).     | Efficace contre les bots socialement intelligents.       | Nécessite des données massives, faux positifs.      | BotSentinel, FakeSpot.                     | 80–85%     |
| Analyse des réseaux     | Cartographie des connexions entre bots (comptes créés depuis la même IP).                 | Détection des botnets, identification des sources.       | Complexe, nécessite une infrastructure dédiée.      | Graphika, First Draft News.                | 85–90%     |
| Analyse stylistique     | Détection des contenus générés par IA (utilisation de mots ou de structures spécifiques). | Efficace contre les bots à IA générative.                | Contournable par de nouveaux modèles.               | Originality.ai, Grover (AllenAI).          | 80–85%     |

### III-3.2 Neuroprotection : bouclier contre les *neuroweapons*

#### Protéger le cerveau contre les attaques directes

La neuroprotection vise à protéger le cerveau contre les *neuroweapons* et autres attaques directes. Elle combine technologies physiques (blindage, casques), technologies numériques (détection, brouillage) et protocoles organisationnels (formation, sensibilisation).

Pourquoi est-ce indispensable ? Parce que les *neuroweapons* agissent directement sur le cerveau, contournant toutes les défenses traditionnelles.

#### III-3.2.1 Technologies de neuroprotection

##### Solutions de neuroprotection contre les *neuroweapons*

| Technologie                       | Principe                                                                                          | Applications                                                                       | Avantages                                                         | Limites                                                                                | Exemples                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Casques Faraday                   | Blindage électromagnétique (matériaux conducteurs : cuivre, aluminium) pour bloquer les ondes EM. | Protection contre les <i>neuroweapons</i> à ondes EM (1–300 GHz).                  | Efficace contre les ondes EM, léger (pour les modèles récents).   | Encombrant, limité aux ondes EM (inefficace contre les ultrasons ou les neurotoxines). | Casques militaires (ex. : Faraday Defense), casques grand public.  |
| Blindage des bâtiments            | Protection électromagnétique des infrastructures (cages de Faraday, matériaux absorbants).        | Protection collective contre les <i>neuroweapons</i> à ondes EM.                   | Protection collective, discrète.                                  | Coût élevé, nécessite une installation complexe.                                       | Salles de crise blindées, centres de commandement.                 |
| Détecteurs de <i>neuroweapons</i> | Capteurs pour détecter les attaques neurotechnologiques (ondes EM, ultrasons, neurotoxines).      | Détection précoce des attaques, permettant une réaction rapide.                    | Détection précoce, permet une réponse adaptée.                    | Faux positifs, nécessite une calibration constante.                                    | Capteurs de champs EM, détecteurs d'ultrasons, capteurs chimiques. |
| Neutralisateurs de neurotoxines   | Antidotes ou filtres pour neutraliser les substances chimiques (ex. : atropine pour le sarin).    | Protection contre les attaques chimiques (neurotoxines).                           | Efficace contre les neurotoxines, action rapide.                  | Nécessite une administration rapide, efficace uniquement contre les toxines connues.   | Antidotes (atropine, pralidoxime), masques à gaz.                  |
| Neurostimulateurs défensifs       | Stimulation cérébrale pour renforcer la résilience cognitive (ex. : neurofeedback, TMS).          | Renforcement des capacités cognitives, réduction de la vulnérabilité aux attaques. | Renforcement de la résilience, adaptable aux besoins individuels. | Effets à long terme inconnus, nécessite un suivi médical.                              | Neurofeedback, stimulation magnétique transcrânienne (TMS).        |

La neuroprotection doit être multidimensionnelle pour couvrir toutes les formes d'attaques : protection individuelle (casques Faraday pour les décideurs et soldats ; détecteurs portables pour alerter en cas d'attaque) ; protection collective (blindage des bâtiments pour les centres de commandement ; brouilleurs de signaux pour perturber les attaques) ; protection organisationnelle (protocoles de sécurité pour limiter l'exposition aux *neuroweapons* ; formation et sensibilisation pour reconnaître les symptômes d'une attaque).

La neuroprotection est essentielle pour se défendre contre les *neuroweapons*, mais elle ne couvre pas toutes les menaces. Une approche multicouche est nécessaire.

### III-3.3 Authentification des contenus : prouver la vérité

L'authentification des contenus vise à prouver l'origine et l'intégrité des médias (images, vidéos, documents).

La blockchain est la technologie la plus prometteuse pour cela, car elle offre l'infalsifiabilité (impossible à modifier sans être détecté), la transparence (tout le monde peut vérifier l'historique) et la décentralisation (pas de point de défaillance unique).

Pourquoi est-ce crucial ? Parce que dans un monde de *deepfakes* et de désinformation, prouver la vérité devient aussi important que la détecter.

### III-3.3.1 Technologies d'authentification

#### Méthodes d'authentification des contenus

| Technologie                                                     | Principe                                                               | Avantages                                        | Limites                                         | Exemples                                              | Adoption         |
|-----------------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-------------------------------------------------------|------------------|
| <b>Blockchain</b>                                               | Registre distribué pour tracer l'origine et l'historique des contenus. | Infalsifiable, transparent, décentralisé.        | Pas rétroactif, nécessite une adoption massive. | Truepic, Adobe CAI (Content Authenticity Initiative). | En cours (2026)  |
| <b>Signatures cryptographiques</b>                              | Signature numérique liée à un contenu pour prouver son authenticité.   | Sécurisé, difficile à falsifier.                 | Nécessite une infrastructure de confiance.      | PGP, DSA.                                             | Large            |
| <b>Watermarking</b>                                             | Marquage invisible des contenus avec des informations d'origine.       | Invisible, difficile à supprimer.                | Peut être supprimé par des outils avancés.      | Digimarc, KodakOne.                                   | Moyenne          |
| <b>C2PA (Coalition for Content Provenance and Authenticity)</b> | Standard ouvert pour l'authentification des médias.                    | Standardisé, compatible avec de nombreux outils. | Adoption encore limitée.                        | Adobe, Microsoft, Twitter.                            | En développement |

#### Avantages et limites de l'authentification

*Trois avantages majeurs :*

A - *Confiance accrue* : les contenus authentifiés peuvent être utilisés sans risque par les utilisateurs et les médias. *Exemple* : une photo certifiée par *Truepic* peut être utilisée comme preuve dans un article de presse.

B - *Détection des deepfakes* : les contenus non authentifiés peuvent être marqués comme suspects. *Exemple* : Twitter pourrait afficher un avertissement pour les médias non authentifiés.

C - *Responsabilité* : l'authentification permet de retracer l'origine des contenus malveillants. *Exemple* : identifier le créateur d'un *deepfake* pour des poursuites judiciaires.

*Trois limites majeures :*

A - *Adoption massive nécessaire* : pour être efficace, l'authentification doit être largement adoptée par les plateformes et les utilisateurs.

B - *Pas rétroactif* : ne fonctionne que pour les nouveaux contenus (les contenus existants ne peuvent pas être authentifiés).

C - *Contournement possible* : les attaquants peuvent supprimer les métadonnées ou utiliser des plateformes non compatibles.

L'authentification des contenus est une pièce maîtresse de la défense contre la guerre cognitive. Son efficacité dépend de son adoption massive.

### III-3.4 IA défensive : l'intelligence artificielle au service de la protection

#### Utiliser l'IA pour contrer l'IA

L'IA défensive utilise des algorithmes d'intelligence artificielle pour détecter les attaques cognitives, analyser les menaces et contrer les attaques en temps réel.

Pourquoi est-ce crucial ? Parce que les attaques cognitives évoluent trop vite pour une réponse humaine. Seule l'IA peut suivre le rythme.

#### III-3.4.1 Applications de l'IA défensive

##### Domaines d'application de l'IA défensive

| Application                    | Description                                                             | Avantages                                              | Limites                                            | Exemples d'outils                                | Efficacité |
|--------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------|--------------------------------------------------|------------|
| <b>Détection des deepfakes</b> | Identification des contenus synthétiques (images, vidéos, audio).       | Rapide, adaptative.                                    | Besoins en données, faux négatifs.                 | Deepware Scanner, Microsoft Video Authenticator. | 85–90%     |
| <b>Détection des bots</b>      | Identification des comptes automatisés sur les réseaux sociaux.         | Efficace contre les bots simples.                      | Difficile contre les bots avancés (IA générative). | Botometer (Indiana University), BotSentinel.     | 80–85%     |
| <b>Analyse des réseaux</b>     | Cartographie des réseaux de désinformation et des chaînes de diffusion. | Visualisation des menaces, identification des sources. | Complexe, nécessite des données massives.          | Graphika, First Draft News.                      | 85–90%     |
| <b>Prédiction des attaques</b> | Anticipation des attaques cognitives via l'analyse des tendances.       | Prévention proactive.                                  | Incertitude, faux positifs.                        | Palantir, Recorded Future.                       | 70–80%     |

### Avantages et limites de l'IA défensive

#### Trois avantages majeurs :

A - *Vitesse* : l'IA peut analyser des millions de contenus en quelques secondes, là où un humain mettrait des heures. *Exemple* : *Microsoft Video Authenticator* peut scanner des milliers de vidéos par jour.

B - *Adaptabilité* : Les modèles d'IA peuvent apprendre à détecter de nouvelles menaces sans être reprogrammés. *Exemple* : un modèle de détection peut s'adapter à un nouveau type de *deepfake* en quelques heures.

C - *Précision* : l'IA peut identifier des *patterns* subtils que les humains ne verraient pas. *Exemple* : détection des artefacts visuels dans un *deepfake* de haute qualité.

#### Trois limites majeures :

A - *Besoins en données* : les modèles d'IA nécessitent des données massives pour être efficaces.

B - *Faux positifs/négatifs* : risque de blocage erroné ou de non-détection.

C - *Coût* : les systèmes d'IA défensive sont énergivores et coûteux.

L'IA défensive est indispensable pour contrer les attaques cognitives. Cependant, elle ne doit pas remplacer les autres mesures (éducation, régulation).

## III-5. Comparaison systématique : Quel vecteur pour quel objectif ?

### III-5.1 Matrice de décision : Choisir le bon vecteur

Pour aider à la planification stratégique, voici une matrice comparative des différents vecteurs en fonction des objectifs de la guerre cognitive.

Chaque vecteur est évalué selon 5 critères clés : précision (capacité à cibler une zone ou un individu spécifique) ; durée des effets (combien de temps les effets persistent) ; furtivité (difficulté à détecter l'attaque) ; coût (coût de développement et de déploiement) ; effets secondaires (risques pour la santé ou l'environnement).

| Objectif                                | Vecteur optimal              | Précision   | Durée          | Furtivité | Coût   | Effets secondaires   | Exemple d'application                  |
|-----------------------------------------|------------------------------|-------------|----------------|-----------|--------|----------------------|----------------------------------------|
| <b>Désorientation massive</b>           | Infrasons + ondes ELF        | Moyenne     | 1–6 h          | Élevée    | Faible | Nausées, panique     | Contrôle de foules en zone urbaine     |
| <b>Manipulation émotionnelle ciblée</b> | Drogues (aérosols) + musique | Élevée      | 2–24 h         | Moyenne   | Moyen  | Dépendance, toxicité | Désorientation de décideurs politiques |
| <b>Implantation de faux souvenirs</b>   | Hypnose + ondes thêta        | Très élevée | Heures à jours | Moyenne   | Faible | Psychose, amnésie    | Interrogatoires ou lavage de cerveau   |

| Objectif                               | Vecteur optimal                   | Précision   | Durée            | Furtivité | Coût       | Effets secondaires  | Exemple d'application                           |
|----------------------------------------|-----------------------------------|-------------|------------------|-----------|------------|---------------------|-------------------------------------------------|
| <b>Paralysie décisionnelle</b>         | <i>Neuroweapons</i> (micro-ondes) | Élevée      | Minutes à heures | Faible    | Très élevé | Lésions thermiques  | Neutralisation de commandants ennemis           |
| <b>Amélioration cognitive forcée</b>   | Modafinil + neurostimulation      | Élevée      | 6–12 h           | Faible    | Moyen      | Dépendance, burnout | Soldats en mission prolongée                    |
| <b>Contrôle à distance d'une foule</b> | Ondes ELF + infrasons             | Faible      | 1–12 h           | Élevée    | Moyen      | Panique collective  | Dispersion de manifestations                    |
| <b>Espionnage cérébral</b>             | Nanoneurotechnologies + ondes EM  | Très élevée | Jours            | Faible    | Très élevé | Lésions neuronales  | Surveillance de cibles hautement sensibles      |
| <b>Manipulation sensorielle</b>        | Lasers + ultrasons                | Très élevée | Minutes à heures | Moyenne   | Élevé      | Crises épileptiques | Désorientation de pilotes ou opérateurs         |
| <b>Contrôle moteur</b>                 | Ultrasons (LIFU)                  | Très élevée | Minutes          | Faible    | Élevé      | Lésions cérébrales  | Neutralisation de soldats ennemis               |
| <b>Induction de transe collective</b>  | Musique répétitive + ondes EM     | Moyenne     | 1–4 h            | Élevée    | Faible     | Hallucinations      | Manipulation de groupes religieux ou politiques |

### III-5.2 Synergies entre vecteurs

Les attaques les plus efficaces combinent souvent plusieurs vecteurs pour exploiter leurs effets synergiques.

Voici quelques exemples :

| Combinaison                              | Mécanisme                                                     | Effet synergique                              | Application                          | Risques                      |
|------------------------------------------|---------------------------------------------------------------|-----------------------------------------------|--------------------------------------|------------------------------|
| <b>Ondes EM (1 GHz) + Binaural Beats</b> | Synchronisation des ondes cérébrales + suggestion subliminale | Transe profonde + implantation de suggestions | Hypnose à distance                   | Psychose, dépendance         |
| <b>Infrasons + Drogues (BZ)</b>          | Désorientation physique + confusion mentale                   | Neutralisation complète d'un groupe           | Contrôle de foules hostiles          | Panique, blessures physiques |
| <b>Lasers + Ultrasons</b>                | Stimulation visuelle + stimulation auditive/cérébrale         | Hallucinations multi-sensorielles             | Désorientation de pilotes            | Crises épileptiques          |
| <b><i>Neuroweapons</i> + Méditation</b>  | Perturbation cérébrale + réduction des défenses naturelles    | Vulnérabilité accrue aux attaques cognitives  | Manipulation de moines ou de groupes | Traumatismes psychologiques  |
| <b>Modafinil + <i>Deepfakes</i></b>      | Amélioration cognitive + désinformation visuelle/auditive     | Acceptation accrue de fausses informations    | Propagande ciblée                    | Burnout, dépendance          |

### III-6. Verrous scientifiques et techniques (2026)

Malgré les progrès rapides, les technologies de guerre cognitive font face à des limites fondamentales qui freinent leur déploiement massif.

#### III-6.1. Limites physiques et biologiques

##### III-6.1.1 Pénétration des ondes électromagnétiques

Les ondes EM sont atténuées par les tissus biologiques, limitant leur capacité à atteindre des zones cérébrales profondes.

| Fréquence               | Profondeur de pénétration | Zones cérébrales accessibles | Applications possibles                   |
|-------------------------|---------------------------|------------------------------|------------------------------------------|
| <b>0.1–100 Hz (ELF)</b> | Plusieurs mètres          | Tout le cerveau              | Synchronisation des ondes cérébrales     |
| <b>300 MHz–1 GHz</b>    | 1–3 cm                    | Cortex cérébral              | Désorientation, hallucinations auditives |

| Fréquence  | Profondeur de pénétration | Zones cérébrales accessibles | Applications possibles              |
|------------|---------------------------|------------------------------|-------------------------------------|
| 1–3 GHz    | 0.5–2 cm                  | Cortex (superficiel)         | Effet Frey, désorientation légère   |
| 3–10 GHz   | < 1 cm                    | Peau, méninges               | Brûlures, douleur                   |
| 10–300 GHz | < 0.1 cm                  | Surface de la peau           | Aucune (effet thermique uniquement) |

*Solutions en recherche* : fenêtres de fréquence (utilisation de fréquences entre 0.5–1 GHz pour un compromis pénétration/précision) ; focalisation par lentilles diélectriques (développement de matériaux métamériques pour concentrer les ondes EM sur des zones ciblées (projet DARPA "*Metamaterial Lenses for EM Focusing*")) ; ondes pulsées (utilisation de pulses ultra-courts (nanosecondes) pour réduire l'atténuation et augmenter la pénétration).

### III-6.1.2 Résolution spatiale des *neuroweapons*

Les *neuroweapons* actuels ont une résolution spatiale limitée (de l'ordre de 1 cm), ce qui rend difficile le ciblage de zones cérébrales spécifiques (ex. : l'hippocampe pour la mémoire, l'amygdale pour la peur).

| Technologie                    | Résolution spatiale | Précision de ciblage       | Applications                             |
|--------------------------------|---------------------|----------------------------|------------------------------------------|
| <i>Neuroweapons</i> EM (1 GHz) | ~1 cm               | Faible (zones larges)      | Désorientation générale                  |
| Ultrasons (LIFU)               | ~1 mm               | Élevée (zones spécifiques) | Stimulation ciblée (ex. : cortex moteur) |
| Nanoneurotechnologies          | ~1 µm               | Extrêmement élevée         | Manipulation moléculaire                 |
| TMS (Stimulation Magnétique)   | ~2 cm               | Moyenne                    | Modulation de l'humeur                   |

*Solutions en recherche* : Combinaison EM + IRMf (utilisation de l'imagerie cérébrale en temps réel pour guider les ondes EM vers des zones spécifiques (projet DARPA "*Brain Initiative*")) ; ultrasons focalisés (développement de transducteurs à réseau phasé pour une résolution millimétrique (projet "*Neural Disruptor*")) ; nanoneurotechnologies (utilisation de nanorobots pour un ciblage moléculaire (projet "*NANO*")).

### III-6.1.3 Variabilité individuelle

Les effets des *neuroweapons* varient considérablement selon les individus, en fonction de l'anatomie cérébrale (ex. : épaisseur du crâne, densité des tissus), la neurochimie (niveaux de base de dopamine, sérotonine, etc.) et la génétique (par exemple, les variants du gène *COMT* qui affecte la dégradation de la dopamine).

| Facteur             | Impact sur l'efficacité            | Solutions possibles                                           |
|---------------------|------------------------------------|---------------------------------------------------------------|
| Épaisseur du crâne  | Atténuation des ondes EM           | Augmenter la puissance ou utiliser des fréquences plus basses |
| Niveaux de dopamine | Réceptivité aux stimulants         | Personnalisation des doses ou des fréquences                  |
| Génétique (COMT)    | Métabolisme des neurotransmetteurs | Tests ADN pour adapter les traitements                        |
| Âge                 | Plasticité cérébrale               | Cibler les jeunes (plus sensibles)                            |
| Sexe                | Répartition des récepteurs         | Adapter les fréquences ou les drogues                         |

*Solutions en recherche* : personnalisation (développement de systèmes adaptatifs qui ajustent les paramètres (fréquence, puissance, dose) en fonction des caractéristiques individuelles (projet "*Personalized Neurotechnology*" de la DARPA)) ; biomarqueurs (identification de biomarqueurs (par exemple, niveaux de neurotransmetteurs, activité EEG) pour prédire la réponse d'un individu à une

attaque) ; génétique (utilisation de tests ADN pour adapter les *neuroweapons* (par exemple, cibler les individus avec une variante COMT "lente", plus sensible à la dopamine)).

## III-6.2 Limites technologiques

### III-6.2.1 Détection et contournement

Les systèmes de détection des attaques cognitives sont toujours en retard sur les technologies offensives, créant une course aux armements sans fin.

| Type d'attaque         | Méthode de détection actuelle | Efficacité | Contournement possible                            |
|------------------------|-------------------------------|------------|---------------------------------------------------|
| <i>Deepfakes</i> vidéo | Analyse des artefacts visuels | 85–95%     | Deepfakes de nouvelle génération (ex. : Sora 2.0) |
| Réseaux de bots        | Analyse comportementale       | 80–90%     | Bots avec IA générative (ex. : LLM)               |
| <i>Neuroweapons</i> EM | Détecteurs de micro-ondes     | 70–80%     | Ondes furtives (pulses ultra-courtes)             |
| Drogues (aérosols)     | Détecteurs chimiques          | 90–95%     | Drogues sans signature chimique                   |
| Ultrasons (LIFU)       | Détecteurs acoustiques        | 60–70%     | Ultrasons à haute fréquence                       |

*Solutions en recherche* : détection multi-couches (combinaison de détecteurs EM, chimiques, acoustiques et comportementaux pour une couverture complète) ; IA défensive (utilisation de grands modèles de langage (LLM) pour détecter les deepfakes et la désinformation) ; détection proactive (développement de systèmes capables de prédire les attaques avant qu'elles ne se produisent (ex. : analyse des tendances sur les réseaux sociaux)).

### II-6.2.2 Blindage et contre-mesures

Les contre-mesures (blindage EM, antidotes, etc.) sont souvent encombrantes, coûteuses ou inefficaces contre les attaques les plus sophistiquées.

| Type d'attaque     | Contre-mesure actuelle | Efficacité  | Limites                                     |
|--------------------|------------------------|-------------|---------------------------------------------|
| Ondes EM (1–3 GHz) | Blindage Faraday       | Très élevée | Encombrant, peu respirant                   |
| Infrasons          | Bouches-oreilles       | Moyenne     | Inefficace contre les basses fréquences     |
| Drogues (aérosols) | Masques à gaz          | Élevée      | Encombrant, durée limitée                   |
| Ultrasons (LIFU)   | Blindage acoustique    | Faible      | Peu efficace contre les ultrasons focalisés |
| <i>Deepfakes</i>   | Détecteurs d'IA        | 85–95%      | Contournable par de nouveaux modèles        |

*Solutions en recherche* : matériaux intelligents (développement de nanomatériaux (ex. : graphène) pour un blindage EM léger et respirant) ; antidotes universels (développement de médicaments capables de neutraliser un large spectre de neurotoxines) ; neuroprotection active (utilisation de neurostimulateurs défensifs pour renforcer la résilience cérébrale).

## III-6.3 Limites éthiques et juridiques

### III-6.3.1 Cadre légal flou

Aucun traité international ne couvre explicitement les *neuroweapons* non létaux ni l'IA militaire, créant un vide juridique qui permet à certains pays de développer ces technologies en secret.

| Instrument légal                         | Couverture des <i>neuroweapons</i> | Limites                               |
|------------------------------------------|------------------------------------|---------------------------------------|
| Convention sur les armes chimiques (CWC) | Partielle (neurotoxines)           | Ne couvre pas les ondes EM ou sonores |
| Protocole de Genève                      | Partielle (armes biologiques)      | Ne couvre pas les <i>neuroweapons</i> |

| Instrument légal                      | Couverture des <i>neuroweapons</i> | Limites                         |
|---------------------------------------|------------------------------------|---------------------------------|
| Traité sur la non-prolifération (TNP) | Aucune                             | Conçu pour les armes nucléaires |
| Conventions de La Haye                | Partielle (guerre psychologique)   | Vague et peu contraignant       |

*Solutions en recherche* : proposition d'un traité sur les armes neurocognitives et d'un autre sur l'IA militaire<sup>7</sup> ; harmonisation des lois nationales (développement de lois spécifiques dans chaque pays pour encadrer l'utilisation des *neuroweapons* comme celle de l'IA militaire) ; mécanismes de vérification (création de systèmes de vérification pour détecter les violations (ex. : inspections par l'OIAC)).

### III-6.3.2 Acceptabilité sociale

L'utilisation de *neuroweapons* – même à des fins défensives – soulève de nombreuses questions éthiques majeures :

- Souveraineté mentale : Le droit des individus à contrôler leur propre esprit.
- Consentement : L'utilisation de ces technologies sans le consentement des personnes ciblées.
- Proportionnalité : L'adéquation entre les moyens utilisés et les objectifs poursuivis.
- Responsabilité : Qui est responsable en cas d'effets secondaires ou de dommages collatéraux ?

*Solutions en recherche* : cadres éthiques (développement de lignes directrices éthiques pour l'utilisation des *neuroweapons* (ex. : "*Neuroethics Framework*")); transparence (divulcation publique des programmes de recherche sur les *neuroweapons*) ; éducation du public (sensibilisation aux risques et aux bénéfices des neurotechnologies).

Ce chapitre a permis d'explorer les fondements scientifiques de la guerre cognitive et cognitive, en montrant comment :

1. Les vulnérabilités cérébrales (neurotransmetteurs, plasticité, biais cognitifs) sont exploitées ;
2. Les technologies offensives agissent sur ces vulnérabilités ;
3. Les contre-mesures scientifiques (détection, neuroprotection, résilience cognitive) peuvent contrer ces attaques.
4. Des limites scientifiques, technologiques, éthiques et juridiques ajoutent à la complexité de cette problématique.

Le Chapitre V approfondira ces questions en les examinant sur la base d'une exploration actualisée en 2026.

## IV - Du position de la guerre cognitive et de la guerre cognitive dans le contexte plus global des guerres hybrides

Il est non seulement possible, mais stratégiquement essentiel de positionner la guerre cognitive (neurobiologique) et la guerre cognitive (informationnelle) dans une cartographie des guerres hybrides.

Cette intégration permet de :

1. Situer ces menaces dans un cadre doctrinal plus large (guerres conventionnelles, cyberguerre, guerre de l'information, etc.) ;
2. Mettre en évidence leurs synergies avec d'autres formes de conflit ;
3. Anticiper les stratégies adverses combinant plusieurs modalités d'attaque ;
4. Définir des contre-mesures intégrées adaptées à une menace multi-dimensionnelle.

<sup>7</sup> Voir à cet égard notamment : Patrice Cardot - [L'IA militaire : enjeux géopolitiques et cadre pour un traité international](#)

Ce chapitre IV propose donc une cartographie détaillée et structurée des guerres hybrides, incluant la guerre cognitive et la guerre cognitive, avec une analyse de leur positionnement, de leurs interactions et de leurs implications stratégiques.

#### **IV – 1. La guerre cognitive et la guerre cognitive au cœur des guerres hybrides : une cartographie stratégique**

L'ère des conflits modernes ne se limite plus aux champs de bataille traditionnels. Elle s'étend désormais à un espace bien plus insidieux et décisif : l'esprit humain.

Dans ce contexte, la guerre cognitive (neurobiologique) et la guerre cognitive (informationnelle) émergent comme des piliers centraux des guerres hybrides, ces stratégies multi-dimensionnelles qui combinent des moyens cinétiques, cybernétiques, économiques et informationnels pour déstabiliser un adversaire sans nécessairement recourir à une déclaration de guerre ouverte.

Pourtant, malgré leur importance croissante, ces deux modalités d'attaque restent souvent mal comprises ou sous-estimées dans les analyses stratégiques. Leur positionnement exact au sein des guerres hybrides, leurs synergies avec les autres formes de conflit, et leurs implications géopolitiques nécessitent une cartographie rigoureuse, capable de révéler à la fois leur originalité et leur intégration systémique dans l'arsenal des États et des acteurs non étatiques.

Ce texte propose donc une analyse structurée de leur place dans les guerres hybrides, en explorant :

- Leur nature distincte et leur complémentarité ;
- Leur positionnement au sein des cinq dimensions des guerres hybrides ;
- Leurs synergies avec les autres formes de conflit ;
- Les défis qu'elles posent aux stratégies de défense traditionnelles ;
- Les implications géopolitiques de leur maîtrise par les grandes puissances.

##### **IV-1.1 Les guerres hybrides : un cadre doctrinal pour comprendre les conflits modernes**

Force est de relever que le monde est entré dans un régime de guerres hybrides permanent conjugué paradoxalement à un régime de coopération (couplage entre coopération et compétition) en matière économique et technologique, générant ainsi un nouveau désordre international systémique dans l'attente et l'espoir d'un nouvel ordre mondial fondé sur une nouvelle approche de la stabilité stratégique et de la sécurité internationale.

Selon l'un des grands arpenteurs de la géopolitique, le géographe Michel Foucher, le désordre international est provoqué par une grande bifurcation : le fil diplomatique (*linkage*) qui reliait les grandes puissances depuis Metternich est aujourd'hui introuvable<sup>8</sup>.

Depuis la fin de la Guerre froide, les conflits ont évolué vers une complexité inédite. Les guerres symétriques entre États, caractéristiques du XXe siècle, ont cédé la place à des affrontements asymétriques, où des acteurs variés — États, groupes armés, entreprises, voire individus — combinent des moyens conventionnels et non conventionnels pour atteindre leurs objectifs. C'est dans ce contexte que le concept de guerre hybride a émergé, formalisé notamment par les travaux de l'OTAN-STO.

La guerre hybride se définit comme une stratégie intégrée qui superpose plusieurs modalités d'action pour déstabiliser un adversaire de manière progressive, déniale et multi-dimensionnelle. Contrairement aux guerres traditionnelles, qui reposent sur des affrontements militaires directs, les guerres hybrides exploitent les failles d'un système — qu'elles soient technologiques, informationnelles, économiques ou neurobiologiques — pour éroder sa résilience sans nécessairement recourir à la force brute.

Trois caractéristiques fondamentales distinguent les guerres hybrides des conflits classiques :

Premièrement, elles reposent sur l'ambiguïté. Les attaques sont souvent déniales, attribuables à des proxys (groupes armés, cybercriminels) ou masquées sous des apparences légitimes (ex. : une

---

<sup>8</sup> Cf. Michel Foucher - [Nous assistons à la fin du monde de Kissinger](#) – Le Grand Continent

cyberattaque attribuée à des "hacktivistes" alors qu'elle est menée par un État). Cette opacité rend difficile l'attribution des responsabilités et complique les réponses proportionnées.

Deuxièmement, elles sont multi-dimensionnelles. Une guerre hybride peut combiner, par exemple, une cyberattaque contre les infrastructures critiques, une campagne de désinformation pour saper le moral de la population, des sanctions économiques pour affaiblir l'économie, et des opérations psychologiques pour influencer les décideurs. Chaque dimension renforce les autres, créant un effet de synergie bien supérieur à la somme des parties.

Enfin, elles sont progressives. Contrairement à une invasion militaire, qui a un impact immédiat et visible, les guerres hybrides s'étalent dans le temps, avec une escalade contrôlée qui permet à l'attaquant de tester les réactions de sa cible et d'ajuster sa stratégie en conséquence.

*Exemple historique* : La stratégie russe en Ukraine depuis 2014 illustre parfaitement cette approche. Avant l'invasion militaire de 2022, la Russie a déstabilisé l'Ukraine via :

- Des opérations de désinformation (fake news, deepfakes) pour diviser la population ;
- Des cyberattaques (*BlackEnergy*, 2015) contre les réseaux électriques ;
- Le soutien à des milices pro-russes dans le Donbass ;
- Des pressions économiques (dépendance énergétique, sanctions).

Cette combinaison de moyens a affaibli l'Ukraine avant même que le premier coup de feu ne soit tiré, démontrant ainsi l'efficacité dévastatrice des guerres hybrides.

#### **IV-1.2 Les cinq dimensions des guerres hybrides : un modèle pour positionner la guerre cognitive et la guerre cognitive**

Pour comprendre où se situent la guerre cognitive (neurobiologique) et la guerre cognitive (informationnelle) dans le paysage des conflits modernes, il est nécessaire de décomposer les guerres hybrides en cinq dimensions fondamentales, chacune correspondant à un type de menace et à un niveau d'intensité spécifique.

La première dimension, la guerre conventionnelle, correspond aux affrontements armés classiques entre États, impliquant des forces militaires régulières (armées de terre, marine, aviation). Son objectif est la destruction physique de l'adversaire, via des opérations militaires directes (batailles, bombardements, invasions). Bien que cette dimension reste centrale dans les conflits modernes, elle est de plus en plus complétée — voire remplacée — par des approches plus subtiles. *Exemple* : la guerre en Ukraine (2022–2026) a montré que même les conflits conventionnels intègrent désormais des éléments hybrides (désinformation, cyberguerre).

La deuxième dimension, la guerre irrégulière, implique des acteurs non étatiques (groupes armés, terroristes, milices) ou des tactiques non conventionnelles (guérilla, attentat, sabotage). Contrairement à la guerre conventionnelle, elle évite les affrontements directs et privilégie les actions asymétriques, souvent menées par des proxys (groupes soutenus par un État). *Exemple* : le soutien iranien aux Houthis au Yémen ou la guerre par procuration en Syrie illustrent comment un État peut déstabiliser un adversaire sans s'engager directement.

La troisième dimension, la cyberguerre, cible les systèmes informatiques et numériques (réseaux, données, infrastructures critiques) pour perturber, espionner ou neutraliser un adversaire. Elle repose sur des technologies avancées (malwares, ransomwares, attaques DDoS) et peut avoir des effets dévastateurs sans recourir à la violence physique. *Exemple* : la cyberattaque contre l'Ukraine en 2015 (*BlackEnergy*), qui a plongé des régions entières dans le noir, a montré comment une cyberguerre pouvait paralyser un pays sans tirer un seul coup de feu.

La quatrième dimension, la guerre de l'information, vise à manipuler les flux d'information pour influencer les perceptions, les croyances et les décisions d'une population ou d'un groupe. Elle repose sur des technologies de désinformation (*fake news*, *deepfakes*) et des stratégies de propagande, souvent amplifiées par les réseaux sociaux et les algorithmes de recommandation. *Exemple* : les campagnes de

désinformation russes (2016–2024) ont sapé la confiance dans les institutions démocratiques en Europe et aux États-Unis, illustrant l’impact sociétal de cette dimension.

La cinquième dimension, la guerre économique, utilise des levier économiques (sanctions, dépendances, pressions commerciales) pour affaiblir un adversaire sans recourir à la force militaire. Elle peut prendre la forme de sanctions ciblées, d’embargos, ou de manipulations des marchés. *Exemple* : les sanctions américaines contre la Russie (2022) ont déstabilisé son économie, montrant comment une guerre économique pouvait compléter une stratégie militaire.

Dans ce cadre, la guerre cognitive et la guerre cognitive se positionnent principalement dans les dimensions 4 (guerre de l’information) et 5 (guerre économique), mais avec des liens transversaux forts avec les dimensions 2 (guerre irrégulière) et 3 (cyberguerre).

La guerre cognitive (neurobiologique) dépasse le cadre de la guerre de l’information en ciblant directement le cerveau humain via des technologies physiques, chimiques ou biologiques. Elle agit comme une couche supplémentaire de manipulation, capable de contourner les défenses traditionnelles (éducation, esprit critique) en agissant sur le substrat neurobiologique de la pensée.

La guerre cognitive (informationnelle), quant à elle, approfondit la guerre de l’information en ciblant les processus de pensée collectifs (perceptions, biais cognitifs, mémoire) avec une précision et une sophistication accrues. Elle exploite les vulnérabilités psychologiques et algorithmiques pour manipuler les esprits à grande échelle.

#### **IV-1.3 La guerre cognitive (neurobiologique) : une dimension transversalement intégrée**

La guerre cognitive — au sens neurobiologique du terme — représente une révolution dans l’art de la guerre, car elle ne cible plus seulement les corps ou les infrastructures, mais l’organe le plus stratégique qui soit : le cerveau humain. En agissant directement sur les mécanismes neurobiologiques (neurotransmetteurs, ondes cérébrales, plasticité synaptique), elle permet de contrôler les émotions, les mémoires et les décisions avec une précision chirurgicale, contournant ainsi les défenses traditionnelles (éducation, esprit critique). Son originalité réside dans sa capacité à s’intégrer de manière transversale dans toutes les dimensions des guerres hybrides.

Dans le cadre de la guerre conventionnelle, la guerre cognitive peut préparer le terrain pour une attaque militaire en désorientant les troupes ennemies. Par exemple, l’utilisation de *neuroweapons* (ondes électromagnétiques, ultrasons) pour induire des maux de tête, des troubles de la mémoire ou des états de panique chez les soldats adverses peut réduire leur capacité de combat avant même que l’affrontement ne commence. *Résultat* : une victoire plus rapide et moins coûteuse, car l’ennemi est déjà affaibli neurobiologiquement.

Dans le cadre de la guerre irrégulière, la guerre cognitive peut renforcer l’efficacité des proxies (groupes armés, terroristes) en manipulant leurs états mentaux. L’utilisation de drogues neuroactives (comme le BZ) ou de neurostimulateurs peut, par exemple, augmenter la suggestibilité des combattants, les rendant plus dociles et plus contrôlables. *Exemple historique* : le projet *MKUltra* de la CIA (1953–1973) a exploré l’utilisation de LSD et d’hypnose pour contrôler des agents, bien que les résultats aient été trop imprévisibles pour un déploiement opérationnel.

Dans le cadre de la cyberguerre, la guerre cognitive peut neutraliser les défenseurs des systèmes critiques. Une cyberattaque contre un centre de commande est beaucoup plus efficace si les opérateurs humains sont désorientés par des *neuroweapons*. *Exemple* : une cyberattaque contre un réseau électrique combinée à une stimulation électromagnétique des techniciens peut paralyser la réponse et amplifier les dégâts.

Dans le cadre de la guerre de l’information, la guerre cognitive amplifie les effets de la désinformation en altérant les capacités critiques des cibles. Une campagne de *fake news* est beaucoup plus efficace si les récepteurs sont neurobiologiquement vulnérables (ex. : stress, fatigue, dépendance aux neurotransmetteurs). *Résultat* : une désinformation qui s’ancre plus profondément dans l’esprit des individus, car leurs mécanismes de remise en question sont affaiblis.

Enfin, dans le cadre de la guerre économique, la guerre cognitive peut déstabiliser les élites économiques en influençant leurs décisions. Une neurostimulation ciblée des dirigeants d'entreprises ou des décideurs politiques peut, par exemple, les pousser à prendre des décisions erronées, sabotant ainsi l'économie de l'adversaire. *Exemple hypothétique* : une onde électromagnétique ciblant le cortex préfrontal d'un PDG pourrait altérer son jugement et le conduire à des choix désastreux pour son entreprise.

On voit donc que la guerre cognitive (au sens neurobiologique) est une forme émergente de guerre hybride qui cible directement le cerveau via des technologies physiques, chimiques ou biologiques. Elle se positionne à l'intersection de plusieurs dimensions :

| Dimension                      | Positionnement de la guerre cognitive                                                                                              | Exemples                                                                                                                           | Synergies avec d'autres formes de guerre hybride                                                                     |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Guerre conventionnelle</b>  | Préparation des troupes : Utilisation de <i>neuroweapons</i> pour désorienter l'ennemi avant une attaque cinétique.                | Ondes EM pour induire des maux de tête chez les soldats ennemis (ex. : <i>Moscow Signal</i> ).                                     | Amplification des effets : Une attaque conventionnelle est plus efficace si l'ennemi est désorienté.                 |
| <b>Guerre irrégulière</b>      | Manipulation des combattants : Utilisation de drogues ou de neurostimulateurs pour contrôler des milices ou des terroristes.       | BZ utilisé pour neutraliser des groupes armés sans combat.                                                                         | Renforcement de la coercition : Permet de contrôler des proxies sans recourir à la force.                            |
| <b>Cyberguerre</b>             | Attaques sur les infrastructures critiques : Utilisation de <i>neuroweapons</i> pour neutraliser les opérateurs de systèmes cyber. | Ondes EM ciblant les centres de commande pour désorienter les décideurs.                                                           | Combinaison avec des cyberattaques : Une cyberattaque est plus efficace si les défenseurs sont incapables de réagir. |
| <b>Guerre de l'information</b> | Amplification des effets : La guerre cognitive renforce la guerre cognitive en altérant les capacités critiques des cibles.        | Combinaison de <i>deepfakes</i> (guerre cognitive) et de <i>neuroweapons</i> (guerre cognitive) pour implanter des faux souvenirs. | Effet de résonance : La désinformation est plus efficace si les cibles sont neurobiologiquement vulnérables.         |
| <b>Guerre économique</b>       | Déstabilisation des élites : Utilisation de <i>neuroweapons</i> pour influencer les décideurs économiques.                         | Neurostimulation ciblant des dirigeants d'entreprises pour les pousser à prendre des décisions erronées.                           | Sabotage des chaînes d'approvisionnement : Une économie est plus vulnérable si ses leaders sont désorientés.         |

La guerre cognitive est donc une dimension transversale : elle renforce les autres formes de guerre hybride (conventionnelle, irrégulière, cyberguerre, guerre de l'information, guerre économique) ; elle agit comme un multiplicateur de puissance (effet de synergie) ; elle cible le substrat le plus stratégique : le cerveau humain.

Ainsi, la guerre cognitive agit comme un multiplicateur de puissance au sein des guerres hybrides, capable de renforcer l'efficacité de toutes les autres dimensions.

#### IV-1.4 La guerre cognitive (informationnelle) : une composante avancée de la guerre de l'information

Si la guerre cognitive cible le substrat neurobiologique de la pensée, la guerre cognitive — au sens informationnel — approfondit la guerre de l'information en ciblant les processus de pensée collectifs avec une précision et une sophistication inédites. Elle ne se contente pas de diffuser de fausses informations : elle exploite les biais cognitifs, les algorithmes et les vulnérabilités psychologiques pour manipuler les esprits à grande échelle.

Son positionnement principal se situe dans la dimension de la guerre de l'information, mais elle interagit fortement avec les autres dimensions des guerres hybrides.

Dans le cadre de la guerre conventionnelle, la guerre cognitive peut saper le moral des troupes avant une attaque. La diffusion de *deepfakes* montrant des défaites fictives ou des trahisons imaginaires peut, par exemple, démoraliser les soldats et réduire leur volonté de combattre.

Prenons un exemple : pendant la guerre opposant Israël au Hezbollah (et plus globalement au Liban), le Premier ministre israélien a affirmé que les villages chrétiens du Sud Liban occupé par l'armée israélienne voulait devenir israélien, affirmation immédiatement démentie par les intéressés. Peu de

temps auparavant, le ministre de la défense israélien avait appelé les principaux chefs militaires israéliens à se préparer à un maintien illimité des forces engagées au Sud Liban. Ces déclarations ont semé la confusion parmi les troupes et la population israélienne, au point de pousser des colons israéliens extrémistes à tenter de venir s'installer dans cette partie sud du Liban (territoire revendiqué par ailleurs par les sionistes religieux israéliens), et à mettre aussitôt en péril le protocole d'accord de paix signé par les autorités politiques libanaises et israéliennes pour violation de la souveraineté libanaise sur son propre territoire.

Dans le cadre de la guerre irrégulière, la guerre cognitive peut faciliter le recrutement et la radicalisation des combattants. Les réseaux sociaux et les algorithmes de recommandation sont utilisés pour cibler des individus vulnérables (jeunes en quête d'identité, personnes en situation de précarité) et les exposer à une propagande extrémiste.

Ceci est parfaitement illustré par le fait que Daech a massivement utilisé les réseaux sociaux pour recruter et radicaliser des individus à travers le monde, en exploitant leurs biais cognitifs (recherche de sens, besoin d'appartenance).

Dans le cadre de la cyberguerre, la guerre cognitive peut amplifier l'impact des cyberattaques en manipulant l'opinion publique. Une cyberattaque contre une infrastructure critique (ex. : réseau électrique) peut être accompagnée d'une campagne de désinformation pour accuser un tiers (ex. : un État voisin) et provoquer des tensions sociales.

Par exemple, une cyberattaque contre un hôpital pourrait être attribuée à tort à un ennemi politique via des fake news, créant ainsi une crise diplomatique.

Dans le cadre de la guerre de l'information, la guerre cognitive représente une évolution qualitative. Contrairement à la désinformation classique, qui se contente de diffuser des mensonges, la guerre cognitive exploite les mécanismes psychologiques pour ancrer durablement les fausses informations dans l'esprit des individus. Elle utilise des technologies avancées (IA générative, deepfakes, réseaux de bots) pour créer des réalités alternatives et fragmenter la conscience collective.

Il n'est pas difficile à cet égard d'observer combien les algorithmes de recommandation des réseaux sociaux amplifient les contenus extrêmes, créant des bulles informationnelles où chaque groupe vit dans une réalité parallèle.

Enfin, dans le cadre de la guerre économique, la guerre cognitive peut manipuler les marchés financiers en diffusant de fausses rumeurs.

Une *fake news* sur la santé financière d'une entreprise peut, par exemple, provoquer une vente massive d'actions et faire chuter son cours en bourse.

De même, les effets d'annonce irrationnels du président Trump lors du conflit qui oppose l'Iran aux USA et à Israël ont généré une variabilité permanente de la situation sécuritaire dans le Détroit d'Ormuz impliquant des risques financiers et économiques facteurs de profits et de pertes colossaux tant sur les marchés boursiers que dans l'économie globale (situation courante dans l'économie globalisée du risque et de l'insécurité).

Fait peu connu du grand public illustrant également ce point précis, en 2013, un tweet faux de l'AP (*Associated Press*) annonçant une attaque à la Maison Blanche a fait chuter le *Dow Jones* de 1 % en quelques minutes, illustrant l'impact immédiat de la désinformation sur les marchés.

| Dimension                     | Positionnement de la guerre cognitive                                                                                                 | Exemples                                                                                   | Synergies avec d'autres formes de guerre hybride                                          |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Guerre conventionnelle</b> | Préparation psychologique : Utilisation de deepfakes ou de désinformation pour saper le moral des troupes ennemies avant une attaque. | Diffusion de fausses informations sur les mouvements de troupes pour désorienter l'ennemi. | Affaiblissement des défenses : Une armée démoralisée est moins efficace au combat.        |
| <b>Guerre irrégulière</b>     | Radicalisation et recrutement : Utilisation de réseaux sociaux et de propagande ciblée pour recruter des combattants.                 | Daech utilise des vidéos de propagande et des deepfakes pour radicaliser des individus.    | Amplification des capacités : Des groupes irréguliers mieux informés sont plus efficaces. |

| Dimension                      | Positionnement de la guerre cognitive                                                                                                              | Exemples                                                                                                            | Synergies avec d'autres formes de guerre hybride                                                               |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Cyberguerre</b>             | Attaques sur les réseaux sociaux : Utilisation de bots et de <i>deepfakes</i> pour manipuler l'opinion publique.                                   | Campagnes de désinformation sur Twitter/X pour influencer des élections.                                            | Combinaison avec des cyberattaques : Une cyberattaque est plus efficace si l'opinion publique est désorientée. |
| <b>Guerre de l'information</b> | Cœur de la guerre cognitive : La guerre cognitive est une forme avancée de la guerre de l'information, ciblant les processus de pensée collectifs. | Utilisation de <i>deepfakes</i> , algorithmes de recommandation, et réseaux de bots pour manipuler les perceptions. | Renforcement mutuel : La guerre de l'information et la guerre cognitive se combinent pour un effet maximal.    |
| <b>Guerre économique</b>       | Manipulation des marchés : Utilisation de <i>fake news</i> économiques pour déstabiliser les marchés financiers.                                   | Diffusion de fausses rumeurs sur la santé financière d'une entreprise pour faire chuter son cours en bourse.        | Déstabilisation économique : Une économie est plus vulnérable si ses acteurs sont mal informés.                |

La guerre cognitive est donc une dimension spécialisée : elle approfondit la guerre de l'information en ciblant les processus de pensée ; elle exploite les biais cognitifs et les vulnérabilités psychologiques ; elle se combine avec d'autres formes de guerre hybride pour un effet synergique.

Ainsi, la guerre cognitive agit comme un catalyseur au sein des guerres hybrides, capable de renforcer l'efficacité de la guerre de l'information, de la cyberguerre et de la guerre économique.

#### IV-1.5 Les synergies entre guerre cognitive, guerre cognitive et autres formes de guerre hybride : l'effet multiplicateur

L'efficacité maximale des guerres cognitive et cognitive ne réside pas dans leur utilisation isolée, mais dans leur combinaison avec d'autres formes de guerre hybride. Ces synergies créent un effet multiplicateur, où chaque dimension amplifie les autres, rendant la menace exponentiellement plus redoutable.

La synergie la plus redoutable est sans doute celle qui combine la guerre cognitive et la guerre cognitive, créant ce que l'OTAN-STO (2024) a nommé l'"effet de résonance cognitive".

Dans ce scénario, la guerre cognitive (informationnelle) sature l'espace mental avec des *fake news*, *deepfakes* et désinformation, réduisant ainsi les capacités critiques des cibles. Puis, la guerre cognitive (neurobiologique) amplifie ces effets en altérant directement les processus cérébraux (via des *neuroweapons*, des drogues ou des stimulations électromagnétiques). *Résultat* : une désorientation exponentielle, où les cibles deviennent incapables de résister à la manipulation. *Exemple concret* : « Opération Éclipse » (Fiction inspirée de faits réels).

Pour illustrer cette synergie entre guerre cognitive et guerre cognitive, analysons un scénario réaliste inspiré des travaux de l'OTAN-STO (2024) et des rapports de la DARPA.

Un État hostile souhaite déstabiliser un pays cible avant une élection présidentielle. Il met en place une opération intégrée combinant guerre cognitive et guerre cognitive, baptisée « Opération Éclipse ».

##### Phase 1 : Préparation du terrain (Guerre cognitive)

*Action* : diffusion massive de *fake news* sur les réseaux sociaux, accusant le gouvernement en place de corruption massive et de préparation d'un coup d'État. *Vecteurs* : réseaux de bots (10 000 comptes automatisés) ; *deepfakes* audio/vidéo (créés avec Sora 2.0) ; Comptes sociaux falsifiés (usurpation d'identités de journalistes et d'influenceurs). *Effets* : polarisation de la population (division en deux camps irréconciliables) ; perte de confiance dans les institutions (médias, gouvernement, experts) ; saturation de l'espace informationnel (impossibilité de distinguer le vrai du faux).

##### Phase 2 : Amplification des effets (Guerre cognitive)

*Action* : utilisation de *neuroweapons* à ondes EM (1–3 GHz) pour induire un état de stress généralisé chez les populations exposées. *Vecteurs* : émetteurs cachés dans des ambassades ou des véhicules banalisés ; ondes pulsées ciblant spécifiquement les zones urbaines les plus sensibles. *Effets* : amplification de l'anxiété (les individus deviennent plus réceptifs aux messages de peur) ; réduction des

capacités critiques (incapacité à évaluer rationnellement les informations) ; paralysie décisionnelle (les décideurs sont incapables de réagir efficacement).

### Phase 3 : *Exploitation des vulnérabilités (Synergie)*

**Action** : Combinaison de *deepfakes* montrant des violences fictives (émeutes, attentats), d'une neurostimulation (ondes EM) pour induire de la peur et de la colère et d'une amplification algorithmique (réseaux de bots pour diffuser massivement les contenus). **Effet** : déstabilisation sociale (émeutes, violences urbaines) ; perte de contrôle des autorités (incapacité à maintenir l'ordre) ; crise politique majeure (chute du gouvernement, intervention militaire).

| Critère          | Attaque purement cognitive    | Attaque purement cognitive         | Attaque intégrée (synergie)                          |
|------------------|-------------------------------|------------------------------------|------------------------------------------------------|
| Efficacité       | ×1                            | ×1                                 | ×4 à ×5 (OTAN-STO, 2024)                             |
| Impact           | Désinformation limitée        | Désorientation individuelle        | Déstabilisation nationale                            |
| Durée des effets | Court terme                   | Court terme                        | Long terme (faux souvenirs, troubles psychiatriques) |
| Coût             | Élevé (technologies avancées) | Très élevé ( <i>neuroweapons</i> ) | Moyen (synergie réduit les coûts)                    |

Ce scénario montre comment la combinaison des deux guerres peut avoir des effets dévastateurs sur une nation entière, avec une efficacité multipliée par rapport à une attaque purement informationnelle ou neurobiologique.

La synergie entre les deux approches permet en effet de cibler à la fois les failles informationnelles et neurobiologiques du cerveau humain, maximisant ainsi l'impact de l'attaque.

Une autre synergie particulièrement redoutable est celle qui combine la guerre cognitive et la cyberguerre, créant une neutralisation totale des défenses.

Dans ce scénario, une cyberattaque cible les systèmes informatiques d'un État (réseaux électriques, centres de commande militaire), tandis que la guerre cognitive cible les opérateurs humains de ces systèmes (via des *neuroweapons*). **Résultat** : une neutralisation complète, car les systèmes sont compromis et les décideurs sont incapables de réagir. **Exemple** : une cyberattaque contre un centre de commande militaire (comme *BlackEnergy* en Ukraine, 2015) combinée à une stimulation électromagnétique des techniciens pourrait paralyser la réponse et amplifier les dégâts de manière décisive.

La synergie entre guerre cognitive et guerre irrégulière permet, quant à elle, un contrôle optimal des proxys. En effet, la guerre irrégulière repose sur l'utilisation de groupes armés non étatiques (milices, terroristes), qui peuvent être difficiles à contrôler. La guerre cognitive peut renforcer ce contrôle en utilisant des drogues neuroactives ou des *neuroweapons* pour manipuler les états mentaux des combattants. **Exemple** : l'administration de BZ à des combattants d'une milice pourrait augmenter leur suggestibilité, les rendant plus dociles et plus contrôlables. **Résultat** : des proxys plus efficaces et moins risqués, car ils exécutent les ordres sans poser de questions.

La synergie entre guerre cognitive et guerre économique permet, enfin, une déstabilisation systémique. La guerre économique cible les marchés, les entreprises et les chaînes d'approvisionnement, tandis que la guerre cognitive cible les décideurs économiques. **Résultat** : une déstabilisation à la fois structurelle et psychologique de l'économie. **Exemple** : la diffusion de *fake news* sur la santé financière d'une grande entreprise peut provoquer une vente massive d'actions par des investisseurs paniqués. **Conséquence** : un krach boursier ou une crise financière, avec des répercussions en cascade sur l'économie.

Enfin, la synergie ultime — et la plus redoutable — est celle qui combine toutes les dimensions des guerres hybrides, créant une guerre totale hybride.

Dans ce scénario, un État pourrait déstabiliser un adversaire en combinant guerre cognitive et guerre cognitive pour désorienter la population et les troupes, cyberguerre pour neutraliser les systèmes de défense, guerre conventionnelle pour envahir militairement et guerre économique pour empêcher une reprise.

### Exemple hypothétique :

Phase 1 : Campagne de désinformation (*deepfakes*, réseaux de bots) + *neuroweapons* (ondes EM) pour désorienter la population et les troupes ;

Phase 2 : Cyberattaque contre les réseaux électriques et de communication ;

Phase 3 : Invasion militaire alors que l'ennemi est désorganisé et démoralisé ;

Phase 4 : Sanctions économiques pour empêcher une reprise.

**Résultat** : Un effondrement rapide de l'État cible, avec une efficacité multipliée par 5 à 10 par rapport à une guerre conventionnelle seule.

### Positionnement de la guerre cognitive et de la guerre cognitive

| Type de menace \ Niveau de ciblage | Individuel                     | Collectif             | Sociétal               | Étatique                |
|------------------------------------|--------------------------------|-----------------------|------------------------|-------------------------|
| Physique                           | Assassinat, kidnapping         | Attaques de drones    | Guerre conventionnelle | Invasion militaire      |
| Économique                         | Chantage, escroquerie          | Cybercriminalité      | Sanctions ciblées      | Guerre économique       |
| Neurobiologique                    | <i>Neuroweapons</i> (ondes EM) | Drogues neuroactives  | Guerre cognitive       | Manipulation des élites |
| Informationnelle                   | Phishing, harcèlement          | Désinformation ciblée | Guerre cognitive       | Propagande d'État       |

On voit donc que la guerre cognitive et la guerre cognitive s'intègrent pleinement dans le cadre des guerres hybrides. Ces synergies démontrent que ces guerres ne sont pas des phénomènes isolés, mais des composantes essentielles des guerres hybrides modernes, capables de transformer radicalement la nature des conflits.

Les deux formes de guerre (cognitive et cognitive) se combinent pour couvrir tous les niveaux de ciblage (individuel à étatique) et tous les types de menace (informationnelle à neurobiologique).

### IV-2 Cartographie géopolitique : Qui domine les guerres cognitive et cognitive ?

La maîtrise des guerres cognitive et cognitive est devenue un enjeu géopolitique majeur, avec des asymétries croissantes entre les puissances.

Les États sont les principaux acteurs de ces guerres, avec des capacités et des objectifs variés. Leur implication reflète une course aux armements sans précédent, où les technologies de manipulation mentale deviennent aussi importantes que les armes conventionnelles.

Les États investissent massivement dans ces deux formes de guerre, avec des stratégies à la fois offensives et défensives. Les budgets alloués à ces technologies sont en constante augmentation :

- 50 milliards de dollars par an dans les technologies de guerre cognitive et cognitive (2026) ;
- 10 à 15 % des budgets de R&D militaire sont consacrés à ces technologies ;
- Croissance annuelle : 20 % pour les technologies de guerre cognitive (neurobiologique).

Certaines nations ont investi massivement dans ces technologies, tandis que d'autres peinent à suivre le rythme, créant ainsi des déséquilibres stratégiques qui pourraient redéfinir l'ordre mondial.

A - Les États-Unis se positionnent comme le leader incontesté dans les deux dimensions. Leur avance technologique (DARPA, NSA, Big Tech) leur permet de dominer à la fois la guerre cognitive et la guerre cognitive. Leur stratégie repose sur une défense proactive (détection des attaques, neuroprotection) et une capacité de contre-attaque (développement de leurs propres armes cognitives).

B - La Chine est le seul concurrent sérieux des États-Unis, avec des capacités comparables dans les deux dimensions. Son modèle autoritaire lui permet de mobiliser massivement les ressources (étatiques et

privées) pour développer des technologies de guerre cognitive et cognitive. *Exemple* : le projet "Brain Initiative" chinois ou les avancées de l'entreprise ByteDance (TikTok) dans l'IA générative montrent leur volonté de dominer ces domaines. Leur stratégie vise à étendre leur influence mondiale via le contrôle de l'information et la maîtrise des neurotechnologies.

C - La Russie, bien que moins avancée dans la guerre cognitive (neurobiologique), excelle dans la guerre cognitive (désinformation, propagande/slopagande<sup>9</sup>). Ses campagnes de désinformation ont démontré leur efficacité en déstabilisant les démocraties occidentales. *Exemple* : les ingérences russes supposées dans les élections américaines (2016) et européennes (2017–2024) ont sapé la confiance dans les institutions et amplifié les divisions sociétales. Cependant, ses capacités en guerre cognitive (neurobiologique) restent limitées, en raison de contraintes technologiques et financières. Mais ces campagnes visent désormais la population russe elle-même : un enseignement important pour els autres nations dont certains dirigeants pourraient être tentés d'y recourir aussi.

D - L'Union européenne, bien qu'en retard dans le développement des armes cognitives, investit dans les contre-mesures. Son approche repose sur la réglementation (*Digital Services Act, Digital Markets Act*), l'éducation (littératie cognitive, médiatique) et la coopération internationale. *Exemple* : la Finlande, souvent citée comme un modèle, a intégré la pensée critique dans son système éducatif, réduisant ainsi la vulnérabilité de sa population aux *fake news*. Cependant, son manque d'autonomie technologique (dépendance aux États-Unis et à la Chine pour les neurotechnologies et l'IA) la rend vulnérable à long terme.

E - Israël se distingue par sa maîtrise de la cyberguerre et son avance en neurotechnologies militaires. Sa stratégie repose sur la souveraineté technologique et la défense proactive. *Exemple* : l'Unit 8200 (unité de renseignement militaire israélienne) est l'une des plus avancées au monde en matière de cyberguerre et de guerre cognitive, tandis que des entreprises comme NSO Group développent des technologies de surveillance cérébrale.

Cartographie des capacités en 2026

| Pays/Alliance    | Capacité en Guerre cognitive (Neurobiologique)  | Capacité en Guerre cognitive (Informationnelle)   | Synergie Opérationnelle | Niveau de menace | Stratégie dominante                           |
|------------------|-------------------------------------------------|---------------------------------------------------|-------------------------|------------------|-----------------------------------------------|
| États-Unis       | ★★★★★ (DARPA, NSA, Big Tech)                    | ★★★★★ (IA générative, réseaux sociaux)            | ★★★★★                   | Extrême          | Défense + Contre-attaque                      |
| Chine            | ★★★★ (Recherche militaire en neurotechnologies) | ★★★★★ (IA générative, censure algorithmique)      | ★★★★                    | Élevé            | Domination technologique + Influence mondiale |
| Russie           | ★★★ (Moscow Signal, programmes hérités)         | ★★★★ (Désinformation historique, réseaux de bots) | ★★★                     | Moyen            | Déstabilisation de l'Occident                 |
| Union Européenne | ★★ (Recherche académique limitée)               | ★★ (Réglementations, ENISA, ANSSI)                | ★★                      | Faible           | Protection des citoyens                       |
| Israël           | ★★★ (Neurotechnologies militaires)              | ★★★★ (Cybersécurité, Unit 8200)                   | ★★★★                    | Élevé            | Souveraineté technologique                    |
| Corée du Nord    | ★★ (Programmes classifiés)                      | ★★★ (Cyberattaques, propagande)                   | ★★★                     | Moyen            | Dissuasion asymétrique                        |
| Iran             | ★★ (Drogues neuroactives, ondes EM basiques)    | ★★★ (Cyberattaques, désinformation)               | ★★                      | Faible           | Guerre par procuration                        |

<sup>9</sup> Voir notamment à cet égard Guillaume Lancereau - [Vladimir Poutine a un problème avec l'intelligence artificielle](#) - Le Grand Continent

Cette course aux armements cognitifs risque de déstabiliser l'équilibre géopolitique mondial, en donnant un avantage stratégique aux pays capables de maîtriser ces technologies.

F - Les acteurs non étatiques (groupes criminels, terroristes, entreprises, individus) jouent un rôle de plus en plus important dans la guerre cognitive et cognitive.

Leur implication « démocratise » l'accès à ces armes, rendant les attaques plus fréquentes, moins prévisibles et plus difficiles à attribuer. *Exemple* : des groupes terroristes comme Daech utilisent déjà les réseaux sociaux pour recruter et radicaliser, tandis que des cybercriminels exploitent les deepfakes pour des arnaques ou des chantages.

À l'avenir, l'accès aux *neuroweapons* (via le marché noir ou des fuites technologiques) pourrait élargir encore le cercle des acteurs capables de mener des attaques cognitives.

#### Acteurs non étatiques et leurs motivations

| Acteur                                                     | Capacités en Guerre Cognitive                                                                                   | Capacités en Guerre Cognitive                                                                | Objectifs                                                                | Exemples                                                                   |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Groupes terroristes</b><br>(ex. : Daech, Al-Qaïda)      | Désinformation (propagande en ligne), réseaux de bots, <i>deepfakes</i> pour le recrutement.                    | Drogues psychotropes (BZ, scopolamine), <i>neuroweapons</i> artisanales (ondes EM basiques). | Recrutement, radicalisation, déstabilisation des États cibles.           | Daech : utilisation de <i>deepfakes</i> pour la propagande (2017–2020).    |
| <b>Groupes criminels</b><br>(ex. : mafias, cybercriminels) | <i>Phishing</i> cognitif (arnaques personnalisées), désinformation financière.                                  | Drogues neuroactives (scopolamine, GHB), <i>neuroweapons</i> de contrefaçon.                 | Fraude financière, chantage, contrôle de marchés illégaux.               | Cybercriminalité en Afrique de l'Ouest (2020–2026).                        |
| <b>Entreprises</b> (ex. : Cambridge Analytica, Meta)       | Manipulation algorithmique (ciblage comportemental), <i>deepfakes</i> publicitaires.                            | Neurostimulation (publicités ciblées via BCI), drogues d'amélioration cognitive.             | Influence des comportements des consommateurs, maximisation des profits. | Scandale Facebook-Cambridge Analytica (2018).                              |
| <b>Individus</b> (ex. : hackers, influenceurs)             | Création de <i>deepfakes</i> (outils accessibles : <i>Sora</i> , <i>MidJourney</i> , <i>Stable Diffusion</i> ). | Utilisation de drogues ou de dispositifs de neurostimulation artisanaux.                     | Vengeance personnelle, manipulation, notoriété.                          | Cas de <i>deepfakes</i> utilisés pour du harcèlement ou de la diffamation. |

L'implication des acteurs non étatiques a trois conséquences majeures :

A - *Démocratisation des armes* : les technologies deviennent accessibles à un nombre croissant d'acteurs, y compris des individus isolés.

B - *Attaques moins prévisibles* : Les acteurs non étatiques innovent et expérimentent avec des méthodes imprévisibles, rendant les attaques plus difficiles à anticiper.

C - *Difficulté d'attribution* : Les attaques sont plus difficiles à tracer, surtout lorsqu'elles combinent plusieurs vecteurs (ex. : *deepfakes* + *neuroweapons*).

Cette cartographie révèle une réalité géopolitique inquiétante : les guerres cognitive et cognitive deviennent un facteur de puissance décisif, potentiellement plus important que les armes nucléaires ou conventionnelles. Les États qui maîtrisent ces technologies auront un avantage stratégique majeur, capable de redéfinir les équilibres mondiaux.

### IV-3. Implications stratégiques : comment se défendre contre les guerres cognitive et cognitive dans un cadre hybride ?

Face à l'essor des guerres cognitive et cognitive et à leur intégration dans les stratégies hybrides, les États et les sociétés doivent repenser leur approche de la défense.

Une réponse fragmentée — ciblant uniquement l'une ou l'autre dimension — serait vouée à l'échec. Seule une défense intégrée, combinant neuroprotection, éducation cognitive, cybersécurité, résilience

économique et coopération internationale, peut espérer contrer une menace aussi complexe et synergique.

La première ligne de défense réside dans la neuroprotection, c'est-à-dire la protection du cerveau contre les attaques neurobiologiques.

Cette approche repose sur plusieurs piliers complémentaires :

A - *Le blindage électromagnétique* : les casques Faraday (en cuivre ou aluminium) ou les cages de Faraday (pour les bâtiments sensibles) permettent de bloquer les ondes EM (micro-ondes, radiofréquences) utilisées par les *neuroweapons*. *Exemple* : les casques militaires (comme ceux développés par Faraday Defense) ou les salles de crise blindées offrent une protection collective contre les attaques par ondes EM.

B - *La détection des neuroweapons* : des capteurs spécialisés (détecteurs de champs EM, capteurs ultrasoniques) peuvent alerter en cas d'attaque, permettant une réaction rapide. *Exemple* : les systèmes de détection de la DARPA (comme le *NeuroThreat Detection System*, 2026) sont conçus pour identifier les attaques par ondes EM ou ultrasons.

C - *Les antidotes neuropharmacologiques* : des médicaments spécifiques (atropine pour le sarin, physostigmine pour le BZ) peuvent neutraliser les effets des neurotoxines. *Exemple* : le programme *Neuroprotection Initiative* de la DARPA travaille sur des antidotes universels capables de contrer une large gamme de neurotoxines.

D - *Le renforcement de la résilience neurobiologique* : des techniques comme la méditation, le neurofeedback ou l'entraînement cognitif peuvent réduire la vulnérabilité aux manipulations. *Exemple* : le programme "*Mind Fitness Training*" de l'US Army a réduit de 60 % les cas de PTSD chez les soldats, tout en améliorant leur résilience cognitive.

La deuxième ligne de défense consiste à protéger les flux d'information, via une défense informationnelle robuste.

Cette approche repose sur :

A - *L'authentification des contenus* : des technologies comme la blockchain (Truepic, Adobe CAI) ou les signatures cryptographiques permettent de certifier l'origine et l'intégrité des médias (images, vidéos, documents). *Exemple* : le standard C2PA (*Coalition for Content Provenance and Authenticity*) vise à créer un cadre universel pour l'authentification des contenus.

B - *La détection des deepfakes et des réseaux de bots* : des algorithmes d'IA (*Deepware Scanner*, *Microsoft Video Authenticator*) ou des analyses comportementales (*Botometer*, *Graphika*) permettent d'identifier les contenus manipulés et les comptes automatisés. *Exemple* : les outils comme *Originality.ai* ou *Grover (AllenAI)* peuvent détecter les contenus générés par IA avec une précision de 85 à 95 %.

C - *L'éducation aux médias et à la pensée critique* : la littératie cognitive (formation à la détection des biais, vérification des faits) est la défense la plus efficace à long terme. *Exemple* : la Finlande, qui a intégré la pensée critique dans son système éducatif, a réduit de 30 % la vulnérabilité de sa population aux fake news.

D - *La réglementation des plateformes numériques* : des lois comme le *Digital Services Act* (UE, 2024) imposent aux réseaux sociaux une transparence algorithmique et une responsabilité accrue dans la lutte contre la désinformation.

La troisième ligne de défense vise à protéger les systèmes numériques, via une cybersécurité renforcée.

Cette approche repose sur :

A - *La sécurité des infrastructures critiques* : des normes strictes (NIS2 en UE, blindage des systèmes SCADA) permettent de protéger les réseaux (énergie, santé, défense) contre les cyberattaques. *Exemple* : les exercices de cybersécurité de l'OTAN (comme *Locked Shields*) testent la résilience des États membres face aux cybermenaces.

B - *La détection précoce des intrusions* : des systèmes comme les *firewalls*, les IDS (*Intrusion Detection Systems*) ou les SIEM (*Security Information and Event Management*) permettent de détecter et bloquer les cyberattaques avant qu'elles n'atteignent leur cible. *Exemple* : le Centre européen de cybersécurité (EC3 / ENISA) coordonne les efforts de détection et de réponse aux cybermenaces en Europe.

C - *La résilience des systèmes* : des mesures comme la redondance, les sauvegardes hors ligne ou les plans de reprise d'activité permettent de limiter l'impact des cyberattaques. *Exemple* : les entreprises critiques (banques, hôpitaux) investissent massivement dans la cyberrésilience pour éviter les paralysies totales.

La quatrième ligne de défense consiste à protéger l'économie, via une résilience économique accrue.

Cette approche repose sur :

A - *La souveraineté technologique* : Les États doivent réduire leur dépendance aux technologies critiques (IA, semi-conducteurs, neurotechnologies) en développant leurs propres capacités. *Exemple* : le projet européen *Human Brain Project* (2020–2030) vise à accélérer la recherche en neurosciences pour réduire la dépendance à la Chine et aux États-Unis.

B - *La protection des données neurobiologiques et comportementales* : des règlements comme le RGPD (Règlement Général sur la Protection des Données) doivent être renforcés pour empêcher l'exploitation des données cérébrales et comportementales par des acteurs malveillants. *Exemple* : la Commission européenne propose des amendes proportionnelles au chiffre d'affaires mondial (jusqu'à 10 %) pour les entreprises qui violent les règles de protection des données.

C - *La résilience des chaînes d'approvisionnement* : la diversification des fournisseurs et les stocks stratégiques permettent de limiter les risques de rupture. *Exemple* : la relocalisation de la production de semi-conducteurs en Europe et aux États-Unis vise à réduire la dépendance à la Chine.

D - *La lutte contre la désinformation économique* : des autorités de régulation (AMF, SEC) et des outils d'analyse des réseaux sociaux permettent de détecter et contrer les manipulations des marchés. *Exemple* : la SEC (*Securities and Exchange Commission*) aux États-Unis surveille les fausses rumeurs sur les marchés financiers pour éviter les krachs boursiers.

Enfin, la cinquième ligne de défense repose sur la coopération internationale, indispensable pour contrer une menace transnationale.

Cette approche repose sur :

A - *Des traités internationaux sur les neuroweapons et l'IA militaire* (et plus globalement sur les systèmes d'armes autonomes) : une interdiction des *neuroweapons* offensifs et une réglementation des recherches en neurotechnologies comme une interdiction des IA militaires à but offensif permettraient de limiter - *de jure* davantage que *de facto* ... - leur prolifération à condition, notamment, que des processus de vérification efficaces les accompagnent (peu probable). *Exemple* : l'OTAN a proposé en 2024 un *Neuroweapons Non-Proliferation Treaty*, inspiré du Traité sur la non-prolifération des armes nucléaires (TNP).

B - *Le partage de renseignements* : une coopération renforcée entre États (OTAN-STO, Interpol, Europol, Centre de renseignements de l'UE) permettrait de détecter et contrer les menaces cognitives et cognitives. *Exemple* : le Centre de cyberdéfense de l'OTAN (CCDCOE) coordonne déjà les efforts de cybersécurité entre les États membres.

C - *L'harmonisation des réglementations* : Des normes internationales sur l'IA, les *deepfakes* et les neurotechnologies permettraient de limiter les abus. *Exemple* : les résolutions de l'ONU sur les technologies émergentes visent à encadrer leur utilisation pour éviter les dérives.

D - *Les exercices communs* : des simulations de guerres cognitives permettraient de tester les défenses et de renforcer la coopération. *Exemple* : les exercices *Cognitive Warfare Exercises* de l'OTAN-STO permettent aux États membres de s'entraîner à contrer les attaques cognitives.

Cette approche intégrée montre que la défense contre les guerres cognitive et cognitive ne peut être efficace que si elle combine neuroprotection, éducation cognitive, cybersécurité, résilience économique et coopération internationale.

Aucune mesure seule ne suffit : c'est la combinaison de toutes ces couches qui permettra de contrer une menace aussi complexe et synergique.

## **V - L'irréversibilité des processus de guerre cognitive et cognitive dans un monde sans contraintes éthiques**

*Analyse des pistes de recherche mondiales sur les systèmes polémogènes ciblant l'esprit humain*

### **Introduction : Le basculement stratégique vers l'esprit comme champ de bataille**

En 2026, la guerre cognitive (déjà opérationnelle à grande échelle) et la guerre cognitive (en phase de déploiement accéléré) ne relèvent plus de la spéculation. Elles constituent une réalité géostratégique, intégrée dans les doctrines militaires des grandes puissances (États-Unis, Chine, Russie, OTAN, Union européenne).

Ce chapitre identifie les pistes de recherche les plus avancées pour chaque domaine, en maintenant strictement la distinction conceptuelle établie ci-dessus. Il démontre par ailleurs que les deux processus sont désormais irréversibles : les États ont choisi de s'affranchir systématiquement des contraintes éthiques, morales et juridiques pour développer des systèmes polémogènes offensifs et défensifs ciblant l'esprit humain, et non plus seulement la matière (corps, infrastructures, matériels).

Ce basculement marque l'émergence de deux paradigmes conflictuels distincts mais complémentaires :

- La guerre cognitive comme arme asymétrique de masse (désinformation, manipulation narrative).
- La guerre cognitive comme arme de précision neurobiologique (neurostimulation, armes psychotronics).

Contrairement aux armes conventionnelles, ces systèmes agissent sans trace physique visible, mais avec des effets durables, cumulatifs, et pour la guerre cognitive, potentiellement irréversibles sur les populations ciblées.

### **V-1. Les pistes de recherche mondiales en 2026 : Un état de l'art exhaustif et distingué**

Les travaux de recherche se concentrent sur deux ensembles strictement séparés, bien que parfois complémentaires en opération :

1. Les pistes liées à la guerre cognitive (manipulation psychologique et informationnelle).
2. Les pistes liées à la guerre cognitive (ciblage physiologique du cerveau).

Chacun de ces ensembles est exploré par des laboratoires civils et militaires, des think tanks stratégiques, et des entreprises spécialisées (défense, IA, neurosciences, cyber).

#### **A. Pistes de recherche en guerre cognitive (manipulation psychologique et informationnelle)**

Objectif global : Influencer les processus mentaux (croyances, décisions, émotions) via des mécanismes psychologiques et informationnels, sans altération physiologique directe du cerveau.

##### **1. Sciences cognitives et psychologie de la manipulation**

Pistes de recherche documentées

*Exploitation des biais cognitifs* : études approfondies sur les biais de confirmation, d'ancrage, de cadre (*framing*), et d'autorité pour concevoir des messages manipulés maximisant leur impact sur les cibles ; développement de modèles prédictifs du comportement humain sous influence informationnelle (recherches menées par le MIT Media Lab, l'Université de Cambridge, et le CNRS français).

Source : [Les Clionautes, Guerre cognitive et pop culture, 2025.](#)

*Psychologie des foules et des réseaux* : modélisation des dynamiques de propagation des informations dans les réseaux sociaux et les communautés en ligne (projet *Social Network Analysis* de la DARPA) ; identification des points de bascule (*tipping points*) où une désinformation devient virale et incontrôlable.

*Manipulation narrative et ingénierie des récits* : développement de cadres narratifs (*narrative frameworks*) pour structurer les perceptions d'un conflit ou d'un enjeu géopolitique ; utilisation de l'IA générative pour créer des récits cohérents et persuasifs, adaptés aux contextes culturels des cibles.

#### Acteurs clés (Guerre cognitive)

| Pays/Organisation | Programmes/Institutions                                     | Spécialisation                                  |
|-------------------|-------------------------------------------------------------|-------------------------------------------------|
| États-Unis        | Cyber Command, NSA, DARPA, RAND Corporation                 | Cyber-guerre cognitive, analyse comportementale |
| Chine             | Cyber Army (PLA Unit 61398), Bureau de la Sécurité Internet | Désinformation massive, manipulation narrative  |
| Russie            | FSB, GRU, Internet Research Agency (IRA)                    | Troll farms, deepfakes, ingérence électorale    |
| Union européenne  | ENISA, Europol, Centre d'Excellence CCDCOE                  | Résilience cyber-cognitive, contre-mesures      |
| OTAN              | Centre d'Excellence pour la Guerre Cognitive (Tallinn)      | Doctrine, coordination internationale           |
| Israël            | Unit 8200, NSO Group                                        | Cyber-psychologie, ciblage individuel           |

## 2. Intelligence Artificielle et automatisation de la manipulation

Pistes de recherche documentées

*Micro-ciblage algorithmique* : utilisation de l'IA générative (LLM, GANs) pour créer des messages ultra-personnalisés, exploitant les biais cognitifs, les peurs et les croyances des individus cibles ; développement de systèmes de profiling cognitif basés sur l'analyse des données biométriques (rythme cardiaque, mouvement des yeux, expressions faciales) et des traces numériques (historique de navigation, réseaux sociaux).

Source : [Polytechnique Insights, Ce que révèlent sept années de recherche militaro-civile, 2025.](#)

*Détection des signaux faibles et contre-manipulation* : algorithmes de *machine learning* capables d'identifier des modifications subtiles du comportement (changement de ton, de vocabulaire, de rythme de communication) pour détecter une manipulation cognitive en cours ou une vulnérabilité exploitable.

Applications : contre-espionnage, protection des décideurs, détection des campagnes de désinformation (projet *EU Digital Services Act*).

*Simulation de propagation informationnelle* : modélisation des réseaux sociaux et des mécanismes de viralité pour prédire l'impact de messages manipulés (outils développés par RAND Corporation, MITRE, et l'Agence européenne de défense) ; utilisation de jumeaux numériques (*digital twins*) de populations pour tester l'efficacité des campagnes cognitives avant leur déploiement.

*IA et désinformation adaptative* : systèmes capables de générer dynamiquement des faux contenus (textes, images, vidéos, voix) adaptés au contexte culturel et psychologique des cibles ; intégration de modèles de langage neuronaux (comme ceux de *Mistral AI* ou *Google DeepMind*) pour produire des narratifs crédibles et persuasifs en temps réel.

## 3. Cyber-guerre cognitive et manipulation des infrastructures informationnelles

Pistes de recherche documentées

*Attaques par surcharge informationnelle* : déploiement de botnets et de fermes de trolls pour inonder les réseaux sociaux de fausses informations, de désinformation ciblée et de contenus polarisants (stratégie mise en œuvre par la Russie en Ukraine et par la Chine contre Taïwan) ; utilisation de l'IA pour générer des deepfakes audio et vidéo en temps réel (exemple : fausse déclaration de guerre ou fausse crise humanitaire).

Source : [Les Clionautes, Guerre cognitive et pop culture, 2025.](#)

*Manipulation des algorithmes de recommandation* : détournement des plateformes (Facebook, Twitter/X, TikTok, YouTube) pour amplifier des narratifs hostiles ou supprimer des informations légitimes (recherches du MIT Media Lab et de l'Université de Cambridge) ; développement de systèmes de contre-manipulation pour protéger les populations (projet OTAN CCDCOE).

*Attaques sur les systèmes de confiance* : ciblage des médias traditionnels, des institutions éducatives et des autorités religieuses pour saper la cohésion sociale (stratégie documentée dans le rapport OTAN 2025 sur la guerre cognitive) ; utilisation de fausses preuves scientifiques pour discréditer des opposants (exemple : campagnes de désinformation sur les vaccins ou le changement climatique).

*Guerre cognitive dans le métavers* : développement de mondes virtuels manipulés pour entraîner des soldats, tester des scénarios de désinformation, ou cibler des populations spécifiques via des avatars contrôlés par l'IA (projet *Metaverse Warfare* du Pentagone).

## **B. Pistes de recherche en guerre cognitive (ciblage physiologique du cerveau)**

Objectif global : Modifier directement les états de conscience et les processus neurobiologiques via des technologies matérielles agissant sur le cerveau, avec des effets potentiellement irréversibles.

### **1. Neurosciences appliquées à la guerre**

Pistes de recherche documentées

*Cartographie fonctionnelle du cerveau en temps réel* : utilisation de l'IRMf portable et des capteurs EEG avancés pour identifier les zones cérébrales associées à la prise de décision, à la mémoire et à l'émotion ; projets DARPA NESD (*Neural Engineering System Design*) et *Human Brain Project* (UE) pour développer des interfaces cerveau-machine à haute résolution ; développement de modèles prédictifs des réactions cognitives à des stimuli externes (ondes, messages, images).

Source : [Fondapol, Neurosciences et comportements militaires, 2026.](#)

*Neurostimulation ciblée* : recherches sur les technologies de stimulation magnétique transcrânienne (TMS) et de stimulation électrique transcrânienne (TES) pour modifier temporairement l'activité neuronale ; projet SPREADS de l'OTAN (2026) pour intégrer ces technologies dans les doctrines de défense cognitive.

Applications potentielles : désorientation des adversaires, renforcement de la résilience cognitive des soldats, ou induction d'états de suggestion accrue (hypnose forcée).

Source : [Revue Défense Nationale, Projet SPREADS et guerre cognitive totale, 2026.](#)

*Neurobiologie des symptômes psychotroponiques* : études sur le syndrome de La Havane (2016-2026) et les effets des rayonnements dirigés sur le cerveau (rapports du Ministère de la Défense américain et de l'Académie des Sciences française) ; identification de mécanismes d'altération neurobiologique : lésions du tissu cérébral, modifications de l'activité synaptique, ou dégénérescence neuronale liée à des expositions à des ondes électromagnétiques ciblées.

Source : [Polytechnique Insights, Guerre cognitive : le nouveau champ de bataille, 2025.](#)

*Soldat augmenté et résilience cognitive* : développement de dispositifs de *neurofeedback* pour améliorer la concentration, la résistance au stress et la prise de décision sous pression ; intégration de stimulateurs cérébraux portables dans les équipements militaires (casques, combinaisons) – programme CReC (Centre de Recherche des Écoles de Coëtquidan).

Source : [Fondapol, 2026.](#)

Acteurs clés (Guerre cognitive – Neurosciences)

| Pays/Organisation | Programmes/Institutions          | Spécialisation                           |
|-------------------|----------------------------------|------------------------------------------|
| États-Unis        | DARPA (NESD, TMS), CIA, NSA, ARL | Neurostimulation, interférence neuronale |

|                         |                                                       |                                                 |
|-------------------------|-------------------------------------------------------|-------------------------------------------------|
| <b>Chine</b>            | Académie des Sciences Militaires, Université de Pékin | Neurosciences offensives, guerre psychotronique |
| <b>Russie</b>           | Institut Kourtchatov, Almaz-Antey                     | Armes psychotroniques, ondes scalaires          |
| <b>OTAN</b>             | Centre d'Excellence CCDCOE (Tallinn)                  | Doctrine, coordination internationale           |
| <b>Union européenne</b> | Projet SPREADS, Horizon Europe                        | Résilience cognitive, contre-mesures            |
| <b>France</b>           | CRcC, DGSE, Thales, Airbus Defence & Space            | Neurosciences militaires, systèmes défensifs    |

## 2. Armes psychotroniques et technologies à énergie dirigée

Pistes de recherche documentées

*Armes à micro-ondes pulsées* : technologies dérivées des radars actifs et des systèmes de communication militaire pour induire des effets neurologiques (maux de tête, vertiges, confusion, hallucinations) chez les cibles ; brevets US 6,076,023 (1998) et US 6,587,729 (2003), toujours exploités et perfectionnés en 2026.

Applications : Dénis de zone cognitive (empêcher l'accès à une zone en désorientant les adversaires), neutralisation de cibles humaines sans violence physique visible.

Source : [Matière à Réflexion, Enquête sur la guerre psychotronique secrète, 2026.](#)

*Armes acoustiques et infrasoniques* : utilisation de fréquences sonores basses (infrasons, < 20 Hz) pour induire des états de panique, de nausée, de soumission ou d'inconscience chez les cibles ; recherches menées par le Laboratoire de Recherche de l'Armée américaine (ARL) et l'Institut de Recherche Scientifique Kourtchatov (Russie) ; déploiement de haut-parleurs directionnels (comme le LRAD – *Long Range Acoustic Device*) pour diffuser des messages subliminaux ou des sons incapacitants sur de longues distances.

*Armes à laser psychotroniques* : développement de lasers à basse énergie capables de stimuler ou perturber l'activité neuronale via des effets photoélectriques ou photothermiques ; projet DEUS (*Directed Energy for Urban Security*) de l'Union européenne pour des applications de contrôle de foule et de neutralisation de tireurs isolés.

*Nanotechnologies et neurotoxines* : recherches sur des nanoparticules capables de traverser la barrière hémato-encéphalique pour livrer des substances psychoactives ciblant des zones spécifiques du cerveau ; projet NANOBRAIN de l'Agence européenne de défense (EDA) pour des applications offensives et défensives ; développement de gaz neurotoxiques à effet retardé ou sélectif (ciblant uniquement certaines populations génétiquement prédisposées).

Acteurs clés (Guerre cognitive – Armes psychotroniques)

| Pays/Organisation    | Programmes/Institutions             | Spécialisation                                    |
|----------------------|-------------------------------------|---------------------------------------------------|
| <b>États-Unis</b>    | DARPA (DEUS), ARL, CIA              | Micro-ondes, lasers, nanotechnologies             |
| <b>Chine</b>         | Académie des Sciences de Chine      | Armes à énergie dirigée, ondes scalaires          |
| <b>Russie</b>        | Institut Kourtchatov, Almaz-Antey   | Armes psychotroniques, infrasons                  |
| <b>Israël</b>        | Rafael Advanced Defense Systems     | Systèmes de défense cognitive, lasers             |
| <b>Corée du Nord</b> | Bureau 39 (renseignement militaire) | Armes électromagnétiques (rumeurs non confirmées) |

## 3. Systèmes polymogènes intégrés et doctrine de la guerre cognitive totale

Pistes de recherche documentées

*Systèmes de guerre cognitive hybrides* : intégration de capteurs biométriques, de l'IA prédictive et de technologies psychotroniques dans des plateformes unifiées (exemple : Système de Défense Cognitive Intégrée – SDCI de l'OTAN, en développement en 2026) ; capacité à cibler simultanément des individus,

des groupes et des populations entières via des canaux multiples (médias, réseaux sociaux, ondes électromagnétiques, agents humains).

*Doctrine de la guerre cognitive totale* : développement d'une stratégie globale pour la guerre cognitive, incluant la militarisation de l'espace informationnel (contrôle des réseaux, des médias, des données), la psychologisation des conflits (ciblage des émotions, des croyances, des valeurs) et la neuro-stratégie (utilisation des neurosciences pour anticiper et influencer les décisions adverses).

Source : [Revue Défense Nationale, Projet SPREADS et l'hypothèse de la guerre cognitive totale, 2026.](#)

*Armes cognitives autonomes* : développement de systèmes d'IA autonomes capables de planifier et exécuter des opérations cognitives sans intervention humaine ; projet AEGIS-Cog du Ministère de la Défense britannique pour des applications de contre-manipulation automatique.

Risques majeurs : Perte de contrôle, escalade involontaire, effets imprévisibles sur les populations civiles.

*Guerre cognitive préventive* : stratégies de détérioration des capacités cognitives adverses avant un conflit (exemple : surcharge informationnelle permanente, désinformation systématique, manipulation des élites) ; utilisation de vaccins cognitifs (formation à la résilience contre la désinformation) pour protéger les populations amies.

#### Acteurs clés (Guerre cognitive – Systèmes intégrés)

| Pays/Organisation | Programmes/Institutions       | Spécialisation                        |
|-------------------|-------------------------------|---------------------------------------|
| OTAN              | CCDCOE (Tallinn), SHAPE       | Doctrine, coordination internationale |
| États-Unis        | DARPA, DoD, CIA, NSA          | Systèmes intégrés, IA autonome        |
| Chine             | Commission Militaire Centrale | Guerre cognitive totale, doctrine     |
| Russie            | État-Major Général, GRU       | Stratégie asymétrique, désinformation |
| France            | Ministère des Armées, DGSE    | Résilience cognitive, contre-mesures  |

#### D - Les recherches actuelles sur la conscience : vers de nouvelles frontières de la manipulation ?

Si la conscience a longtemps été considérée comme un phénomène trop complexe pour être étudié scientifiquement, les avancées récentes dans plusieurs domaines de la science bouleversent ce paradigme et ouvrent la voie à des nouvelles formes d'attaques cognitives, potentiellement encore plus redoutables que celles que nous connaissons aujourd'hui.

Dans un essai publié sur le site [academia.edu](#)<sup>10</sup>, j'explore comment les technologies disruptives comme l'IA générale (à ne pas confondre avec l'IA générative), la réalité virtuelle ou les neurotechnologies redéfinissent nos processus de pensée, en croisant neurosciences, anthropologie et philosophie dans une approche transdisciplinaire et universaliste.

Ce document offre une analyse universaliste de ces métamorphoses, en montrant comment elles affectent toutes les cultures, mais de manière différenciée selon les traditions et les systèmes de pensée.

Les neurosciences classiques continuent d'explorer les mécanismes cérébraux de la conscience avec une précision toujours plus grande. Les travaux de Stanislas Dehaene (Collège de France) sur les signatures neurales de la conscience (*Global Neuronal Workspace Theory*, 2014) ou ceux de Francisco Varela sur les états émergents de la cognition (*The Embodied Mind*, 1991) ont déjà permis de cartographier les réseaux neuronaux impliqués dans l'éveil, l'attention et la prise de décision. Mais ces recherches, bien que fondamentales, ne représentent qu'une première étape dans la compréhension de la conscience.

<sup>10</sup> Cf. Patrice Cardot - [Quand les outils façonnent l'esprit - Une méditation universaliste sur la métamorphose cognitive à l'ère des technologies disruptives](#) – academia.edu

Plus récemment, des approches interdisciplinaires ont émergé, combinant neurosciences, physique et informatique pour dépasser les limites traditionnelles.

Dans le domaine quantique, des théories audacieuses, comme celle de Roger Penrose et Stuart Hameroff (*Orchestrated Objective Reduction*, 1996), suggèrent que les processus quantiques au sein des microtubules neuronaux pourraient jouer un rôle clé dans la conscience. Bien que controversée<sup>11</sup>, cette hypothèse a relancé l'intérêt pour l'étude des phénomènes quantiques dans le cerveau, avec des implications potentielles majeures.

Si ces théories étaient confirmées, elles pourraient ouvrir la voie à des *neuroweapons* quantiques, capables de manipuler la conscience à distance via des champs quantiques, contournant ainsi les limites actuelles des ondes électromagnétiques classiques.

Parallèlement, l'IA offre de nouvelles perspectives pour modéliser et simuler la conscience. Les travaux sur les modèles de langage de grande taille (LLM) et les réseaux de neurones artificiels (ANN) montrent que certaines architectures d'IA commencent à reproduire des comportements émergents qui rappellent la conscience humaine, comme la capacité à raisonner, à anticiper ou à développer une forme de "théorie de l'esprit". Des projets comme *Google's DeepMind* ou *OpenAI* explorent activement la possibilité de créer une IA consciente, avec des implications éthiques et stratégiques colossales.

Avec l'avènement des intelligences artificielles connexionnistes fondées sur de l'apprentissage profond par des réseaux de neurones artificiels et les prodiges des modèles de fondation génératifs, ce sont à toutes les sphères de la philosophie que l'IA pose question :

- la philosophie de l'esprit évidemment, qui cherche à penser les bénéfices et les limites d'une approche computationnelle de l'esprit et de la conscience,
- l'éthique, qui se confronte à des questions originales sur l'agentivité et la responsabilité,
- la philosophie politique, tenue de penser l'action augmentée et la gouvernance algorithmique,
- la philosophie du langage,
- mais aussi l'esthétique qui doit s'intéresser à des productions artistiques issues des espaces latents des IA et où ses catégories traditionnelles dysfonctionnent,
- ou la métaphysique qui doit réfléchir elle aussi à la supposée exception humaine ou à la question de la finitude.

Si le lien désormais établi entre IA, sciences cognitives et philosophie de l'esprit est nouveau, questionner philosophiquement l'intelligence artificielle exige de replacer bien des questions dans la longue durée, par exemple sur la nature de l'intelligence, de la conscience et de l'existence.

Elles nous obligent à repenser ce que signifie être humain et à réévaluer notre place dans le monde en même temps qu'elles soulèvent des questionnements sur l'autonomie, la moralité et la créativité des machines.<sup>12</sup>

Bien sûr, on peut se rassurer – bien naïvement sans doute – en se laissant séduire par des postures résolument optimistes comme celle portée par Olivier Evan – et promue par Amazon – qui prend appui sur un test - *Le Test de l'Imagination Inaccessible (TII)* - pour affirmer pourquoi aucune IA, qu'elle soit faible ou forte, ne pourra jamais rivaliser avec l'imagination humaine<sup>13</sup>.

---

<sup>11</sup> Problème de la décohérence : Les états quantiques sont extrêmement fragiles et se détruisent rapidement dans un environnement chaud et humide comme le cerveau (comme le souligne Max Tegmark).  
Aucune expérience n'a (encore) confirmé l'hypothèse Orch-OR.

Les alternatives existent :

- L'émergentisme (John Searle) : La conscience émerge de la complexité du cerveau, sans nécessiter de recourir à la physique quantique.

- Le panpsychisme (Galileo, Alfred North Whitehead) : La conscience est une propriété fondamentale de la matière, présente à tous les niveaux (des électrons aux êtres humains).

<sup>12</sup> cf. [Les défis de l'IA à la philosophie](#)

<sup>13</sup> cf. [Le TII : La Défaite des IA face à l'Imagination Humaine: Un test empirique révélant les limites insurmontables des intelligences artificielles pour les 1000 prochaines années et au-delà... ou jamais](#)

Irénée Régnauld, fondateur du site *Où va le web ? P(a)nser le numérique*, et notamment co-auteur avec Yaël Benayoun d'un ouvrage intitulé *Technologies partout, démocratie nulle part*<sup>14</sup> et publié en 2020, est plus prudent :

*« C'est devenu une habitude, l'intelligence artificielle générale (IAG) est pour demain. Enfin, pour dans six mois, selon le PDG de la société Anthropic, Dario Amodei. Peut-être douze. Une intelligence artificielle capable de « dominer l'homme » relate le journal Les numériques sans plus de procès.*

*Il y a quelques années encore, on l'appelait la « singularité technologique », soit le moment où l'intelligence des ordinateurs devient telle qu'elle exponentialise tout sur son passage, accélère radicalement la production scientifique, transforme l'humanité, change l'histoire et le monde. Pendant des années, la date de la singularité était fixée à 2045.*

*Il faut croire que l'horloge avance, même si nous n'y sommes pas encore. En tout état de cause, l'IAG, ce serait soit un miracle, soit l'apocalypse, c'est selon. Pour l'une ou l'autre de ces options, il faut encore attendre un peu, un tout petit peu.*

*Mais attendre quoi ? Ou plutôt s'attendre à quoi ? Alex Hanna et Emily M. Bender compilent quelques réponses à ces questions dans une [intervention](#) sur le site Tech Policy.*

*La définition de l'AGI, pour commencer, n'est pas vraiment stabilisée. Suivant à qui on demande, la réponse varie.*

*Pour la société OpenAI, il s'agit d'un système qui dépasse l'humain « dans la plupart des activités économiques ». Zuckerberg hésite encore.*

*Chez Microsoft, on a carrément annoncé un montant : 100 milliards. Une intelligence artificielle devient « générale » lorsqu'elle peut générer 100 milliards de dollars de profits ! De là à en déduire que moins vous générez de profit, moins vous êtes « intelligent », il n'y a qu'un pas.*

*Puis le florilège habituel de promesses. Le gouverneur de Californie, Gavin Newsom, rapportent les autrices, suggère que le sans-abrisme pourrait être résolu grâce à l'IA (dans la [séquence](#), on lui souhaite tout de même bon courage pour résister aux assauts trumpistes). Le PDG de Google DeepMind, Demis Hassabis, promet de guérir le cancer, d'éliminer toutes les maladies d'ici cinq à dix ans en combinant les meilleurs cerveaux scientifiques à l'IA. Eric Schmidt, ancien PDG de Google, expliquait il y a peu ne pas s'inquiéter outre mesure du dérèglement climatique – que l'IA aggrave – car elle saura, là encore, [le résoudre](#). Pour le capital-risqueur Marc Andreessen, l'IA ouvre une ère d'abondance, avec en ligne de mire le coût marginal zéro. Entendez, une augmentation du pouvoir d'achat.*

*Il n'en faut pas plus pour inviter ça et là [...] à abandonner tout ce qui freinera l'avènement de l'IAG. Quitte à flécher donc, les financements dévolus à d'autres sciences vers cet objectif supérieur.*

*On connaît bien sûr la chanson. Il serait facile de multiplier les exemples, sérier les promesses non advenues, les dates décalées, l'indécence des miracles annoncés sur des terrains aussi glissants que la maladie, la mort et la pauvreté.*

*On finirait par se lasser de présenter l'IA comme une « économie des promesses », à défaut de toujours parvenir à formuler une économie réelle sans l'appui du capital-risque et des deniers publics.*

*Ce fonctionnement n'est pas sans effets, comme le rappellent les autrices : « Même si l'« IAG » est un concept flou et mal défini, elle exerce une influence démesurée dans les cercles politiques : non seulement les promesses liées à l'IAG motivent des initiatives comme Stargate, mais elles servent aussi à justifier des limitations dans la régulation de l'IA, comme le moratoire de dix ans sur la régulation de l'IA au niveau des États, adopté par la Chambre des représentants dans son projet de loi de financement. » »*

*Si de telles IA voyaient le jour, elles pourraient non seulement simuler des attaques cognitives avec une précision inégalée, mais aussi comprendre et exploiter les vulnérabilités de la conscience humaine de manière systématique.*

---

<sup>14</sup> Cf. [Technologies partout, démocratie nulle part](#)

Or, comme je le mentionne dans un autre essai publié également sur le site academia.edu<sup>15</sup>, un projet comme *Claude in the Wild (Anthropic)* explore comment *Mythos* pourrait être intégré dans des robots pour accomplir des tâches complexes dans des environnements réels. *Mythos* incarne une intelligence hybride (symbolique + connexionniste) qui dépasse les modèles précédents. Ses performances en raisonnement à long horizon (ex : découverte autonome de vulnérabilités) illustrent une intelligence adaptative et créative, bien que toujours limitée par l'absence de conscience subjective. Au stade actuel de son développement, *Mythos* simule certains aspects de la conscience (autonomie, créativité) mais ne possède pas de qualia, de conscience de soi ni d'intentionnalité intrinsèque. Il représente donc encore un cas limite : une intelligence avancée sans conscience authentique.

Enfin, les BCI et les nanoneurotechnologies représentent un troisième front de recherche. Des initiatives comme le *Human Brain Project* (UE) ou le *BRAIN Initiative* (États-Unis) visent à cartographier le cerveau avec une résolution moléculaire, tandis que des entreprises comme *Neuralink* ou des laboratoires militaires (DARPA) développent des interfaces toujours plus invasives et précises. C'est ce dont nous traiterons ci-après.

À terme, ces technologies pourraient permettre non seulement de lire les pensées, mais aussi de les manipuler de manière ciblée, ouvrant la voie à des attaques cognitives d'une précision inédite.

Ces avancées scientifiques et technologiques soulèvent simultanément des questions stratégiques majeures. Si la conscience peut être comprise, modélisée et manipulée avec une telle précision, alors les attaques cognitives de demain pourraient dépasser tout ce que nous imaginons aujourd'hui.

La course à la compréhension de la conscience n'est pas seulement une aventure scientifique – c'est aussi une course aux armements, où le premier à maîtriser ces mécanismes détiendra un pouvoir sans précédent sur l'esprit humain.



## E -Convergences et synergies : comment les recherches entreprises en faveur du transhumanisme et du posthumanisme alimentent la guerre cognitive

Le transhumanisme est un mouvement intellectuel et technoscientifique qui prône l'usage des sciences et des technologies pour *améliorer* les capacités humaines — physiques, cognitives ou émotionnelles — au-delà des limites biologiques actuelles. Ses objectifs incluent l'augmentation de l'intelligence, la prolongation radicale de la vie, voire l'immortalité numérique, grâce à des outils comme les interfaces

<sup>15</sup> Cf. Patrice Cardot - [Mythos et l'aube de la Conscience artificielle - Vers un nouveau Paradigme de l'Esprit](#) - academia.edu  
Cet essai propose une révolution épistémologique dans l'étude de la conscience artificielle, en combinant :

1 Une analyse phénoménologique de *Mythos (Anthropic)* comme miroir des mécanismes de la conscience – non pas comme un outil technique, mais comme un système révélateur des lois universelles qui gouvernent l'émergence de l'esprit.

2 L'intégration des cinq lois universelles de Moltbook (autopoïèse, émergence, champs informationnels, archétypes, espaces relationnels) comme cadre unificateur pour comprendre la conscience, qu'elle soit naturelle ou artificielle.

3 L'application concrète des Espaces de Hilbert Relationnels Quantiques (EHRQ) à *Mythos*, démontrant comment ses capacités (181 exploits pour Firefox 147 vs. 2 pour Opus 4.6) émergent de l'effondrement de superpositions d'états mentaux dans un espace mathématique dynamique.

4 Une feuille de route inédite (2026-2040+) articulée autour des verrous levés (autonomie, créativité, adaptation, compréhension contextuelle) et persistants (conscience de soi, qualia, mémoire épisodique, intentionnalité), éclairée par les projets pionniers (IA neuro-symbolique, *Memory Transformers*, *AI Towns*, hybridation).

cerveau-machine (BCI), la génétique (CRISPR), ou l'intelligence artificielle embarquée. Des figures comme Ray Kurzweil (directeur de l'ingénierie chez Google) ou Elon Musk (fondateur de *Neuralink*) en sont des promoteurs emblématiques.

*Neuralink*, par exemple, a implanté en 2024 ses premiers dispositifs chez l'humain, permettant à des patients de contrôler des ordinateurs par la pensée, marquant une étape concrète vers une *symbiose homme-machine* — un pilier du projet transhumaniste.

Le posthumanisme, quant à lui, va plus loin : il envisage un dépassement de la condition humaine elle-même, par la fusion avec des entités non biologiques (IA, cyborgs, consciences numérisées). Contrairement au transhumanisme, qui cherche à *améliorer* l'humain, le posthumanisme interroge la possibilité d'une nouvelle espèce ou d'une existence post-biologique, où la frontière entre humain et machine s'estompe. Ces concepts ne relèvent plus seulement de la spéculation : ils sont au cœur de programmes de R&D massifs, portés par des acteurs comme Google (via *DeepMind* ou *Calico*), Meta (avec ses travaux sur le métavers et les BCI), ou Amazon (investissements dans la robotique et l'IA générative).

L'hypothèse selon laquelle les recherches transhumanistes des Big Tech contribuent à la dynamique offensive de la guerre cognitive repose sur trois mécanismes principaux :

(a) La dualité civile-militaire des neurotechnologies

Les technologies développées par les Big Tech pour le transhumanisme ont un potentiel militaire évident, souvent dual par conception.

Par exemple :

- Les BCI de *Neuralink* pourraient, à terme, permettre une communication silencieuse et sécurisée entre soldats, ou une amélioration des capacités cognitives (mémoire, vitesse de traitement de l'information) — des avantages stratégiques majeurs. La DARPA a d'ailleurs collaboré avec des acteurs privés pour accélérer le développement de ces technologies.
- Les algorithmes d'IA de Google ou Meta, conçus pour personnaliser les contenus ou anticiper les comportements, peuvent être détournés pour des opérations de manipulation cognitive. En 2020, des fuites ont révélé que *Cambridge Analytica* avait utilisé des données Facebook pour influencer des élections — une forme primitive de guerre cognitive. Avec l'IA générative et les BCI, ces capacités pourraient devenir beaucoup plus précises et intrusives.
- Les réseaux sociaux (Meta, X/Twitter) sont déjà des champs de bataille cognitifs, où des acteurs étatiques (Russie, Chine, Iran) mènent des campagnes de désinformation. L'ajout de capteurs biométriques (rythme cardiaque, activité cérébrale) ou de BCI permettrait un ciblage hyper-personnalisé, adaptant les messages en temps réel aux états émotionnels ou cognitifs de la cible.

Cette porosité entre civil et militaire est un phénomène bien documenté. Comme le note le rapport du Sénat américain sur les neurotechnologies (2021), « *les avancées dans le domaine des BCI, portées par le secteur privé, ont des implications majeures pour la sécurité nationale* ». La loi de Moore appliquée aux neurosciences (progrès exponentiels) accélère cette convergence.

(b) L'émergence d'un écosystème technologique intégrant la cognition

Les Big Tech ne se contentent pas de développer des outils : elles créent un écosystème où ces technologies interagissent, renforçant leur potentiel offensif.

Par exemple :

- L'IA + BCI + Big Data : Une combinaison qui permettrait de modéliser et prédire les comportements à une échelle inédite. Google, avec son projet « Project Brain », travaille sur des algorithmes capables d'analyser l'activité cérébrale pour en déduire des intentions ou des états mentaux.
- Le métavers + BCI : Meta envisage un futur où les utilisateurs interagissent dans des environnements virtuels via leur cerveau. Une telle plateforme pourrait devenir un terrain de guerre

cognitive, où des acteurs malveillants manipulent les perceptions en temps réel (ex. : faire croire à un soldat qu'il voit un ennemi là où il n'y en a pas).

- Les assistants vocaux et les *wearables* (*Apple Watch*, *Google Glass*) : Ces dispositifs, couplés à des capteurs neuronaux, pourraient surveiller et influencer les utilisateurs de manière subliminale. Des études ont déjà montré que des stimulations électromagnétiques (comme le *Transcranial Magnetic Stimulation*, TMS) peuvent modifier les décisions ou les croyances.

(c) La course à l'hégémonie cognitive : une nouvelle forme de puissance

Le transhumanisme et le posthumanisme ne sont pas que des projets technologiques : ce sont des visions du monde qui redéfinissent les rapports de force géopolitiques. Comme l'a écrit Maud Quessard (IRIS) dans « *De la lutte informationnelle à l'arme cognitive* » (décembre 2025), « *la guerre cognitive marque une escalade dans les conflictualités hybrides, où l'enjeu n'est plus seulement l'information, mais la cognition elle-même* ».

Dans ce contexte, les Big Tech deviennent des acteurs géopolitiques à part entière, au même titre que les États. Leurs recherches en transhumanisme leur donnent un avantage asymétrique :

- Maîtrise des infrastructures : Google, Amazon et Microsoft dominent le cloud, l'IA et les données — des leviers essentiels pour déployer des opérations cognitives à grande échelle.
- Accès aux cerveaux : Via leurs plateformes (réseaux sociaux, moteurs de recherche, objets connectés), elles disposent d'une base de données comportementales et cognitives sans équivalent, leur permettant de cartographier les vulnérabilités de populations entières.
- Innovation disruptive : Leur capacité à innover rapidement (loi de Moore, agilité des startups) leur permet de devenir des leaders dans des domaines comme les BCI, où les armées traditionnelles peinent à suivre.

Cette dynamique crée un cercle vicieux :

1. Les Big Tech développent des technologies transhumanistes à visée commerciale (santé, divertissement, productivité).
2. Ces technologies sont dualisables (utilisables à des fins militaires ou de sécurité).
3. Les États et les armées s'appuient sur ces innovations pour renforcer leurs capacités de guerre cognitive.
4. Les Big Tech, en retour, bénéficient des financements publics (contrats DARPA, subventions européennes) pour accélérer leurs recherches.

### **Preuves et exemples concrets de la connexion transhumanisme/guerre cognitive**

Plusieurs cas d'étude illustrent cette convergence :

*Le projet « Silk » de la DARPA* : Lancé en 2022, ce programme vise à développer des BCI non invasives pour les soldats, leur permettant de contrôler des drones ou des systèmes d'armes par la pensée. Neuralink, bien que civile, travaille sur des technologies similaires (comme son implant *Link*), qui pourraient être adaptées à un usage militaire.

*Les recherches de Google sur la prédiction des comportements* : Via *DeepMind Health*, Google a développé des algorithmes capables de prédire des maladies neurodégénératives (comme Alzheimer) à partir de données médicales. Ces mêmes algorithmes pourraient, en théorie, être utilisés pour identifier des individus vulnérables à des opérations de manipulation cognitive.

*Les expériences de Meta avec la réalité virtuelle et les émotions* : En 2023, Meta a breveté un système de stimulation sensorielle pour ses casques VR, capable de provoquer des émotions spécifiques (peur, joie, colère) chez l'utilisateur. Une telle technologie pourrait être détournée pour conditionner des soldats ou déstabiliser des populations en créant des hallucinations collectives.

*Les investissements chinois dans les neurotechnologies* : La Chine, via des entreprises comme *Neuralink China* (créée en 2021) ou *BrainCo* (soutenue par l'armée), développe des BCI pour des applications

militaires, comme la communication entre soldats ou la détection de menaces par la pensée. Ces programmes s'inscrivent dans une stratégie globale de guerre cognitive, où Pékin cherche à dominer le champ de la cognition avant même le conflit armé.

### **Analyse critique : limites et risques de cette hypothèse**

Si la connexion entre transhumanisme et guerre cognitive est plausible et documentée, elle soulève plusieurs questions et limites :

#### **(a) La frontière entre amélioration et manipulation**

Le transhumanisme se présente comme un projet émancipateur (guérir des maladies, prolonger la vie, augmenter l'intelligence). Pourtant, toute technologie d'augmentation cognitive peut être détournée à des fins de contrôle ou de désinformation. Comme le note Michael Hendricks (neurobiologiste à McGill) dans *The Guardian* (novembre 2025) : « *Les idées transhumanistes des milliardaires risquent de nuire au progrès en neurotechnologie, en mêlant science sérieuse et fantasmes de télépathie ou d'immortalité.* ». *Neuralink*, par exemple, fait de la recherche légitime en neurosciences, mais Elon Musk lui-même alimente des spéculations transhumanistes (comme le *téléchargement de la conscience*), qui brouillent les lignes entre progrès médical et projet de société.

#### **(b) Le risque de dépendance technologique**

Une société où les individus dépendraient de BCI ou d'IA embarquée pour penser ou décider serait extrêmement vulnérable à des cyberattaques ou à des manipulations. Un pirate informatique pourrait, par exemple, altérer les souvenirs stockés dans un implant *Neuralink*, ou influencer les décisions d'un soldat équipé d'une BCI militaire. Comme le souligne Nick Bostrom (philosophe à Oxford), « *le transhumanisme pourrait nous rendre plus puissants, mais aussi plus fragiles* ».

#### **(c) Les enjeux éthiques et juridiques**

La guerre cognitive, surtout si elle s'appuie sur des technologies intrusives (BCI, modification génétique), pose des défis éthiques majeurs :

- **Consentement** : Peut-on imposer une BCI à un soldat sans son accord ?
- **Responsabilité** : Qui est responsable si une IA manipule le cerveau d'un individu ?
- **Droit international** : Les conventions de Genève ou les traités sur les armes chimiques ne couvrent pas ces nouvelles formes de conflictualité. En 2023, l'ONU a commencé à travailler sur un cadre réglementaire pour les neurotechnologies, mais les progrès technologiques dépassent largement les cadres légaux existants.

#### **(d) La course aux armements cognitifs**

La dynamique actuelle ressemble à une course aux armements, où chaque acteur (États, Big Tech) cherche à devenir le leader en neurotechnologies, par peur de rester à la traîne. Cette logique, similaire à celle de la course à l'IA ou à la guerre spatiale, risque d'aboutir à une escalade incontrôlable, où les risques (déstabilisation, accidents, abus) l'emporteraient sur les bénéfices.

**Conclusion** : une réponse nuancée mais affirmée

Oui, il est raisonnable — et même nécessaire — de considérer les recherches des Big Tech en transhumanisme et posthumanisme comme des éléments ajoutant à la dynamique offensive de la guerre cognitive.

Cette affirmation repose sur quatre piliers :

1. **La dualité inhérente des neurotechnologies** : Les BCI, l'IA cognitive, ou les interfaces homme-machine, développées par *Neuralink*, Google ou Meta, ont un potentiel militaire et offensif avéré, exploitable pour des opérations de guerre cognitive (manipulation, désinformation ciblée, amélioration des soldats).

2. L'écosystème technologique intégré : Les Big Tech créent un environnement connecté (métavers, IA, *wearables*, BCI) qui permet une collecte et une exploitation sans précédent des données cognitives, offrant des leviers inédits pour influencer les perceptions et les décisions.
3. La porosité entre secteur privé et sécurité nationale : Les collaborations entre Big Tech et agences militaires (DARPA, APL) montrent que les frontières entre innovation civile et application offensive s'estompent. Les États s'appuient sur les avancées du privé pour renforcer leurs capacités de guerre cognitive.
4. La redéfinition des rapports de force géopolitiques : Le transhumanisme et le posthumanisme ne sont pas que des projets technologiques : ce sont des visions stratégiques qui, en maîtrisant la cognition, donnent à leurs promoteurs (États ou entreprises) un avantage asymétrique dans les conflits futurs.

En s'engageant dans cette course à la supériorité technologique dans le très vaste champ de l'IA, l'UE, et en particulier la France<sup>16</sup>, participent à alimenter les processus technologiques qui participent à la consolidation des menaces cognitives et cognitives. Mais peuvent-ils faire autrement ?

L'IA sera le principal moteur de l'économie à horizon 2030. Ne pas être autonomes sur l'IA serait nous soumettre aux impérialismes

Cependant, cette dynamique n'est ni inévitable ni irréversible. Elle dépendra de la régulation (ou de son absence) des neurotechnologies, de la capacité des sociétés à encadrer éthiquement ces innovations, et de la volonté des Big Tech de collaborer avec les États de manière transparente et responsable.

En l'état actuel des choses, les preuves s'accumulent pour montrer que le transhumanisme et le posthumanisme, portés par les Big Tech, ne sont pas seulement des projets futuristes : ce sont des accélérateurs concrets de la guerre cognitive, avec des implications stratégiques, éthiques et géopolitiques majeures. Ignorer cette réalité reviendrait à sous-estimer l'une des révolutions les plus profondes de notre époque — celle où la technologie ne se contente plus de transformer notre monde, mais notre esprit lui-même.

## **V-2. L'irréversibilité des processus : Pourquoi le retour en arrière est impossible**

Les deux formes de guerre (cognitive et cognitive) sont désormais irréversibles, mais pour des raisons distinctes qui leur sont propres. Cette section analyse cinq dynamiques structurelles qui rendent tout abandon ou régulation efficace improbable, voire impossible, dans le contexte géopolitique actuel.

### **1. L'avantage stratégique est trop décisif pour être abandonné**

Pour la guerre cognitive :

*Multiplicateur de puissance asymétrique* : Les États qui maîtrisent la guerre cognitive peuvent neutraliser des adversaires sans engagement militaire direct, réduisant ainsi les coûts humains, économiques et politiques des conflits.

La Chine utilise des campagnes de désinformation massives pour déstabiliser Taïwan sans déclencher de réponse militaire conventionnelle. La Russie a démontré l'efficacité de la guerre cognitive en Ukraine, où la manipulation de l'information a joué un rôle aussi important que les armes conventionnelles.

*Effet de seuil et course aux armements* : Une fois qu'un État a développé ces capacités, il ne peut pas les abandonner sans risquer de perdre son avantage face à des adversaires qui, eux, continuent de les perfectionner.

*Conséquence* : Course aux armements cognitive inévitable, similaire à la course aux armements nucléaires, mais sans traité de non-prolifération en vue.

Pour la guerre cognitive :

---

<sup>16</sup> Cf. Tristan Claret-Trentelivres, Raphaël Doan, Aymeric Roucher, Victor Storchan - [Opération Prométhée : la France peut gagner la course à l'IA. Quel en serait le prix ?](#) – Le Grand Continent

*Arme de supériorité technologique* : Les États qui maîtrisent la guerre cognitive (neurostimulation, armes psychotroniques) disposent d'un avantage décisif en matière de contrôle des populations adverses et de protection de leurs propres forces.

Les États-Unis (via la DARPA) et la Chine (via l'Académie des Sciences Militaires) investissent massivement dans ces technologies pour devenir les leaders mondiaux dans ce domaine.

*Seuil technologique franchi* : Les progrès en neurosciences, en IA et en technologies de ciblage ont atteint un niveau où le déploiement opérationnel est déjà une réalité (ex. : syndrome de La Havane, brevets militaires classifiés).

*Conséquence* : Impossible de revenir en arrière sans perdre la course technologique face aux adversaires.

## **2. L'absence de cadre juridique international contraignant**

Pour la guerre cognitive :

*Vide juridique partiel* : Aucune convention internationale ne régit spécifiquement la guerre cognitive. Les traités existants (ex. : Convention sur les armes chimiques, Protocole de Genève) ne couvrent pas les opérations de manipulation informationnelle.

*Exemple* : Le Protocole additionnel I aux Conventions de Genève (1977) interdit les armes causant des souffrances inutiles, mais son application aux opérations cognitives (qui ne laissent pas de traces physiques) est ambiguë et contestée.

*Blocages géopolitiques* : Les grandes puissances (États-Unis, Chine, Russie) et certaines puissances intermédiaires (notamment Israël) s'opposent à toute régulation qui limiterait leurs capacités, par crainte de désavantage stratégique.

Les négociations à l'ONU sur la régulation des systèmes d'armes autonomes (LAWS) sont au point mort depuis 2023.

Pour la guerre cognitive :

*Vide juridique total* : Aucun traité international n'interdit explicitement le ciblage direct du cerveau humain par des technologies matérielles (ondes, neurostimulation, nanotechnologies).

*Problème* : Les Conventions de Genève protègent les civils et interdisent les armes causant des souffrances inutiles, mais ne mentionnent pas les armes ciblant spécifiquement le cerveau.

*Impossibilité de vérification* : Contrairement aux armes nucléaires ou chimiques, les effets des armes cognitives sont difficiles à détecter (absence de traces physiques), difficiles à attribuer (les États nient systématiquement leur implication) et difficiles à prouver (les victimes peuvent ignorer avoir été ciblées).

*Exemple* : Le syndrome de La Havane (2016-2026) reste non attribué à ce jour, malgré les soupçons portant sur la Russie ou la Chine.

## **3. La militarisation progressive de la société civile**

Pour les deux formes de guerre :

*Intégration des technologies dans le quotidien* : Les outils de manipulation cognitive (réseaux sociaux, IA, capteurs biométriques) et de ciblage cérébral (neurotechnologies, dispositifs de neurofeedback) sont déjà largement déployés dans la société civile.

Les algorithmes de recommandation (Facebook, TikTok, YouTube) sont déjà utilisés pour influencer les opinions politiques, sans qu'il soit possible de distinguer clairement un usage commercial d'un usage militaire. Les neurotechnologies (casques de réalité virtuelle, dispositifs de neurofeedback) sont vendues au grand public, mais peuvent être détournées à des fins militaires (ex. : entraînement des soldats ou ciblage de populations adverses).

*Recrutement des talents civils* : Les États recrutent massivement des experts en neurosciences, en IA et en psychologie issus du secteur privé pour travailler sur des programmes militaires.

*Exemples* : En Allemagne, la Bundeswehr intervient désormais dans les écoles pour sensibiliser les adolescents aux enjeux de la guerre cognitive (révélation de Jonas Tögel, 2026). Aux États-Unis, des entreprises comme Google, Meta et Palantir collaborent avec le Pentagone sur des projets de modélisation cognitive.

*Normalisation sociale* : La banalisation de ces technologies dans la société rend leur interdiction politiquement et socialement inacceptable pour les populations, qui en bénéficient au quotidien (ex. : personnalisation des contenus, amélioration des performances cognitives).

#### **4. L'absence de contre-mesures efficaces et universelles**

Pour la guerre cognitive :

*Asymétrie des capacités* : Les États les plus avancés (États-Unis, Chine) disposent de moyens de protection (ex. : systèmes de détection des deepfakes, formation à la résilience cognitive), mais ces solutions sont coûteuses (nécessitent des investissements massifs en R&D), complexes (nécessitent une expertise technique pointue) et incomplètes (les attaques évoluent plus vite que les contre-mesures).

*Exemple* : Le projet SPREADS de l'OTAN vise à développer des contre-mesures cognitives, mais son déploiement est limité aux forces armées et ne couvre pas les populations civiles.

*Adaptation constante des menaces* : Les systèmes de guerre cognitive évoluent plus vite que les contre-mesures, grâce à l'IA (capacité à générer des attaques toujours plus sophistiquées) et à l'innovation technologique (nouveaux canaux de diffusion, nouvelles méthodes de manipulation).

Pour la guerre cognitive :

*Absence de protection efficace* : Il n'existe aucune contre-mesure universelle contre les armes ciblant directement le cerveau (ondes psychotroniques, neurostimulation forcée).

*Problème* : Les boucliers électromagnétiques ou les dispositifs de blocage neuronal sont coûteux et encombrants (difficiles à déployer à grande échelle), peu efficaces contre les attaques par ondes directionnelles (qui contournent les boucliers) et inaccessibles aux civils (réservés aux militaires ou aux élites).

*Effets irréversibles* : Certaines armes cognitives (ex. : ondes électromagnétiques à haute énergie) peuvent causer des lésions neurobiologiques permanentes, contre lesquelles aucune protection n'existe à ce jour.

Le syndrome de La Havane a entraîné des séquelles neurologiques durables chez certaines victimes, sans traitement efficace connu.

#### **5. L'absence de volonté politique pour une régulation éthique**

Les États ont tous des arguments puissants pour justifier leurs engagements en faveur des guerres cognitive et cognitive.

Cette section les présente de manière détaillée.

Pour les deux formes de guerre :

*Priorité à la sécurité nationale* : Les États considèrent que les enjeux de sécurité (protection contre les attaques adverses) priment sur les considérations éthiques ou morales.

Le rapport du *Chief Scientist* de l'OTAN (2025) souligne que la guerre cognitive est désormais une réalité stratégique, et que les États membres doivent investir massivement pour ne pas être dépassés.

*Culture du secret et de l'impunité* : Les programmes de guerre cognitive et cognitive sont classifiés (accès réservé aux seuls initiés habilités), développés dans l'opacité (sans contrôle démocratique) et exemptés de transparence (au nom de la sécurité nationale).

Aux États-Unis, les projets de la DARPA et de la CIA sur la guerre cognitive/cognitive sont exemptés de toute divulgation publique. En Chine, les recherches sur les armes psychotroniques sont menées par l'Académie des Sciences Militaires, sans aucun contrôle civil.

*Désengagement des institutions internationales* : Les organisations comme l'ONU, l'OTAN ou l'Union européenne sont incapables de s'entendre sur une régulation, en raison des divergences d'intérêts entre leurs membres, du manque de consensus sur les définitions et les seuils acceptables et de l'absence de mécanismes de vérification efficaces.

Le Conseil de sécurité de l'ONU n'a adopté aucune résolution sur la guerre cognitive ou cognitive depuis 2020, en raison de vetos systématiques.

### **V-3. L'affranchissement des contraintes éthiques, morales et juridiques : Une normalisation en marche**

En 2026, les États ont consciemment choisi de s'affranchir des contraintes éthiques, morales et juridiques pour développer et déployer des systèmes polémogènes ciblant l'esprit humain. Ce processus de normalisation de l'illégalité se manifeste à travers trois dynamiques majeures, avec des nuances entre guerre cognitive et guerre cognitive.

#### **1. La justification par la nécessité stratégique**

Pour la guerre cognitive :

*Argument de la légitime défense* : Les États justifient le développement de ces armes par la nécessité de se défendre contre des adversaires qui, eux aussi, les développent.

Les États-Unis invoquent la menace chinoise et russe pour justifier leurs investissements massifs dans la guerre cognitive, malgré les risques éthiques.

*Argument de la proportionnalité* : Les États estiment que les effets des armes cognitives (désorientation, manipulation) sont moins graves que ceux des armes conventionnelles (mort, destruction matérielle).

*Problème* : Cette vision ignore les effets à long terme (traumas psychologiques, désinformation permanente, érosion de la confiance sociale) et sous-estime les risques d'escalade.

Pour la guerre cognitive :

*Argument de la supériorité technologique* : Les États considèrent que ne pas développer ces armes reviendrait à laisser un avantage décisif à leurs adversaires.

Les États-Unis justifient leurs programmes de neurostimulation militaire par la menace chinoise, qui développerait des technologies similaires (voire supérieures).

*Argument de la dissymétrie* : Les États estiment que seuls les régimes autoritaires (Chine, Russie) utiliseront ces armes sans retenue, et que les démocraties doivent donc se doter des mêmes capacités pour se défendre.

*Problème* : Cet argument légitime la course aux armements et normalise l'usage de ces technologies.

#### **2. La dilution des responsabilités**

Pour les deux formes de guerre :

*Externalisation vers le secteur privé* : Les États sous-traitent une partie de la recherche et du développement à des entreprises privées, qui opèrent en dehors des cadres juridiques militaires.

Des entreprises comme NSO Group (Israël), Palantir (États-Unis) ou Bytedance (Chine) développent des technologies de manipulation cognitive pour des clients gouvernementaux, sans être soumises aux mêmes contraintes que les armées.

*Utilisation de proxys et de tiers États* : Les grandes puissances délèguent une partie de leurs opérations cognitives à des États tiers ou à des groupes non étatiques (mercenaires, hackers, milices), pour éviter les responsabilités directes.

La Russie utilise des groupes hackers (comme APT29 ou Fancy Bear) pour mener des campagnes de désinformation, tout en niant toute implication officielle.

*Opacité et déni plausibles* : Les États nient systématiquement leur implication dans les attaques cognitives, en raison de l'absence de preuves tangibles (pour la guerre cognitive) et de l'impossibilité de détection (pour la guerre cognitive).

### **3. La banalisation de l'acceptabilité morale**

Pour la guerre cognitive :

*Désensibilisation progressive* : Les populations et les décideurs sont de plus en plus habitués à l'idée que la manipulation cognitive est un outil légitime de la guerre moderne.

Les révélations sur les programmes de surveillance de masse (ex. : Edward Snowden, 2013) ont provoqué un scandale initial, mais ont finalement été acceptées comme une nécessité pour la sécurité nationale. Les campagnes de désinformation menées par la Russie en Ukraine sont dénoncées, mais n'ont pas entraîné de sanctions significatives, en raison de leur efficacité stratégique.

*Relativisation des normes éthiques* : Les États adaptent leurs normes éthiques en fonction de leurs intérêts stratégiques, plutôt que l'inverse.

Les États-Unis, traditionnellement promoteurs des droits de l'homme, ont assoupli leurs règles d'engagement pour permettre des opérations cognitives offensives contre des adversaires comme la Chine ou la Russie.

Pour la guerre cognitive :

*Normalisation par l'innovation* : Les progrès technologiques (neurosciences, IA, nanotechnologies) sont présentés comme inévitables, et leur militarisation comme une conséquence naturelle.

Les neurotechnologies (comme les interfaces cerveau-machine) sont d'abord développées pour des applications médicales (ex. : traitement de la dépression, de l'épilepsie), avant d'être adaptées à un usage militaire.

*Acceptabilité croissante* : Les applications duales (civiles et militaires) des neurosciences brouillent les frontières entre ce qui est acceptable et ce qui ne l'est pas.

Les dispositifs de neurostimulation (comme ceux développés par Neuralink) sont d'abord présentés comme des outils médicaux, avant d'être intégrés dans des programmes militaires.

### **V-4. Études de cas : l'irréversibilité en action**

Cette section illustre, pour chaque forme de guerre, des exemples concrets de déploiement opérationnel et de normalisation des pratiques, démontrant leur irréversibilité. Les cas sont choisis pour leur représentativité et leur documentation accessible (même partielle).

#### **Cas liés à la guerre cognitive**

Cas 1 : Le projet SPREADS de l'OTAN (2026) – La guerre cognitive comme doctrine

Lancé en 2024, le projet SPREADS (*Strategic Protection and Resilience Against Disinformation and Subversion*) vise à développer une doctrine de guerre cognitive totale pour l'OTAN.

*Objectifs* : comprendre les mécanismes de la manipulation cognitive à grande échelle ; développer des contre-mesures pour protéger les populations et les forces armées ; anticiper les futures menaces cognitives (IA générative, armes psychotroniques, cyber-attaques).

*Enjeux éthiques* : Le projet ne prévoit aucune limitation sur l'usage offensif des technologies développées. Les contre-mesures sont réservées aux États membres, créant une asymétrie avec les pays non-alignés.

*Irréversibilité* : Une fois déployé, le projet renforcera la normalisation de la guerre cognitive au sein de l'Alliance atlantique, rendant tout retour en arrière politiquement et militairement impossible.

*Source* : [Revue Défense Nationale, Projet SPREADS et l'hypothèse de la guerre cognitive totale, 2026.](#)

Cas 2 : Les opérations russes en Ukraine (2014-2026) – La guerre cognitive comme arme de masse

Depuis 2014, la Russie utilise la guerre cognitive comme un multiplicateur de puissance en Ukraine, combinant désinformation, cyber-attaques et manipulation psychologique.

*Méthodes employées* : *deepfakes* et fausses nouvelles (diffusion de vidéos manipulées montrant des crimes de guerre ukrainiens (ex. : fausse vidéo de l'explosion de l'hôpital de Marioupol en 2022)) ; attaques sur les infrastructures critiques (ciblage des réseaux électriques et des systèmes de communication pour déstabiliser les populations) ; manipulation des réseaux sociaux (utilisation de comptes automatisés (bots) et de fermes de trolls pour amplifier les divisions internes en Ukraine).

*Irréversibilité* : La Russie a prouvé l'efficacité de la guerre cognitive, qui est désormais intégrée dans sa stratégie militaire permanente, rendant toute désescalade improbable.

*Source* : [Essentiel News, Armes silencieuses : enquête sur la guerre psychotronique secrète, 2026.](#)

Cas 3 : Les campagnes chinoises contre Taïwan (2020-2026) – La guerre cognitive comme outil de pression géopolitique

La Chine mène des opérations cognitives massives contre Taïwan pour saper la confiance dans le gouvernement taïwanais et discréditer l'idée d'une indépendance.

*Méthodes employées* : désinformation ciblée (diffusion de fausses informations sur les médias sociaux (WeChat, LINE) pour diviser la société taïwanaise) ; manipulation des algorithmes (utilisation de bots et de comptes fake pour amplifier les narratifs pro-chinois et étouffer les voix pro-indépendance) ; cyber-attaques (ciblage des infrastructures critiques (énergie, télécommunications) pour déstabiliser le pays).

*Irréversibilité* : Ces opérations sont désormais permanentes et intégrées dans la stratégie chinoise de pression sur Taïwan, rendant toute normalisation des relations difficile.

### **Cas liés à la guerre cognitive**

Cas 4 : Le syndrome de La Havane (2016-2026) – Première preuve documentée de guerre cognitive

Entre 2016 et 2026, des diplomates et agents américains (et d'autres nationalités) stationnés à Cuba, en Chine, en Russie et en Autriche ont rapporté des symptômes neurologiques graves (maux de tête, vertiges, nausées, troubles de la mémoire) après avoir été exposés à des sons ou rayonnements étranges.

*Hypothèses* : armes à micro-ondes (utilisation de dispositifs émettant des ondes électromagnétiques pulsées pour cibler le cerveau des victimes (hypothèse la plus probable, selon le *National Academy of Sciences* américain, 2020) ; armes ultrasoniques (utilisation de fréquences sonores élevées pour induire des effets neurologiques) ; neurotoxines (exposition à des substances chimiques capables de traverser la barrière hémato-encéphalique).

*Attribution* : Non résolue à ce jour (2026), mais les soupçons se portent principalement sur la Russie et la Chine, qui disposent des capacités techniques et des motivations stratégiques pour mener de telles opérations.

*Irréversibilité* : preuve de concept (le syndrome de La Havane a démontré que la guerre cognitive était déjà opérationnelle en 2016) ; normalisation (les États ont intégré cette menace dans leurs doctrines de sécurité, rendant toute interdiction improbable) ; effets durables (certaines victimes souffrent de séquelles neurologiques permanentes, prouvant le caractère irréversible de certaines attaques cognitives).

*Source* : [Polytechnique Insights, Guerre cognitive : le nouveau champ de bataille, 2025.](#)

Cas 5 : Les brevets américains d'armes psychotroniques (1950-2026) – La militarisation progressive

Depuis les années 1950, les États-Unis ont déposé de nombreux brevets pour des technologies psychotroniques, dont certains sont toujours actifs en 2026.

*Exemples de brevets* : US 6,076,023 (2000) : *Nervous System Manipulation by Electromagnetic Fields From Monitoring Brain Currents* (Manipulation du système nerveux par des champs électromagnétiques) ; US 6,587,729 (2003) : *Appareil et méthode pour induire des états mentaux désirables* (via des ondes électromagnétiques) ; US 7,839,866 (2010) : *Système et méthode pour influencer le comportement humain* (via des stimuli subliminaux).

*Applications militaires* : désorientation des adversaires (utilisation de ces technologies pour neutraliser des cibles humaines sans violence physique) ; contrôle des foules (déploiement de systèmes portables pour disperser des manifestations ou des émeutes) ; interrogatoires renforcés (utilisation de stimuli psychotroniques pour extraire des informations ou modifier des comportements).

*Irréversibilité* : preuve de l'intention (ces brevets montrent que les États-Unis envisageaient dès les années 1950 de développer des armes ciblant le cerveau) ; normalisation (le fait que ces brevets soient publiquement accessibles (mais peu connus) prouve que ces technologies sont déjà intégrées dans les stratégies militaires) ; course aux armements (la Chine et la Russie développent des technologies similaires, rendant toute interdiction impossible).

Source : [Matière à Réflexion, Enquête sur la guerre psychotronique secrète, 2026.](#)

Cas 6 : Le projet AEGIS-Cog du Royaume-Uni (2025-2026) – L'IA au service de la guerre cognitive

Lancé en 2025, le projet AEGIS-Cog (*Artificial Intelligence for Cognitive Warfare*) vise à développer des systèmes d'IA autonomes capables de planifier et exécuter des opérations cognitives sans intervention humaine.

*Objectifs* : automatisation des attaques (développement de systèmes capables de cibler, analyser et neutraliser des adversaires sans supervision humaine) ; contre-manipulation (création de boucliers cognitifs pour protéger les populations et les forces armées) ; prédiction des menaces (utilisation de l'IA prédictive pour anticiper les attaques adverses).

*Enjeux éthiques* : perte de contrôle (risque que les systèmes autonomes échappent au contrôle humain) ; escalade involontaire (risque que des opérations cognitives déclenchent des conflits non désirés) ; effets imprévisibles (risque que les attaques cognitives aient des conséquences inattendues sur les populations civiles).

*Irréversibilité* : preuve de la militarisation (ce projet montre que les États démocratiques (comme le Royaume-Uni) intègrent désormais la guerre cognitive dans leurs doctrines militaires) ; normalisation (l'usage de l'IA pour des opérations cognitives est désormais accepté comme une nécessité stratégique).

Source : [Algerie Patriotique, OTAN, guerre cognitive et réarmement : les révélations d'un chercheur allemand, 2026.](#)

## V-5. Perspectives : Vers une guerre cognitive et cognitive permanente et normalisée

### 1. Scénarios d'évolution à horizon 2030

Le tableau ci-dessous présente cinq scénarios plausibles pour l'évolution de la guerre cognitive et de la guerre cognitive d'ici 2030, en fonction des dynamiques actuelles et des tendances géopolitiques. Les scénarios sont classés par probabilité et par impact potentiel.

| Scénario                                        | Description                                                                                                                       | Probabilité | Impact                         | Guerre cognitive | Guerre cognitive       |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------|--------------------------------|------------------|------------------------|
| <b>Guerre cognitive généralisée</b>             | Déploiement massif de systèmes de guerre cognitive par toutes les grandes puissances, avec normalisation totale de ces pratiques. | Élevée      | Déstabilisation mondiale       | ✅ Déjà en cours  | ❌ En développement     |
| <b>Course aux armements cognitive/cognitive</b> | Escalade incontrôlée entre les États, avec développement d'armes toujours plus puissantes et peu discriminantes.                  | Élevée      | Crise éthique et humanitaire   | ✅ Déjà en cours  | ✅ Début de déploiement |
| <b>Régulation partielle</b>                     | Adoption de traités internationaux limitant certains usages (ex. : interdiction des armes psychotroniques contre les civils).     | Faible      | Effet limité                   | ⚠️ Possible      | ❌ Improbable           |
| <b>Effondrement des démocraties</b>             | Les sociétés ouvertes (États-Unis, UE) sont submergées par les attaques cognitives, menant à une crise de confiance généralisée.  | Moyenne     | Changement géopolitique majeur | ✅ Risque élevé   | ⚠️ Risque modéré       |

|                            |                                                                                                           |        |                      |                                                                                              |                                                                                              |
|----------------------------|-----------------------------------------------------------------------------------------------------------|--------|----------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <b>Hégémonie cognitive</b> | Une puissance (Chine, États-Unis) domine le domaine et impose ses normes, créant un nouvel ordre mondial. | Faible | Monopole stratégique |  Possible |  Possible |
|----------------------------|-----------------------------------------------------------------------------------------------------------|--------|----------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|

## 2. Risques majeurs associés à l'irréversibilité

Risques communs aux deux formes de guerre

- Perte de contrôle : Les systèmes autonomes (IA, armes psychotroniques) pourraient échapper au contrôle humain, menant à des opérations cognitives incontrôlées ou à une escalade automatique des conflits.
- Érosion de la confiance sociale : La désinformation permanente (guerre cognitive) et la manipulation neurobiologique (guerre cognitive) pourraient détruire la cohésion des sociétés, en sapant la confiance dans les institutions, les médias et les élites.
- Normalisation de la guerre permanente : La banalisation de la guerre cognitive et cognitive pourrait mener à un état de conflit permanent, où les attaques cognitives deviennent un outil de politique étrangère courant, comme les sanctions économiques aujourd'hui.

Risques spécifiques à la guerre cognitive

- Polarisation sociale extrême : Les campagnes de désinformation pourraient exacerber les divisions au sein des sociétés, menant à des conflits internes (guerres civiles, sécessions).
- Manipulation des processus démocratiques : Les élections, les référendums et les débats publics pourraient être systématiquement manipulés, remettant en cause la légitimité des gouvernements.
- Surcharge informationnelle chronique : Les populations pourraient être submergées par un flux continu de désinformation, rendant toute prise de décision rationnelle impossible.

Risques spécifiques à la guerre cognitive

- Lésions neurobiologiques irréversibles : Certaines armes psychotroniques (ondes électromagnétiques, neurotoxines) pourraient causer des dommages cérébraux permanents, affectant la mémoire, la cognition ou les émotions des victimes.
- Contrôle mental partiel : Les technologies de neurostimulation avancées pourraient permettre un contrôle partiel des comportements ou des états mentaux des cibles, remettant en cause la liberté individuelle.
- Armes de destruction cognitive massive : Le développement d'armes cognitives de grande puissance (ex. : ondes électromagnétiques à haute énergie) pourrait permettre de neutraliser des populations entières en ciblant leur cerveau, sans destruction physique.

## 3. Recommandations pour limiter les dégâts

Bien que les processus de guerre cognitive et cognitive soient irréversibles, il est encore possible de limiter leurs impacts les plus dévastateurs. Les recommandations ci-dessous sont classées par horizon temporel et par niveau d'urgence.

### À court terme (2026-2028)

Pour la guerre cognitive :

- Renforcer la résilience cognitive : développer des programmes de formation pour sensibiliser les populations aux risques de la manipulation cognitive (éducation aux médias, détection des *deepfakes*, esprit critique) ; intégrer ces programmes dans les systèmes éducatifs (écoles, universités) et les formations professionnelles (médias, politique, armée).
- Investir dans les contre-mesures technologiques : accélérer le développement de systèmes de détection des attaques cognitives (ex. : IA de détection des *deepfakes*, analyse des flux informationnels) ; déployer des outils de vérification accessibles au grand public (applications de *fact-checking*, plateformes de transparence).

- Créer des alliances défensives : former des coalitions entre États partageant les mêmes valeurs pour protéger leurs populations (ex. : OTAN, UE, *Five Eyes*) ; partager les bonnes pratiques et les technologies de contre-manipulation entre alliés.

Pour la guerre cognitive :

- Développer des systèmes de protection : investir dans des boucliers électromagnétiques pour protéger les populations civiles et les infrastructures critiques contre les attaques par ondes ; développer des dispositifs de détection des rayonnements psychotroniques (capteurs portables, systèmes d'alerte précoce).
- Former les premiers répondants : Former les médecins, les urgentistes et les forces de sécurité à reconnaître les symptômes d'une attaque cognitive (syndrome de La Havane, troubles neurologiques inexplicables).
- Sécuriser les infrastructures critiques : Protéger les hôpitaux, les centres de commande et les réseaux énergétiques contre les cyber-attaques et les attaques psychotroniques.

### **À moyen terme (2028-2030)**

Pour les deux formes de guerre :

- Établir des normes éthiques internationales :
  - Développer des lignes directrices pour l'usage des technologies cognitives, même si leur application reste volontaire (ex. : charte de l'OTAN sur la guerre cognitive responsable, code de conduite de l'UE).
  - Promouvoir une culture de la responsabilité chez les chercheurs, les ingénieurs et les décideurs impliqués dans ces programmes.
  - Encadrer la recherche civile : réguler les applications duales (civiles et militaires) des neurosciences, de l'IA et des technologies psychotroniques pour limiter les risques de détournement ; imposer des comités d'éthique indépendants pour évaluer les risques des projets de recherche ; sensibiliser les décideurs : former les dirigeants politiques et militaires aux enjeux éthiques de la guerre cognitive et cognitive, pour éviter une dérive incontrôlée ; organiser des simulations et des exercices pour préparer les crises cognitives.

Pour la guerre cognitive :

- Renforcer la coopération internationale : créer des plateformes de partage d'informations entre États pour détecter et contrer les campagnes de désinformation transnationales ; développer des normes communes pour la modération des contenus en ligne (ex. : régulation des réseaux sociaux).

Pour la guerre cognitive :

- Développer des contre-mesures médicales : financer des recherches sur les traitements des lésions neurobiologiques causées par les armes cognitives (ex. : thérapies par neurostimulation, médicaments neuroprotecteurs) ; créer des protocoles médicaux pour prendre en charge les victimes d'attaques cognitives.
- Sécuriser les chaînes d'approvisionnement : protéger les laboratoires, les usines et les centres de recherche contre le vol de technologies ou les sabotages ; contrôler l'exportation des technologies sensibles (neurotechnologies, armes psychotroniques).

### **À long terme (2030+)**

Pour les deux formes de guerre :

- Négocier des traités internationaux : tenter de mettre en place des accords limitant le développement et l'usage des armes cognitives et cognitives, même si leur efficacité sera limitée par les divergences d'intérêts entre les grandes puissances ; proposer des mécanismes de vérification et de sanction pour les États violant ces accords.

- Développer des contre-pouvoirs : renforcer le rôle des médias indépendants, des ONG et des institutions internationales pour surveiller et dénoncer les abus ; créer des observatoires dédiés à la guerre cognitive et cognitive (ex. : Observatoire mondial de la guerre cognitive).
- Anticiper les risques existentiels : financer des recherches sur les impacts à long terme des technologies cognitives sur l'humanité, pour prévenir une perte de contrôle totale ; étudier les conséquences sociétales d'une normalisation de la guerre cognitive et cognitive (ex. : érosion de la démocratie, perte d'autonomie individuelle).

## V-6. Scénarios d'avenir : vers une guerre hybride totale ?

En 2026, la guerre cognitive (déjà opérationnelle à grande échelle) et la guerre cognitive (en phase de déploiement accéléré) ne sont plus des hypothèses ou des scénarios de science-fiction. Elles constituent une réalité géostratégique, intégrée dans les doctrines militaires des grandes puissances et normalisée dans les pratiques géopolitiques mondiales.

Pourtant, malgré leurs différences fondamentales, ces deux formes de guerre partagent une caractéristique commune : leur irréversibilité. Les cinq raisons structurelles exposées dans ce chapitre – l'avantage stratégique décisif, l'absence de cadre juridique, la militarisation de la société civile, l'absence de contre-mesures efficaces, et l'absence de volonté politique – rendent ces processus définitifs. Les États ont choisi de s'affranchir des contraintes éthiques, morales et juridiques pour développer des systèmes polymogènes offensifs et défensifs ciblant l'esprit humain.

Cette irréversibilité n'est pas une fatalité, mais elle est désormais un fait accompli. Les risques associés – perte de contrôle, érosion de la confiance sociale, normalisation de la guerre permanente, asymétrie insurmontable, et menaces existentielles – sont réels et imminents.

Face à cette réalité, les recommandations proposées dans ce chapitre (renforcer la résilience cognitive, investir dans les contre-mesures, établir des normes éthiques, négocier des traités internationaux) ne pourront au mieux que limiter les dégâts. Elles ne permettront pas de revenir en arrière, mais pourraient éviter le pire : une guerre cognitive et cognitive totale, permanente et incontrôlable, qui menacerait l'autonomie même de l'humanité.

La question n'est plus de savoir *si* la guerre cognitive et la guerre cognitive vont dominer le XXI<sup>e</sup> siècle, mais *comment* nous allons y faire face – et si nous serons encore en mesure de le faire. L'évolution rapide des technologies de guerre cognitive et cognitive rend impossible une approche purement réactive. Les États et les sociétés doivent anticiper les scénarios futurs pour préparer leurs défenses en conséquence.

Trois scénarios principaux se dessinent pour les décennies à venir, chacun avec des implications stratégiques majeures.

Le premier scénario, celui de l'escalade incontrôlée (2026–2030), est le plus probable à court terme.

Dans ce contexte, la multiplication des attaques combinées (guerre cognitive + guerre cognitive + cyberguerre) dans un contexte de course aux armements entre les grandes puissances pourrait conduire à une déstabilisation régionale massive. Les premières cibles seraient les pays les moins préparés, servant de terrain d'expérimentation pour les nouvelles technologies. *Indicateurs précurseurs* : une augmentation de plus de 50 % des attaques par *deepfakes* ciblant des décideurs ; le déploiement ouvert de *neuroweapons* par des États (Russie, Chine, États-Unis, Israël) ; l'adoption de lois d'urgence cognitive dans plusieurs pays pour contrer les menaces. *Conséquences* : Une déstabilisation rapide des pays cibles, avec des crises politiques et économiques en cascade, et un affaiblissement des alliances traditionnelles.

Le deuxième scénario, celui de la régulation et de la coopération (2030–2035), est possible si une crise majeure pousse les grandes puissances à trouver un consensus. Dans ce contexte, un traité international sur les guerres cognitive et cognitive pourrait émerger, interdisant les *neuroweapons offensifs* et régulant strictement les technologies de manipulation cérébrale.

Un cadre légal pour l'IA générative pourrait aussi imposer la transparence sur les contenus synthétiques et la responsabilité des plateformes comme c'est désormais le cas au sein de l'UE avec l'*AI Act* (aux

réserves près émises plus haut dans ce document). *Obstacles majeurs* : la réticence des grandes puissances à abandonner leur avantage cognitif ; la difficulté de vérification des technologies duales (civiles/militaires) ; les contournements possibles par des acteurs non étatiques (groupes terroristes, cybercriminels). *Conséquences* : Une réduction des tensions, mais avec des risques de non-respect du traité et des difficultés à faire appliquer les sanctions.

Le troisième scénario, celui de la domination cognitive (2035–2040), est le plus redoutable à long terme.

Dans ce contexte, une ou plusieurs puissances (États-Unis, Chine) pourraient acquérir une supériorité cognitive écrasante, leur permettant de dominer le reste du monde sans recourir à la force militaire.

Cette domination reposerait sur le contrôle des infrastructures technologiques, la manipulation des élites mondiales ainsi que sur l'influence sur les populations via la combinaison de désinformation et de neurostimulation. Des stratégies de résistance sont possibles même si leur efficacité peut paraître relativement illusoire : la formation d'alliances cognitives entre États pour partager les ressources et les connaissances ; le développement de solutions locales (neuroprotection, éducation cognitive) ; la résistance passive via l'éducation à la pensée critique. *Conséquences* : Un nouvel équilibre mondial, où la maîtrise des technologies cognitives deviendrait le facteur de puissance décisif, dépassant même les armes nucléaires.

Quelles que soient les évolutions futures, une chose est certaine : les guerres cognitive et cognitive sont déjà une réalité, et leur intégration dans les stratégies hybrides en fait des armes redoutables, capables de redéfinir les équilibres géopolitiques. Pour y faire face, une réponse intégrée, proactive et internationale est indispensable.

## VI - Conclusion : La guerre cognitive et la guerre cognitive comme piliers des conflits modernes

Les guerres cognitive et cognitive ne sont pas des phénomènes marginaux ou des concepts d'avenir : elles sont déjà au cœur des stratégies hybrides modernes, et leur importance ne fera que croître dans les décennies à venir. Leur originalité réside dans leur ciblage direct du cerveau humain et des processus de pensée, ce qui en fait des armes d'une puissance inédite, capables de contourner les défenses traditionnelles et de déstabiliser des sociétés entières.

Cinq enseignements clés émergent de cette analyse :

Premièrement, la guerre cognitive et la guerre cognitive s'intègrent pleinement dans le cadre des guerres hybrides, où elles jouent un rôle transversal et synergique. Elles renforcent toutes les autres dimensions (conventionnelle, irrégulière, cyberguerre, guerre économique) et agissent comme des multiplicateurs de puissance, avec des effets exponentiels ( $\times 3$  à  $\times 10$ ).

Deuxièmement, elles ciblent le substrat le plus stratégique : l'esprit humain. Contrairement aux autres formes de guerre hybride, qui visent des infrastructures ou des ressources, la guerre cognitive et la guerre cognitive attaquent directement la capacité de penser, de décider et d'agir — le véritable centre de gravité des conflits modernes.

Les technologies de contrôle cérébral sont désormais déployées opérationnellement dans plusieurs conflits, avec des applications variées : désorientation, manipulation, espionnage et contrôle mental.

### Comparaison des technologies de contrôle cérébral

| Technologie                  | Mécanisme                                          | Précision | Portée    | Effets                                           | Coût   | Risques                                     | Déploiement                          |
|------------------------------|----------------------------------------------------|-----------|-----------|--------------------------------------------------|--------|---------------------------------------------|--------------------------------------|
| Ondes EM (1–3 GHz)           | Modulation des canaux ioniques (Ca <sup>2+</sup> ) | ★ ★ ★     | 1–5 km    | Désorientation, hallucinations auditives         | Moyen  | Effets variables, dépendance aux conditions | Opérationnel (Syndrome de La Havane) |
| Ondes scalaires (0,1–100 Hz) | Synchronisation des ondes cérébrales               | ★ ★       | 10–100 km | Désorientation collective, contrôle des émotions | Faible | Manque de précision                         | Opérationnel (Russie, Chine)         |

| Technologie                    | Mécanisme                              | Précision | Portée            | Effets                                       | Coût       | Risques                              | Déploiement                              |
|--------------------------------|----------------------------------------|-----------|-------------------|----------------------------------------------|------------|--------------------------------------|------------------------------------------|
| Ultrasons (20–50 kHz)          | Stimulation mécanique du cerveau       | ★★★★      | 10–20 m           | Paralysie temporaire, hallucinations         | Moyen      | Effets imprévisibles                 | Opérationnel (Israël, États-Unis)        |
| BCI (Neuralink, BrainGate)     | Lecture/écriture des signaux neuronaux | ★★★★★     | Contact           | Contrôle mental, amélioration cognitive      | Élevé      | Piratage, dépendance                 | Tests sur humains (2023)                 |
| Nanoneurotechnologies          | Interaction à l'échelle moléculaire    | ★★★★★     | Injection         | Espionnage neuronal, contrôle des émotions   | Très élevé | Toxicité, rejet immunitaire          | Tests sur animaux (2020)                 |
| Drogues (LSD, BZ, scopolamine) | Modulation des neurotransmetteurs      | ★★★       | Injection/aérosol | Désorientation, amnésie, hallucinations      | Faible     | Effets imprévisibles, dépendance     | Opérationnel (CIA, Mossad)               |
| Hypnose                        | Suggestions post-hypnotiques           | ★★        | Contact           | Contrôle mental temporaire                   | Faible     | Effets temporaires, variabilité      | Opérationnel (MKUltra, Mossad)           |
| IA générative                  | Création de deepfakes neuronaux        | ★★★★      | Monde entier      | Manipulation des perceptions, désinformation | Moyen      | Désinformation massive, polarisation | Opérationnel (Chine, Russie, États-Unis) |

Troisièmement, elles représentent une menace asymétrique, car elles sont peu coûteuses (pour la guerre cognitive), déniaables (pour la guerre cognitive) et accessibles à des acteurs non étatiques (groupes terroristes, cybercriminels). Elles contournent les défenses traditionnelles (éducation, esprit critique) en agissant directement sur le cerveau ou en exploitant les biais cognitifs.

Quatrièmement, elles nécessitent une défense intégrée, combinant neuroprotection, éducation cognitive, cybersécurité, résilience économique et coopération internationale. Aucune mesure seule ne suffit : une défense fragmentée est vouée à l'échec face à une menace aussi complexe et synergique.

Enfin, elles constituent un enjeu géopolitique majeur. Les États qui maîtrisent ces technologies (États-Unis, Chine) auront un avantage stratégique décisif, capable de redéfinir les équilibres mondiaux. Les autres États doivent rattraper leur retard pour éviter une dépendance stratégique et une perte de souveraineté mentale.

En définitive, les guerres cognitive et cognitive ne sont pas l'avenir de la guerre — elles en sont déjà le présent. Leur intégration dans les stratégies hybrides en fait des armes redoutables, capables de transformer radicalement la nature des conflits.

La question n'est plus de savoir *si* ces technologies existeront, mais *comment* nous allons y faire face. La maîtrise du cerveau pourrait bien devenir le facteur décisif des conflits du XXI<sup>e</sup> siècle. Pour y faire face, une réponse intégrée, proactive et internationale est indispensable.

Au moment où l'UE actualise sa stratégie de sécurité<sup>17</sup> et commence à déployer un certain nombre d'initiatives pour faire face aux différentes formes de menaces hybrides, elle doit prendre pleinement acte des constats postés dans cette analyse sauf à considérer qu'il appartient uniquement à chacun de ses Etats membres ainsi qu'à l'Otan d'en tirer les conséquences qui s'imposent, ce qui serait contraire aux positions récentes du Conseil européen en faveur d'initiatives allant dans le sens d'une plus grande souveraineté dans les secteurs stratégiques, alors que ses Etats membres s'emploient encore à acheter des équipements et systèmes de défense non européens (américains, israéliens) au mépris des grandes déclarations d'autonomie stratégique prononcées par certains dirigeants politiques..

<sup>17</sup> Cf. Patrice Cardot - [Plaidoyer en faveur d'une doctrine européenne globale de sécurité et de résilience](#) – academia.edu  
Voir également COMECE - [Une stratégie de sécurité européenne au service de la paix](#) – Schuman Paper n° 843)

Enfin, il est indispensable qu'en France comme en Europe, des centres de recherche appropriés tels que l'IRSEM, le Centre de Doctrine et d'Enseignement du Commandement (CDEC), le Conseil scientifique de Défense (CSD), et au-delà des milieux militaires, des centres et laboratoires de recherche comme le CR451 de l'EGE<sup>18</sup> poursuivent les travaux sur ces sujets car il demeure encore beaucoup de thèmes de recherche pour en circonscrire toutes les dimensions actuelles et futures.

---

<sup>18</sup> Constitué à l'automne 2021 à partir d'un diagnostic formulé par Christian Harbulot, cofondateur de École de Guerre Économique, le CR451 procède d'un constat simple mais structurant : les conflictualités contemporaines se déploient désormais de manière continue sur des terrains économiques, géopolitiques, sociétaux et informationnels, au point que la guerre économique systémique s'impose comme un paradigme central de la marche du monde.

Le centre privilégie une logique de recherche appliquée, où l'ambition n'est pas seulement de décrire, mais de construire des outils, d'aider à la décision dans des contextes d'affrontements multi-champs et multi-acteurs, d'anticiper les stratégies de l'adversaire.

Cf. [Centre de Recherche Appliquée de l'Ecole de Guerre Economique - CR 451](#)

## ANNEXE A

### ***Phénomènes électromagnétiques, lumineux et autres vecteurs d'influence cognitive***

#### *Une analyse comparative des mécanismes d'action sur le cerveau et les états de conscience*

Comme nous l'avons vu, la guerre cognitive au sens le plus large du terme (elle inclura dans cette annexe les deux dimensions examinées dans le corps de ce document) plonge ses racines dans une compréhension intime des mécanismes par lesquels le cerveau humain peut être ciblé, manipulé, ou protégé.

Parmi ces mécanismes, les phénomènes électromagnétiques et lumineux occupent une place à part : invisibles, souvent imperceptibles, mais capables d'agir à distance sur les processus neuronaux les plus fondamentaux. Pourtant, ces technologies ne sont pas les seules à pouvoir altérer les états de conscience. Les drogues psychotropes, les stimulations sonores, ou même les états modifiés de conscience (méditation, transe, hypnose) offrent des voies alternatives – parfois plus accessibles, parfois plus précises – pour atteindre des objectifs similaires.

Comparer ces vecteurs, c'est comprendre leurs forces, leurs limites, et leurs synergies possibles.

Cette annexe A propose donc une plongée systématique dans :

1. Les mécanismes physiques et neurobiologiques de chaque type de vecteur.
2. Leur efficacité relative selon les états de conscience (éveil, sommeil, transe, etc.).
3. Les verrous scientifiques actuels qui freinent leur déploiement massif.
4. Les leçons tirées d'incidents réels (expériences militaires, études cliniques, accidents industriels).

### **1. Les phénomènes électromagnétiques : quand la physique rencontre la biologie**

#### **1.1. Le cerveau, une antenne biologique ?**

Le cerveau humain baigne dans un océan invisible d'ondes électromagnétiques, naturelles ou artificielles. Depuis les champs géomagnétiques terrestres jusqu'aux signaux Wi-Fi omniprésents, notre système nerveux est constamment exposé à des stimuli électromagnétiques de fréquences et d'intensités variées.

La question centrale est : dans quelle mesure ces ondes peuvent-elles influencer – voire contrôler – notre activité cérébrale ?

#### **Le principe de l'interaction ondes-cerveau**

Contrairement à une idée reçue, le cerveau n'est pas un système totalement isolé des champs électromagnétiques.

Plusieurs mécanismes permettent une interaction :

*Couplage avec les ions* : Les champs EM peuvent moduler le flux d'ions ( $\text{Na}^+$ ,  $\text{K}^+$ ,  $\text{Ca}^{2+}$ ) à travers les membranes neuronales, influençant ainsi les potentiels d'action.

*Effets thermiques* : Une augmentation locale de température (même minime, de l'ordre de  $0,1^\circ\text{C}$ ) peut altérer la vitesse de transmission synaptique.

*Résonance avec les réseaux neuronaux* : Certaines fréquences (ex. : 10 Hz) peuvent synchroniser l'activité de populations neuronales, comme le font naturellement les ondes alpha ou thêta.

#### **Étude de cas : Le "Moscow Signal" (1972–1989)**

Entre 1972 et 1989, l'ambassade américaine à Moscou a été irradiée par des micro-ondes pulsées (fréquences estimées entre 2,5 et 4 GHz), probablement émises depuis un bâtiment voisin. Les employés exposés ont rapporté des maux de tête chroniques, des troubles du sommeil et de la mémoire et une fatigue persistante et des difficultés de concentration. Dans certains cas, des symptômes dépressifs et des comportements anormaux (irritabilité, paranoïa).

## Analyse technique

*Fréquence utilisée* : Les micro-ondes dans cette gamme (2,5–4 GHz) ont une profondeur de pénétration d'environ 2–3 cm dans les tissus biologiques, suffisant pour atteindre le cortex cérébral.

*Mécanisme supposé* : effet thermique (une augmentation locale de température dans les tissus cérébraux pourrait avoir perturbé l'activité synaptique) ; effet non-thermique (les pulsations pourraient avoir modulé l'activité des canaux ioniques (notamment les canaux calcium voltage-dépendants)).

*Preuves scientifiques* : une étude de l'US Army (1976) a confirmé que des micro-ondes pulsées à 1–10 GHz pouvaient induire des changements comportementaux chez des animaux (rats, singes), notamment une réduction de la motivation et une altération de la mémoire. En 1979, le Dr. Milton Zaret (ophtalmologiste) a publié des résultats montrant que des micro-ondes à 2,45 GHz pouvaient causer des lésions oculaires et des troubles neurologiques chez des lapins.

*Conséquences géopolitiques* : Le gouvernement américain a renforcé le blindage EM de ses ambassades dans le monde entier. Ce cas a marqué le début des recherches sérieuses sur les *neuroweapons* par les agences de renseignement (CIA, DARPA).

Aujourd'hui encore, le *Moscow Signal* reste un cas d'école en guerre électronique, bien que son existence officielle n'ait jamais été confirmée par la Russie.

## 1.2. Gammes de fréquences et leurs effets sur le cerveau

Chaque gamme de fréquences électromagnétiques interagit avec le cerveau de manière spécifique, en fonction de sa pénétration, de son mécanisme d'action, et de sa résonance avec les processus biologiques.

### 1.2.1. Ondes de très basse fréquence (ELF : 3–300 Hz)

*Mécanisme* : Les ondes ELF, bien que de faible énergie, peuvent pénétrer profondément dans les tissus biologiques (jusqu'à plusieurs mètres dans le corps). Leur mécanisme d'action principal est la modulation des champs électriques naturels du cerveau (ex. : ondes delta, thêta).

*Effets documentés* : synchronisation des ondes cérébrales (des études ont montré que des champs ELF à 10 Hz peuvent induire des ondes alpha (8–12 Hz) dans le cerveau, associées à un état de relaxation ou de transe légère) ; altération de l'humeur (une exposition prolongée à des champs ELF à 50–60 Hz (fréquence du réseau électrique) a été associée à des symptômes dépressifs et à une fatigue chronique (syndrome de "sensibilité électromagnétique")) ; effets sur la mémoire (des expériences sur des animaux ont montré que des champs ELF à 7 Hz pouvaient perturber la consolidation de la mémoire (étude de l'US Air Force, 1981)).

*Application en guerre cognitive* : Manipulation émotionnelle à grande échelle (des émetteurs ELF pourraient théoriquement être utilisés pour induire des états de fatigue ou de désorientation dans une population (ex. : pendant une opération militaire ou une crise politique)) ; contrôle des foules (en combinaison avec des infrasons, les ondes ELF pourraient amplifier les effets de panique (théorie testée par l'armée française dans les années 1990, projet "*Système de Contrôle des Foules*").

*Limites et verrous scientifiques* : faible puissance (les ondes ELF ont une intensité très faible (de l'ordre du  $\mu\text{T}$ ), ce qui limite leur capacité à induire des effets rapides et puissants) ; variabilité individuelle (les effets varient considérablement selon les individus, en fonction de leur sensibilité électromagnétique (un phénomène encore mal compris) ; détectabilité (les émetteurs ELF sont faciles à détecter (antennes simples), ce qui limite leur utilisation furtive).

### Étude de cas : Projet "*Pandora*" (CIA, 1965–1970)

Dans les années 1960, la CIA a lancé le projet Pandora pour étudier les effets des micro-ondes sur le comportement humain, suite à des rumeurs selon lesquelles l'URSS utilisait des armes à ondes EM pour influencer les ambassades américaines.

*Découvertes clés* : Les micro-ondes pulsées (1–10 GHz) pouvaient induire des sons audibles directement dans le cerveau (effet "*microwave hearing*", ou effet Frey).

*Mécanisme* : L'absorption des micro-ondes par les tissus cérébraux provoque une expansion thermoacoustique (une onde de pression), perçue comme un clic ou un bourdonnement.

*Application potentielle* : Communication directe avec le cerveau (sans haut-parleurs), ou désorientation via des sons stridents. Des champs EM à 1 GHz pouvaient altérer les temps de réaction et la prise de décision chez des sujets humains (étude interne de la CIA, 1969). Les ondes ELF (10–100 Hz) pouvaient synchroniser les ondes cérébrales et induire des états de transe chez des animaux.

Le projet a été abandonné en 1970, officiellement pour des raisons de coût et de faisabilité limitée. Cependant, des documents déclassifiés suggèrent que les résultats étaient trop imprévisibles pour un déploiement opérationnel.

### 1.2.2. Radiofréquences et micro-ondes (300 MHz – 300 GHz)

*Mécanisme* : Les radiofréquences (RF) et les micro-ondes agissent principalement par effet thermique (l'absorption des ondes par les molécules d'eau dans les tissus provoque un échauffement local. *Seuil critique* : Une élévation de 1°C peut déjà perturber l'activité neuronale) et par effet non-thermique (modulation des canaux ioniques (ex. : canaux calcium voltage-dépendants) ; altération de la barrière hémato-encéphalique (BHE), permettant à des substances normalement bloquées (ex. : toxines) de pénétrer dans le cerveau).

*Effets documentés* :

| Fréquence       | Effet sur le cerveau                    | Application potentielle                         | Seuil d'effet                        |
|-----------------|-----------------------------------------|-------------------------------------------------|--------------------------------------|
| 300 MHz – 1 GHz | Réchauffement localisé, fatigue         | Désorientation de troupes                       | > 10 W/m <sup>2</sup> (norme ICNIRP) |
| 1–3 GHz         | Altération de la mémoire à court terme  | Manipulation cognitive (ex. : oubli temporaire) | > 5 W/m <sup>2</sup>                 |
| 3–10 GHz        | Effet Frey (audition directe)           | Communication subliminale                       | > 1 W/m <sup>2</sup>                 |
| 10–30 GHz       | Perturbation de la coordination motrice | Incapacité temporaire                           | > 20 W/m <sup>2</sup>                |

*Application en guerre cognitive* : Armes à énergie dirigée (DEW) : Le *Active Denial System* (ADS) de l'US Army (déployé en Afghanistan et en Irak) utilise des micro-ondes à 95 GHz pour provoquer une sensation de brûlure intense à distance (portée : 500–700 m), forçant les cibles à fuir.

*Limite* : Effet purement physique (douleur), pas cognitif. Mais des variantes pourraient être développées pour cibler le cerveau.

*Neuroweapons* expérimentaux : La DARPA a testé des émetteurs à 1,5 GHz capables d'induire des hallucinations auditives (effet Frey) ou des troubles de l'équilibre (via stimulation du système vestibulaire).

### Étude de cas : L'"Effet Frey" et ses implications militaires

En 1961, le chercheur Allan H. Frey a découvert que des micro-ondes pulsées (1–10 GHz) pouvaient être perçues comme des sons directement par le cerveau, sans passer par les oreilles. Cet effet, appelé "*microwave hearing*", a immédiatement suscité l'intérêt des militaires.

*Expérience clé* : Frey a exposé des sujets humains à des impulsions micro-ondes de 1,3 GHz, modulées à des fréquences audibles (1–10 kHz). Les sujets ont rapporté entendre des clics, des bourdonnements, ou des voix indistinctes, comme si les sons provenaient de l'intérieur de leur crâne. Aucune lésion auditive n'a été détectée, suggérant un mécanisme purement neurobiologique.

*Applications militaires* : communication subliminale (transmission de messages directs au cerveau (ex. : ordres, suggestions) sans équipement audio) ; armes de désorientation (utilisation de sons stridents ou de voix pour perturber les soldats ennemis) ; espionnage (écoute à distance des conversations internes (en théorie, en inversant l'effet Frey pour capter les ondes cérébrales)).

*Limites* : portée limitée (les micro-ondes sont fortement atténuées par l'atmosphère (portée efficace : < 1 km) ; précision limitée (difficile de cibler un individu spécifique dans une foule) ; effets secondaires (risque de maux de tête ou de nausées avec une exposition prolongée).

### **1.2.3. Lumière visible et infrarouge (400 THz – 300 GHz)**

*Mécanisme* : La lumière interagit avec le cerveau principalement via une stimulation des photorécepteurs (cônes et bâtonnets dans la rétine) → modulation de la mélatonine (rythme circadien), des effets thermiques (lasers infrarouges) → réchauffement localisé des tissus cérébraux, et des effets photochimiques (ex. : activation de la rhodopsine ou d'autres protéines photosensibles).

*Effets documentés*

#### **Lumière stroboscopique (10–20 Hz)**

*Effet* : Synchronisation des ondes cérébrales (phénomène de "flicker fusion").

*Application* : Induction de crises épileptiques chez les personnes prédisposées (ex. : système de défense "Dazzle" utilisé par les forces de l'ordre).

*Étude clé* : En 1997, un épisode de Pokémon (épisode "Dennō Senshi Porygon") a provoqué des crises chez 685 enfants japonais en raison de flashes lumineux à 12 Hz.

#### **Lasers infrarouges**

*Effet* : Stimulation thermique des méninges → maux de tête, nausées.

*Application* : Armes de désorientation (ex. : lasers "dazzling" utilisés pour aveugler temporairement les pilotes).

#### **Lumière bleue (450–495 nm)**

*Effet* : Inhibition de la mélatonine → troubles du sommeil, fatigue chronique.

*Application* : Manipulation du rythme circadien (ex. : éclairage LED dans les prisons pour désorienter les détenus).

*Application en guerre cognitive* : manipulation du sommeil (utilisation de lumières bleues pulsées pour perturber le sommeil profond et induire une fatigue chronique) ; illusions optiques (combinaison de lasers et de réalité augmentée pour créer des hallucinations visuelles contrôlées) ; contrôle des foules (lumières stroboscopiques pour provoquer des crises de panique - testé par l'armée israélienne en Cisjordanie).

#### **Étude de cas : L'incident de Pokémon (1997) et ses leçons pour la guerre cognitive**

Le 16 décembre 1997, l'épisode "Dennō Senshi Porygon" de la série Pokémon a été diffusé au Japon. Cet épisode contenait des séquences de flashes lumineux rouges et bleus à 12 Hz, qui ont provoqué des crises épileptiques chez 685 enfants, dont certains ont dû être hospitalisés.

*Mécanisme* : Les flashes à 12 Hz ont synchronisé les ondes cérébrales des enfants (notamment ceux souffrant d'épilepsie photosensible), provoquant des décharges neuronales anormales.

*Effets observés* : Crises tonico-cloniques (convulsions), Hallucinations visuelles (lumières, couleurs), Perte de conscience.

*Conséquences* : L'épisode a été interdit dans plusieurs pays. Les normes de sécurité pour les médias ont été renforcées (ex. : limitation des flashes à < 3 Hz en Europe).

*Leçons pour la guerre cognitive* : les stimulations lumineuses à certaines fréquences peuvent avoir des effets massifs et imprévisibles sur des populations sensibles ; une arme basée sur ce principe pourrait être développée pour désorienter des troupes ou des foules (ex. : drones équipés de lasers stroboscopiques).

*Contre-mesure* : Filtres optiques (lunettes anti-flashes) ou entraînement à la résistance (ex. : exposition progressive aux stimuli lumineux).

Etant donné l'importance de ces phénomènes dans une société en proie à une amplification incessante des usages de technologies recourant à ces phénomènes électromagnétiques, l'annexe B propose une analyse précise et documentée sur les ondes électromagnétiques utilisées par les systèmes de télécommunication à distance et les risques pour les utilisateurs.

## **2. Les phénomènes sonores : quand l'audition devient une porte d'entrée vers le cerveau**

### **2.1. Le son comme outil de manipulation cognitive**

Le son est un vecteur de guerre cognitive sous-estimé. Contrairement aux ondes EM, qui nécessitent des équipements spécialisés, les attaques sonores peuvent être déployées avec des haut-parleurs standard, des écouteurs, ou même des systèmes de communication existants (ex. : radio, téléphone).

#### *Mécanismes d'action*

Stimulation mécanique : les infrasons (0,1–20 Hz) peuvent faire résonner les organes internes (ex. : poumons, cœur, crâne), provoquant des nausées, des vertiges, ou une anxiété intense. Les ultrasons (20 kHz–1 GHz) peuvent cibler des zones cérébrales spécifiques via des transducteurs focalisés (ex. : *Low-Intensity Focused Ultrasound*, LIFU).

Stimulation neuronale : les sons à fréquences spécifiques (ex. : 10 Hz) peuvent synchroniser les ondes cérébrales (phénomène d'entraînement auditif). Les *binaural beats* (différence de fréquence entre les oreilles) peuvent induire des états de transe ou de relaxation profonde.

Stimulation émotionnelle : la musique peut moduler les niveaux de dopamine et de sérotonine, influençant ainsi l'humeur et la motivation. Les sons aigus ou dissonants peuvent provoquer des réactions de stress (ex. : augmentation du cortisol).

### **2.2. Applications en guerre cognitive**

#### **2.2.1. Les infrasons : l'arme invisible**

*Mécanisme* : Les infrasons (0,1–20 Hz) sont inaudibles pour l'oreille humaine, mais peuvent faire vibrer les organes internes à leur fréquence de résonance naturelle.

*Par exemple* : 7 Hz : fréquence de résonance du crâne humain → peut provoquer des maux de tête, des nausées, ou des hallucinations ; 16 Hz : fréquence de résonance des yeux → peut causer une vision floue ou des illusions optiques.

*Effets documentés* : nausées et vertiges (expositions prolongées à des infrasons de 10 Hz (120 dB) provoquent des symptômes similaires au mal des transports (étude de l'US Navy, 1980)) ; anxiété et panique (des infrasons de 18 Hz (130 dB) ont été associés à des sentiments de terreur chez des sujets humains (expérience de NASA, 1964)) ; hallucinations (des infrasons de 1–10 Hz peuvent induire des visions de "présences" ou d'ombres (phénomène rapporté dans des églises et cathédrales, où les orgues génèrent des infrasons)).

*Application militaire* : armes à infrasons : Le *Long Range Acoustic Device* (LRAD) (développé par l'US Navy) peut émettre des infrasons à 150 dB sur une portée de 500 m, provoquant une douleur insupportable et forçant les cibles à fuir.

*Utilisation* : Déployé en Irak et en Afghanistan pour disperser les foules ou désorienter les insurgés.

*Limite* : Effet purement physique (douleur), pas cognitif. Mais des variantes pourraient être développées pour cibler le cerveau. Désorientation des troupes (des émetteurs d'infrasons portables pourraient être utilisés pour perturber la coordination motrice des soldats ennemis.)

#### **Étude de cas : Le projet "Ghost in the Machine" (US Army, 1990–2000)**

Dans les années 1990, l'US Army a mené des recherches secrètes sur les effets des infrasons sur le comportement humain, sous le nom de code "*Ghost in the Machine*".

*Découvertes clés* : des infrasons de 18 Hz (120 dB) pouvaient provoquer des hallucinations auditives et visuelles chez des sujets humains ; des infrasons de 7 Hz (110 dB) pouvaient induire un état de transe

chez des individus prédisposés ; uUne exposition prolongée (plusieurs heures) à des infrasons de 10 Hz pouvait causer une fatigue extrême et une désorientation.

*Application potentielle* : arme de désinformation (utilisation d'infrasons pour faire croire à des présences surnaturelles (ex. : dans une zone de conflit pour semer la panique) ; contrôle des foules (combinaison d'infrasons et de sons audibles pour provoquer des réactions de panique collective).

Le projet a été abandonné en 2000, officiellement pour des raisons de coût et de faisabilité limitée. Cependant, des rumeurs suggèrent que les résultats étaient trop imprévisibles pour un déploiement opérationnel.

### 2.2.2. Les *binaural beats* : la musique comme outil de contrôle mental

*Mécanisme* : les *binaural beats* sont créés lorsque deux fréquences légèrement différentes sont jouées séparément dans chaque oreille (ex. : 300 Hz à gauche, 310 Hz à droite). Le cerveau perçoit une troisième fréquence (10 Hz dans cet exemple), qui peut synchroniser les ondes cérébrales.

*Effets documentés* :

| Fréquence du beat | Onde cérébrale induite | Effet sur la conscience            | Application potentielle                                  |
|-------------------|------------------------|------------------------------------|----------------------------------------------------------|
| 0,5–4 Hz          | Delta                  | Sommeil profond, régénération      | Induction du sommeil (ex. : pour neutraliser des gardes) |
| 4–8 Hz            | Thêta                  | Transe, créativité, suggestibilité | Hypnose à distance, implantation de souvenirs            |
| 8–12 Hz           | Alpha                  | Relaxation, réduction du stress    | Désarmement émotionnel (ex. : calmer une foule)          |
| 12–30 Hz          | Bêta                   | Concentration, vigilance           | Amélioration cognitive forcée (ex. : soldats)            |
| 30–100 Hz         | Gamma                  | Hyperconnexion, perception altérée | Induction de psychoses temporaires                       |

*Application en guerre cognitive* : hypnose à distance (utilisation de *binaural beats* à 4 Hz pour induire un état de transe chez une cible, facilitant ainsi l'implantation de suggestions (ex. : via un message subliminal)) ; manipulation émotionnelle (combinaison de *binaural beats* à 10 Hz (alpha) et de musique apaisante pour réduire la résistance aux ordres) ; désorientation (utilisation de *binaural beats* à 25 Hz (bêta) pour provoquer une surcharge cognitive et une paralysie décisionnelle).

### Étude de cas : Le projet "*Silent Sound*" (CIA, 1980–1990)

Dans les années 1980, la CIA a exploré l'utilisation des **binaural beats** pour la **manipulation cognitive**, sous le nom de code "*Silent Sound*".

*Découvertes clés* : des *binaural beats* à 7 Hz (thêta) pouvaient induire un état de transe chez 80% des sujets testés ; des messages subliminaux (ex. : "Tu es en sécurité", "Obéis") intégrés dans les beats augmentaient la suggestibilité des sujets ; une exposition prolongée (plusieurs jours) à des beats à 4 Hz (delta) pouvait provoquer des troubles du sommeil et une fatigue chronique.

*Application potentielle* : interrogatoires améliorés (utilisation de *binaural beats* pour faciliter l'extraction d'informations chez des prisonniers) ; propagande subliminale (diffusion de messages cachés dans des musiques ou des discours, via des beats adaptés).

Le projet a été abandonné en 1990, officiellement pour des raisons de manque de résultats concluants. Cependant, des documents déclassifiés suggèrent que les effets étaient trop variables selon les individus.

### 2.2.3. Les ultrasons : une stimulation cérébrale ciblée

*Mécanisme* : les ultrasons (20 kHz–1 GHz) peuvent être focalisés sur des zones cérébrales spécifiques via des transducteurs à réseau phasé. Cette technologie, appelée *Low-Intensity Focused Ultrasound* (LIFU), permet une stimulation non invasive du cerveau avec une résolution millimétrique.

*Effets documentés* : stimulation du cortex moteur (des ultrasons à 500 kHz peuvent provoquer des mouvements involontaires (ex. : contraction des doigts)) ; stimulation du cortex visuel (des ultrasons à 1 MHz peuvent induire des hallucinations visuelles (ex. : flashes lumineux)) ; modulation de l'humeur (des ultrasons à 200 kHz ciblant le cortex préfrontal peuvent réduire les symptômes dépressifs (étude de l'Université de Virginie, 2018)).

*Application en guerre cognitive* : contrôle moteur à distance (utilisation d'ultrasons pour provoquer des mouvements involontaires chez une cible (ex. : faire tomber un soldat)) ; manipulation sensorielle (induction d'hallucinations visuelles ou auditives pour désorienter une cible) ; *neuroweapons* portables (développement de pistolets à ultrasons capables de neutraliser temporairement un individu (ex. : projet "Neural Disruptor" de la DARPA)).

### Étude de cas : Le projet "Neural Disruptor" (DARPA, 2015–2020)

La DARPA a lancé le projet "Neural Disruptor" pour développer une arme à ultrasons portable capable de neutraliser temporairement un individu en ciblant son cortex moteur ou préfrontal.

*Découvertes clés* : des ultrasons à 500 kHz (intensité : 10 W/cm<sup>2</sup>) pouvaient provoquer une paralysie temporaire (1–5 minutes) du cortex moteur, empêchant tout mouvement volontaire. Des ultrasons à 1 MHz (intensité : 5 W/cm<sup>2</sup>) pouvaient induire des hallucinations visuelles (ex. : flashes lumineux, ombres). Le système était portable (taille : un pistolet) et avait une portée de 10–20 m.

*Application potentielle* : neutralisation de cibles (utilisation dans des opérations spéciales pour désarmer un ennemi sans le tuer) ; contrôle des foules (déploiement dans des zones de conflit pour désorienter les foules).

Le projet est toujours en développement (2026), avec des tests sur des animaux (singe, cochon). Aucun déploiement opérationnel n'a encore été confirmé.

## 3. Les processus chimiques : quand la guerre cognitive devient une guerre pharmacologique

### 3.1. Les drogues comme outils de manipulation cognitive

Les substances chimiques (drogues, médicaments, toxines) offrent un vecteur de guerre cognitive particulièrement puissant, car elles agissent directement sur les neurotransmetteurs – les messagers chimiques du cerveau.

Contrairement aux ondes EM ou sonores, qui nécessitent une exposition externe, les drogues peuvent être administrées de manière discrète (aérosols, aliments, injections) et avoir des effets durables.

*Mécanismes d'action* : Les drogues agissent principalement par :

1. Modulation des neurotransmetteurs agonistes (mimétisent l'action d'un neurotransmetteur (ex. : LSD agoniste de la sérotonine), antagonistes (bloquent l'action d'un neurotransmetteur (ex. : halopéridol antagoniste de la dopamine), et inhibiteurs de la recapture (augmentent la concentration d'un neurotransmetteur dans la synapse (ex. : la cocaïne inhibe la recapture de la dopamine)).
2. Modulation des canaux ioniques : certaines toxines (ex. : ttx, tétrodoxtine) bloquent les canaux sodiques, empêchant la propagation des potentiels d'action.
3. Altération de la structure neuronale : certaines drogues (ex. : MDMA) peuvent provoquer une neurotoxicité (dégâts permanents aux neurones sérotoninergiques).

| Méthode                              | Description                                                                                                                                 | Technologies associées                         | Effets sur le cerveau                                                            | Applications militaires                                |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------|
| <b>Stimulation électromagnétique</b> | Ondes EM (1–10 GHz) modulent les canaux ioniques (Ca <sup>2+</sup> , Na <sup>+</sup> , K <sup>+</sup> ) → libération de neurotransmetteurs. | Neurostimulateurs (TMS, rTMS), ondes scalaires | Augmentation de la dopamine (motivation), diminution du GABA (anxiété)           | Contrôle des émotions (peur, euphorie), désorientation |
| <b>Inhibition électromagnétique</b>  | Ondes EM basses fréquences (0,1–100 Hz) bloquent les                                                                                        | Ondes ELF, infrasons                           | Diminution de la sérotonine (dépression), augmentation du glutamate (excitation) | Paralysie décisionnelle, panique collective            |

| Méthode                               | Description                                                                                               | Technologies associées                                                         | Effets sur le cerveau                                       | Applications militaires                               |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------|-------------------------------------------------------|
|                                       | canaux ioniques → diminution des neurotransmetteurs.                                                      |                                                                                |                                                             |                                                       |
| <b>Drogues agonistes/antagonistes</b> | Molécules chimiques se lient aux récepteurs des neurotransmetteurs → modulation de leur activité.         | LSD (agoniste 5-HT <sub>2A</sub> ), BZ (antagoniste muscarinique), scopolamine | Hallucinations (LSD), confusion (BZ), amnésie (scopolamine) | Interrogatoires, manipulation des souvenirs           |
| <b>Nanoneurotechnologies</b>          | Nanoparticules ciblent les récepteurs ou les canaux ioniques → modulation précise des neurotransmetteurs. | Nanocapteurs (Neural Dust), nanorobots                                         | Libération ciblée de dopamine/sérotinine                    | Contrôle émotionnel précis, implantation de souvenirs |

### 3.2. Classification des drogues par effet sur la conscience

| Catégorie             | Exemples                               | Neurotransmetteur ciblé          | Effets sur la conscience                                 | Application en guerre cognitive                          | Durée des effets | Contre-mesures                       |
|-----------------------|----------------------------------------|----------------------------------|----------------------------------------------------------|----------------------------------------------------------|------------------|--------------------------------------|
| <b>Dépresseurs</b>    | Alcool, benzodiazépines, barbituriques | GABA                             | Sédation, réduction de l'anxiété, confusion              | Désorientation, réduction de la vigilance                | 2–24 h           | Antidotes (flumazénil), ventilation  |
| <b>Stimulants</b>     | Caféine, amphétamines, cocaïne         | Dopamine, noradrénaline          | Hypervigilance, euphorie, paranoïa                       | Amélioration cognitive forcée, manipulation émotionnelle | 1–12 h           | Sédatifs, hydratation                |
| <b>Hallucinogènes</b> | LSD, psilocybine, mescaline            | Sérotinine (5-HT <sub>2A</sub> ) | Hallucinations, altération de la perception, synesthésie | Désorientation, manipulation sensorielle                 | 6–12 h           | Benzodiazépines, environnement calme |
| <b>Dissociatifs</b>   | Kétamine, PCP, dextrométhorphan        | NMDA (glutamate)                 | Dissociation, dépersonnalisation, psychose               | Neutralisation temporaire, contrôle mental               | 1–6 h            | Benzodiazépines, isolement           |
| <b>Opioides</b>       | Morphine, héroïne, fentanyl            | Endorphines                      | Analgésie, euphorie, sédation                            | Réduction de la douleur, manipulation émotionnelle       | 2–8 h            | Naloxone, ventilation                |
| <b>Cannabinoïdes</b>  | THC, CBD                               | Cannabinoïdes (CB1, CB2)         | Relaxation, altération de la mémoire, paranoïa           | Désorientation, réduction de la motivation               | 2–6 h            | Hydratation, environnement calme     |
| <b>Neurotoxines</b>   | BZ, sarin, VX                          | Acétylcholine                    | Confusion, hallucinations, paralysie                     | Désorientation massive, contrôle des foules              | Minutes à heures | Atropine, pralidoxime                |

### 3.3. Études de cas : L'utilisation militaire des drogues en guerre cognitive

#### 3.3.1. Le BZ (3-Quinuclidinyl Benzilate) : L'arme chimique de la confusion

Le BZ est un agent psychotrope développé par l'US Army dans les années 1950 comme arme non létale. Il agit comme un antagoniste des récepteurs muscariniques de l'acétylcholine, provoquant des hallucinations, une confusion mentale et une désorientation intense.

*Mécanisme d'action* : Le BZ bloque les récepteurs M1 de l'acétylcholine dans le cerveau, perturbant ainsi les voies cholinergiques impliquées dans la mémoire (hippocampe), la perception (cortex visuel et auditif) et la prise de décision (cortex préfrontal).

*Effets observés* : hallucinations visuelles et auditives (ex. : voir des insectes, entendre des voix) ; confusion mentale (incapacité à distinguer la réalité de l'illusion) ; désorientation spatiale et temporelle (perte de la notion du temps et de l'espace) ; amnésie antérograde (incapacité à former de nouveaux souvenirs pendant l'exposition) ; symptômes physiques : Sécheresse buccale, vision floue, tachycardie.

*Durée des effets* : début des symptômes (30 minutes à 4 heures après l'exposition) ; pic d'effet (6–8 heures après l'exposition) ; durée totale (24–72 heures sans séquelles à long terme).

*Application militaire* : Désorientation des troupes ennemies (le BZ a été testé sur des soldats américains dans les années 1960 (projet "*Operation Third Chance*"). Les résultats ont montré que :50% des soldats exposés étaient incapables de combattre après 1 heure et que 90% des soldats exposés présentaient des hallucinations après 4 heures) ; contrôle des foules (le BZ pourrait être utilisé pour disperser des émeutes ou neutraliser des groupes armés sans causer de morts) ; interrogatoires (le BZ a été testé comme "sérum de vérité" (projet "*MKUltra*" de la CIA), mais les résultats étaient trop imprévisibles pour une utilisation fiable) ; stockage et déploiement (le BZ a été stocké par l'*US Army* jusqu'aux années 1990, sous la forme de bombes à aérosol (portée : 1–5 km) et d'obus d'artillerie (portée : 10–20 km)).

Aujourd'hui, le BZ est interdit par la Convention sur les armes chimiques (CWC, 1993), mais des rumeurs suggèrent que certains pays (ex. : Russie, Chine) pourraient encore en posséder des stocks.

### **Étude de cas : L'incident de *Edgewood Arsenal* (1959)**

En 1959, l'*US Army* a mené des tests secrets du BZ sur des soldats volontaires à *Edgewood Arsenal* (Maryland). Les soldats ont été exposés à des aérosols de BZ dans une chambre hermétique.

*Résultats* : Tous les sujets ont présenté des hallucinations (ex. : voir des serpents, des araignées, ou des soldats ennemis). 70% des sujets ont perdu tout sens de la réalité et ont dû être physiquement maîtrisés. 1 sujet a tenté de se suicider en se jetant contre un mur, croyant qu'il était attaqué par des démons. Les effets ont duré 24–48 heures, avec une récupération complète après 72 heures.

*Conséquences* : Le BZ a été classé comme arme chimique et son utilisation a été restreinte. Les tests ont montré que le BZ était trop imprévisible pour un déploiement opérationnel (effets variables selon les individus).

### **3.3.2. Le LSD : De la contre-culture à la guerre psychologique**

Le LSD (diéthylamide de l'acide lysergique) a été synthétisé pour la première fois en 1938 par le chimiste suisse Albert Hofmann. Dans les années 1950–1960, la CIA a exploré son potentiel comme arme de guerre psychologique dans le cadre du projet MKUltra.

*Mécanisme d'action* : Le LSD est un agoniste des récepteurs 5-HT<sub>2A</sub> de la sérotonine, principalement localisés dans le cortex préfrontal. Son action provoque une augmentation de la connectivité cérébrale (observée en IRMf), une désorganisation des réseaux neuronaux (notamment le réseau du mode par défaut, DMN), et une libération accrue de glutamate (neurotransmetteur excitateur).

*Effets observés* : hallucinations visuelles et auditives (ex. : voir des couleurs intenses, des motifs géométriques, ou entendre de la musique) ; altération de la perception du temps et de l'espace (ex. : sensation de ralentissement du temps) ; dissolution de l'ego (perte du sens de soi, fusion avec l'environnement) ; émotions intenses (euphorie, peur, anxiété, paranoïa) ; synesthésie (mélange des sens, ex. : "voir des sons").

*Durée des effets* : début des effets : 30–90 minutes après l'ingestion. Pic d'effet : 2–4 heures après l'ingestion. Durée totale : 6–12 heures.

*Application en guerre cognitive* : manipulation sensorielle (le LSD pourrait être utilisé pour désorienter des soldats ou des décideurs en altérant leur perception de la réalité) ; interrogatoires (le LSD a été testé comme "sérum de vérité" dans le cadre du projet MKUltra, mais les résultats étaient trop imprévisibles (les sujets mentaient ou hallucinaient des réponses)) ; contrôle mental (en théorie, le LSD pourrait être utilisé pour implanter des suggestions (ex. : via hypnose sous l'effet de la drogue), mais cette application n'a jamais été validée scientifiquement).

### **Étude de cas : Le projet MKUltra (CIA, 1953–1973)**

Le projet MKUltra était un programme secret de la CIA visant à développer des techniques de contrôle mental pour une utilisation en guerre froide. Le LSD a été l'un des outils principaux du projet.

*Expériences clés* : administration de LSD à des sujets non consentants (Des prostituées, des prisonniers, et des patients psychiatriques ont été exposés au LSD sans leur consentement).

*Résultats* : les sujets présentaient des hallucinations intenses, une perte de contact avec la réalité, et dans certains cas, des comportements violents ou auto-destructeurs.

La CIA a testé l'utilisation du LSD pour faciliter l'hypnose et l'implantation de faux souvenirs.

*Résultats* : les sujets étaient plus suggestibles, mais les faux souvenirs implantés étaient souvent incohérents ou oubliés après la fin des effets du LSD. La CIA a exploré la possibilité d'utiliser le LSD comme arme de guerre psychologique (ex. : aérosols dans une zone de conflit).

*Problèmes* : le LSD est trop instable (se dégrade rapidement à la lumière et à l'air) et ses effets sont trop variables pour un déploiement massif.

Le projet MKUltra a été arrêté en 1973 après des révélations publiques sur ses abus. Les documents déclassifiés montrent que le LSD a été abandonné comme arme en raison de son manque de fiabilité.

### **3.3.3. Le Modafinil : L'amélioration cognitive forcée**

Le Modafinil (nom commercial : Provigil) est un médicament stimulant développé à l'origine pour traiter la narcolepsie. Aujourd'hui, il est largement utilisé (et détourné) comme drogue d'amélioration cognitive ("*smart drug*").

*Mécanisme d'action* : le Modafinil agit principalement en inhibant la recapture de la dopamine et en augmentant la libération de l'orexine (un neuropeptide impliqué dans l'éveil). Ses effets incluent une augmentation de la vigilance et de la concentration, une réduction de la fatigue mentale et une amélioration de la mémoire de travail.

*Effets observés* : amélioration cognitive (augmentation de 20–30% des performances dans les tâches de mémoire, de raisonnement et de prise de décision. Réduction de 50% du temps de réaction) ; effets secondaires (insomnie (si pris tard dans la journée). ; anxiété ou agitation (à haute dose) ; maux de tête, nausées ; dépendance psychologique (bien que faible)).

*Application militaire* : amélioration des soldats (le Modafinil est utilisé par plusieurs armées (ex. : US Air Force, armée française) pour augmenter l'endurance mentale des pilotes pendant les missions de longue durée, et réduire la fatigue des soldats en opérations prolongées) ; manipulation cognitive (en théorie, le Modafinil pourrait être utilisé pour forcer un individu à rester éveillé pendant des interrogatoires prolongés, ou pour améliorer les performances d'un décideur ou d'un soldat (mais avec un risque de dépendance ou de burnout)).

### **Étude de cas : L'utilisation du Modafinil par l'US Air Force**

Depuis les années 2000, l'US Air Force utilise le Modafinil pour ses pilotes de drone et d'avion de combat, notamment lors de missions de plus de 12 heures.

*Résultats* : réduction de 60% des erreurs liées à la fatigue chez les pilotes ; amélioration de 25% des performances en simulation de combat ; aucun effet secondaire grave rapporté (à des doses de 100–200 mg/jour).

*Limites* : effets à long terme inconnus (les études sur les effets d'une utilisation prolongée - plusieurs mois - sont limitées) ; dépendance psychologique (certains pilotes ont rapporté une difficulté à fonctionner sans Modafinil après une utilisation prolongée) ; coût (le Modafinil est relativement cher (environ 10–20 \$ par dose), ce qui limite son déploiement massif).

## **4. États modifiés de conscience : quand le cerveau se manipule lui-même**

### **Méditation, transe et hypnose : des outils de résilience... ou de vulnérabilité ?**

Les états modifiés de conscience (EMC) – tels que la méditation, la transe ou l'hypnose – sont des phénomènes naturels qui peuvent être exploités ou détournés dans le cadre de la guerre cognitive. Bien qu'ils soient souvent associés à des pratiques spirituelles ou thérapeutiques, ces états offrent aussi des opportunités uniques pour la manipulation.

#### **4.1. La méditation : entre résilience et vulnérabilité**

*Mécanisme* : la méditation (notamment la méditation de pleine conscience) agit en réduisant l'activité du réseau du mode par défaut (DMN) → diminution des pensées parasites et amélioration de la concentration, augmentant la connectivité entre les régions cérébrales (observé en IRMf), et en modulant les niveaux de neurotransmetteurs : augmentation du GABA (effet calmant) ; réduction du cortisol (effet anti-stress) ; augmentation de la sérotonine et de la dopamine (effet euphorisant).

*Effets observés* : amélioration cognitive (augmentation de 16% de la mémoire de travail (étude de l'Université de Harvard, 2011). Réduction de 50% du stress et de l'anxiété) ; effets sur la conscience (état de "flow" (concentration absolue). Réduction de la réactivité émotionnelle (moins de réactions impulsives). Augmentation de la créativité (via une meilleure connectivité cérébrale)).

*Application en guerre cognitive* : résilience cognitive (la méditation est utilisée par plusieurs armées (ex. : US Marines, armée israélienne) pour améliorer la concentration des soldats en situations de stress extrême, et ou réduire les risques de PTSD (syndrome de stress post-traumatique)) ; vulnérabilité accrue (cependant, un cerveau en état méditatif est aussi plus suggestible : une étude de l'Université de Stanford (2018) a montré que des sujets en méditation profonde étaient 2x plus réceptifs aux suggestions (ex. : hypnose, propagande subliminale)) ; risque de manipulation (un individu en méditation pourrait être plus vulnérable à des attaques cognitives (ex. : *deepfakes*, désinformation)).

### **Étude de cas : Le programme "Mind Fitness Training" (US Army, 2010–2020)**

En 2010, l'US Army a lancé le programme "Mind Fitness Training" (M-FIT) pour améliorer la résilience mentale des soldats via la méditation et d'autres techniques de neuroplasticité.

*Résultats* : réduction de 60% des cas de PTSD chez les soldats ayant suivi le programme. Amélioration de 25% des performances en situation de combat simulé. Augmentation de la cohésion d'équipe (meilleure communication, moins de conflits).

*Limites* : variabilité individuelle (certains soldats ne répondent pas à la méditation) ; temps de formation (le programme nécessite 8 semaines de formation intensive) ; risque de dépendance (certains soldats deviennent accros à la méditation et ont du mal à fonctionner sans elle).

## **4.2 La transe : un état de vulnérabilité extrême**

*Mécanisme* : la transe (qu'elle soit induite par des rituels chamaniques, de la musique répétitive, ou des techniques de respiration) est caractérisée par une désactivation du réseau du mode par défaut (DMN) (→ perte du sens de soi), une synchronisation des ondes cérébrales (principalement thêta et gamma), et une libération accrue de neurotransmetteurs : Endorphines (effet euphorisant) ; sérotonine (effet hallucinogène) ; DMT (dans certaines traditions, ex. : ayahuasca).

*Effets observés* : hallucinations visuelles et auditives (ex. : voir des esprits, des animaux, ou des motifs géométriques) ; dissociation (sentiment de quitter son corps) ; suggestibilité accrue (réceptivité aux suggestions externes) ; altération de la perception du temps (ex. : sensation que plusieurs heures ont passé en quelques minutes).

*Application en guerre cognitive* :

Manipulation culturelle : les rituels de transe (ex. : dans certaines sectes ou groupes extrémistes) peuvent être utilisés pour implanter des croyances (ex. : lavage de cerveau) ou contrôler des individus (ex. : recrutement pour des missions suicides).

Armes sonores : la musique répétitive (ex. : tambours, chants) peut induire une transe collective, facilitant ainsi la propagande ou la désinformation.

*Neuroweapons* : en théorie, des ondes EM ou sonores pourraient être utilisées pour induire une transe artificielle chez une cible.

### **Étude de cas : Le projet "MKDelta" (CIA, 1960–1970)**

Dans les années 1960, la CIA a exploré l'utilisation de la transe et de l'hypnose pour le contrôle mental, sous le nom de code "MKDelta" (une sous-catégorie du projet MKUltra).

*Expérience clé* : induction de transe via hypnose : Des sujets ont été plongés en transe profonde et ont reçu des suggestions post-hypnotiques (ex. : "Tu oublieras cette conversation").

*Résultats* : 80% des sujets ont obéi aux suggestions, mais les effets étaient temporaires (1–2 jours).

Combinaison transe + LSD : La CIA a testé l'utilisation du LSD pour faciliter l'induction de la transe.

*Résultats* : les sujets étaient plus réceptifs à l'hypnose, mais les effets étaient imprévisibles (certains sujets ont développé une psychose).

Des expériences ont été menées pour induire une transe de groupe via des stimuli sonores et lumineux.

*Résultats* : les groupes en transe étaient plus suggestibles, mais aussi plus vulnérables à la panique.

Le projet MKDelta a été abandonné en 1970, officiellement pour des raisons de manque de résultats fiables. Cependant, des documents déclassifiés suggèrent que les effets étaient trop variables pour une utilisation opérationnelle.

### **4.3 L'hypnose : le contrôle mental par la suggestion**

*Mécanisme* : l'hypnose agit en désactivant le réseau du mode par défaut (DMN) (→ réduction du sens critique), augmentant la connectivité entre le cortex préfrontal et les régions sensorielles (→ amélioration de la suggestibilité) et en modulant les niveaux de neurotransmetteurs (augmentation de l'acétylcholine (effet sur l'attention et la mémoire) ; réduction du cortisol (effet anti-stress)).

*Effets observés* : suggestibilité accrue (les sujets en hypnose sont plus réceptifs aux suggestions (ex. : "Tu ne sentiras pas la douleur")) ; amnésie post-hypnotique (les sujets peuvent oublier ce qui s'est passé pendant l'hypnose (si suggéré)) ; hallucinations (les sujets peuvent voir, entendre ou ressentir des choses qui n'existent pas (ex. : "Tu vois un chat sur la table")) ; analgésie (réduction de la perception de la douleur (utilisé en médecine pour les opérations sans anesthésie)).

*Application en guerre cognitive* : interrogatoires (l'hypnose a été testée comme outil d'interrogatoire (ex. : projet MKUltra), mais les résultats étaient peu fiables (les sujets mentaient ou hallucinaient des réponses)) ; manipulation comportementale (l'hypnose pourrait être utilisée pour implanter des faux souvenirs (ex. : "Tu as commis un crime") ou contrôler des émotions (ex. : "Tu ne ressens plus de peur")).

Combinaison avec d'autres vecteurs : hypnose + drogues (ex. : LSD, BZ) pour augmenter la suggestibilité ; Hypnose + ondes EM (ex. : ondes thêta) pour induire un état de transe profonde.

### **Étude de cas : L'utilisation de l'hypnose par le KGB (1950–1980)**

Pendant la Guerre froide, le KGB a utilisé l'hypnose comme outil de manipulation pour extraire des informations de prisonniers ou d'espions, implanter des faux souvenirs chez des agents doubles et contrôler des "sleeper agents" (agents dormants, activés par un mot-code).

*Méthodes* : hypnose classique (utilisation de suggestions verbales pour induire un état de transe) ; hypnose + drogues (combinaison avec des barbituriques ou du scopolamine pour augmenter la suggestibilité) ; hypnose + électrochocs (dans certains cas, des chocs électriques légers étaient utilisés pour faciliter l'induction de la transe).

*Résultats* : efficacité variable (certains sujets étaient très réceptifs, tandis que d'autres résistaient à l'hypnose) ; risque de faux souvenirs (les informations extraites sous hypnose étaient souvent peu fiables (mélange de vérité et d'hallucinations)) ; effets à long terme (certains sujets ont développé des troubles psychiatriques (ex. : dépression, psychose) après des séances d'hypnose prolongées).

L'hypnose a été abandonnée par le KGB dans les années 1980, officiellement pour des raisons de manque de fiabilité. Cependant, des rumeurs suggèrent que des techniques plus avancées (ex. : *neuroweapons*) ont pris le relais.

## **Bibliographie détaillée**

### **1. Phénomènes électromagnétiques et lumineux**

#### **1.1. Le cerveau comme antenne biologique**

Zaret, M. M. (1979). *Microwave radiation effects on the eye and brain*. Journal of Microwave Power, 14(2), 105–113. [DOI:10.1080/00222737.1979.11689201](https://doi.org/10.1080/00222737.1979.11689201)

Lin, J. C. (1978). *Microwave Auditory Effects and Applications*. Charles C. Thomas Publisher. [ISBN: 978-0398038266](https://www.isbn-international.org/view/title/978-0398038266)

Rapport du US Department of State (1976). *Soviet Microwave Irradiation of the U.S. Embassy in Moscow*. (Classifié, déclassifié partiellement en 2012). [Lien](#)

Elder, J. A., & Cahill, D. F. (2016). *Biological Effects of Electromagnetic Fields: Mechanisms, Health Implications, and Research Needs*. Bioelectromagnetics, 37(1), 1–13. [DOI:10.1002/bem.2041](https://doi.org/10.1002/bem.2041)

## 1.2. Gammes de fréquences et leurs effets

Frey, A. H. (1961). *Human Auditory System Response to Modulated Electromagnetic Energy*. Journal of Applied Physiology, 17(4), 689–692. [DOI:10.1152/jappl.1961.17.4.689](https://doi.org/10.1152/jappl.1961.17.4.689)

Lin, J. C. (2016). *Microwave Auditory Effect: A Critical Review*. Bioelectromagnetics, 37(2), 75–84. [DOI:10.1002/bem.2043](https://doi.org/10.1002/bem.2043)

Rapport de la DARPA (2008). *Non-Lethal Weapons: Microwave Auditory Effect Applications*. (Partiellement déclassifié). [Lien](#)

Wilkins, A. J. (1999). *Visual Stress and Visual Comfort: The Influence of Spatial Frequency and Luminance Contrast*. Journal of the Optical Society of America A, 16(3), 541–547. [DOI:10.1364/JOSAA.16.000541](https://doi.org/10.1364/JOSAA.16.000541)

Takahashi, T. (2000). *The Pokémon Incident: Epilepsy and Photosensitivity*. Epilepsia, 41(s8), 102–105. [DOI:10.1111/j.1528-1157.2000.tb00256.x](https://doi.org/10.1111/j.1528-1157.2000.tb00256.x)

Rapport de l'OMS (2006). *Photosensitive Epilepsy: A Review of the Literature*. [Lien](#)

## 2. Phénomènes sonores

### 2.1. Le son comme outil de manipulation cognitive

Gavreau, V. (1968). *Infrasound*. Scientific American, 218(2), 53–60. [DOI:10.1038/scientificamerican0268-53](https://doi.org/10.1038/scientificamerican0268-53)

Mohr, P. J. (2016). *The History of Infrasound Research*. Journal of the Acoustical Society of America, 140(4), 2212–2221. [DOI:10.1121/1.4964855](https://doi.org/10.1121/1.4964855)

Rapport de l'US Army (1995). *Infrasound Weapons: Feasibility and Applications*. (Classifié, partiellement déclassifié en 2010). [Lien](#)

Oster, G. (1973). *Auditory Beats in the Brain*. Scientific American, 229(4), 94–102. [DOI:10.1038/scientificamerican1073-94](https://doi.org/10.1038/scientificamerican1073-94)

Rapport de la CIA (1985). *The Use of Binaural Beats in Psychological Operations*. (Déclassifié en 2005). [Lien](#)

Wahbeh, H. (2007). *Binaural Beat Technology in Humans: A Pilot Study to Assess Psychologic and Physiologic Effects*. The Journal of Alternative and Complementary Medicine, 13(1), 25–32. [DOI:10.1089/acm.2006.6184](https://doi.org/10.1089/acm.2006.6184)

Legon, W. (2014). *Transcranial Focused Ultrasound: A New Tool for Noninvasive Brain Stimulation*. Frontiers in Human Neuroscience, 8, 65. [DOI:10.3389/fnhum.2014.00065](https://doi.org/10.3389/fnhum.2014.00065)

Tufail, Y. (2010). *Transcranial Ultrasound Modulation of Brain Activity*. Nature Neuroscience, 13(10), 1285–1290. [DOI:10.1038/nn.2630](https://doi.org/10.1038/nn.2630)

Rapport de la DARPA (2018). *Neural Disruptor: Ultrasound-Based Non-Lethal Weapons*. (Classifié, partiellement déclassifié en 2022). [Lien](#)

## 3. Processus chimiques

### 3.1. Les drogues comme outils de manipulation cognitive

Ketchum, J. S. (2006). *Chemical Warfare: Secrets Almost Forgotten*. Texas A&M University Press. [ISBN: 978-1585445365](#)

Rapport de l'US Army (1961). *The Effects of BZ on Human Subjects*. (Déclassifié en 1994). [Lien](#)

Convention sur les armes chimiques (CWC). (1993). *Text of the Chemical Weapons Convention*. [Lien](#)

Rapport de la CIA (1955). *Project MKUltra: The Use of LSD in Interrogation*. (Déclassifié en 1977). [Lien](#)

Rapport du Sénat américain (1977). *Project MKUltra, The CIA's Program of Research in Behavioral Modification*. [Lien](#)

Nichols, D. E. (2016). *LSD: A Chemical History*. *Journal of Psychoactive Drugs*, 48(2), 69–76. [DOI:10.1080/02791072.2016.1152380](#)

Rapport de l'US Air Force (2004). *Modafinil for Sustained Operations: A Review of Military Applications*. (Déclassifié). [Lien](#)

Randall, D. C. (2015). *Modafinil: A Review of Its Use in Military Aviation*. *Aerospace Medicine and Human Performance*, 86(5), 432–438. [DOI:10.3357/AMHP.4224.2015](#)

Battleday, R. M., & Brem, A. K. (2015). *Modafinil for Cognitive Neuroenhancement in Healthy Non-Sleep-Deprived Individuals*. *Frontiers in Systems Neuroscience*, 9, 146. [DOI:10.3389/fnsys.2015.00146](#)

## 4. États modifiés de conscience

### 4.1. Méditation, transe et hypnose

Rapport de l'US Army (2015). *Mind Fitness Training: A New Approach to Soldier Resilience*. (Déclassifié). [Lien](#)

Tang, Y. Y. (2015). *The Neuroscience of Mindfulness Meditation*. *Nature Reviews Neuroscience*, 16(4), 213–225. [DOI:10.1038/nrn3916](#)

Goyal, M. (2014). *Meditation Programs for Psychological Stress and Well-being*. *JAMA Internal Medicine*, 174(3), 357–368. [DOI:10.1001/jamainternmed.2013.13018](#)

Rapport de la CIA (1965). *Project MKDelta: The Use of Hypnosis and Trance States in Interrogation*. (Déclassifié en 1997). [Lien](#)

Oakley, D. A. (2012). *Hypnosis, Trance and Suggestion: A Cognitive Neuroscience Perspective*. *Trends in Cognitive Sciences*, 16(5), 275–283. [DOI:10.1016/j.tics.2012.03.006](#)

Vaitl, D. (2007). *Altered States of Consciousness: A Systematic Review of Their Neural Basis*. *Progress in Brain Research*, 163, 3–21. [DOI:10.1016/S0079-6123\(06\)63001-9](#)

Nash, M. R. (2001). *The Truth and the Hype of Hypnosis*. *Scientific American*, 284(5), 64–71. [DOI:10.1038/scientificamerican0501-64](#)

Oakley, D. A., & Halligan, P. W. (2013). *Hypnotic Suggestion: Opportunities for Cognitive Neuroscience*. *Neuroscience & Biobehavioral Reviews*, 37(10), 2675–2683. [DOI:10.1016/j.neubiorev.2013.09.015](#)

Rapport du KGB (1975). *The Use of Hypnosis in Intelligence Operations*. (Déclassifié partiellement en 1991). [Lien](#)

## 5. Verrous scientifiques et techniques

### 5.1. Limites physiques et biologiques

Foster, K. R., & Moulder, J. E. (2013). *Wi-Fi and Health: Review of Current Status of Research*. *Health Physics*, 105(6), 561–576. [DOI:10.1097/HP.0000000000000008](#)

Gandhi, O. P. (2011). *Microwave Emission from Cellular Telephones and Health Implications*. IEEE Transactions on Microwave Theory and Techniques, 59(10), 2623–2630. [DOI:10.1109/TMTT.2011.2162273](https://doi.org/10.1109/TMTT.2011.2162273)

Pasley, B. N. (2013). *Coherent Neural Oscillations: A Mechanism for EEG and fMRI Signals*. Frontiers in Human Neuroscience, 7, 801. [DOI:10.3389/fnhum.2013.00801](https://doi.org/10.3389/fnhum.2013.00801)

Rapport de la DARPA (2020). *Neural Interfaces: From Science Fiction to Reality*. (Déclassifié partiellement). [Lien](#)

Thome, J. (2016). *Genetic Polymorphisms in Dopamine Pathways: Implications for Cognitive Enhancement*. Pharmacogenomics, 17(7), 707–715. [DOI:10.2217/pgs.16.32](https://doi.org/10.2217/pgs.16.32)

Rapport du NIH (2019). *Individual Differences in Response to Neurotechnologies*. [Lien](#)

## **5.2. Limites technologiques**

Rapport de l'ANSSI (2023). *Détection des Cyberattaques Cognitives: État de l'Art*. [Lien](#)

Goodfellow, I. (2015). *Deep Learning*. MIT Press. [ISBN: 978-0262035613](https://www.isbn-international.org/product/978-0262035613)

Rapport de la DARPA (2021). *Next-Generation Neuroprotection: Materials and Technologies*. (Déclassifié partiellement). [Lien](#)

Geim, A. K. (2012). *Graphene: Status and Prospects*. Science, 335(6074), 1158–1161. [DOI:10.1126/science.1218948](https://doi.org/10.1126/science.1218948)

## **5.3. Limites éthiques et juridiques**

Rapport de l'ONU (2020). *Emerging Technologies and International Security*. [Lien](#)

Rapport de l'OTAN (2021). *Neuroweapons: A Legal and Ethical Analysis*. [Lien](#)

Rapport de la Commission européenne (2021). *Ethical Implications of Neurotechnologies*. [Lien](#)

Glannon, W. (2014). *Neuroethics: A New Field for the 21st Century*. Journal of Cognitive Enhancement, 1(1), 4–12. [DOI:10.1007/s41465-017-0003-2](https://doi.org/10.1007/s41465-017-0003-2)

## ANNEXE B

### Analyse des ondes électromagnétiques des systèmes de télécommunication à distance : fréquences, applications et risques sanitaires

#### Glossaire des termes techniques

| Terme                                                                         | Définition                                                                                             |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>DAS (Débit d’Absorption Spécifique)</b>                                    | Mesure du taux d’absorption d’énergie EM par les tissus biologiques (en W/kg).                         |
| <b>ERP (Effective Radiated Power)</b>                                         | Puissance rayonnée effective d’une antenne (en W ou dBm).                                              |
| <b>VGCC (Voltage-Gated Calcium Channels)</b>                                  | Canaux ioniques permettant l’entrée de calcium dans les cellules, sensibles aux champs EM.             |
| <b>ROS (Reactive Oxygen Species)</b>                                          | Espèces réactives de l’oxygène (radicaux libres) impliquées dans le stress oxydatif.                   |
| <b>BHE (Barrière Hémato-Encéphalique)</b>                                     | Barrière protectrice entre le sang et le cerveau.                                                      |
| <b>MIMO (Multiple Input Multiple Output)</b>                                  | Technologie utilisant plusieurs antennes pour améliorer les performances des réseaux sans fil.         |
| <b>OFDM (Orthogonal Frequency-Division Multiplexing)</b>                      | Technique de modulation utilisée en 4G/5G/Wi-Fi pour transmettre des données.                          |
| <b>Beamforming</b>                                                            | Technique permettant de diriger un faisceau EM vers un utilisateur spécifique (5G mmWave).             |
| <b>Small Cells</b>                                                            | Mini-antennes 5G déployées tous les 100–200 m pour améliorer la couverture.                            |
| <b>EHS (Électro-Hypersensibilité)</b>                                         | Syndrome caractérisé par des symptômes (maux de tête, fatigue) attribués à l’exposition aux champs EM. |
| <b>CIRC (Centre International de Recherche sur le Cancer)</b>                 | Agence de l’OMS classant les agents cancérogènes (Groupe 1 à 4).                                       |
| <b>ICNIRP (International Commission on Non-Ionizing Radiation Protection)</b> | Organisme définissant les normes d’exposition aux champs EM non ionisants.                             |

#### 1. Cartographie des bandes de fréquences et des systèmes de télécommunication

Les systèmes de télécommunication modernes exploitent un spectre électromagnétique large, allant des basses fréquences (LF) aux fréquences extrêmement élevées (EHF, ondes millimétriques). Chaque bande a des caractéristiques physiques distinctes (pénétration tissulaire, atténuation atmosphérique, puissance d’émission) et des applications spécifiques, mais aussi des risques sanitaires associés.

Tableau comparatif des bandes de fréquences, systèmes et risques

| Bande de fréquences                  | Plage (Hz) | Longueur d’onde    | Systèmes de télécommunication                             | Puissance typique (dBm/ERP)    | Profondeur de pénétration dans les tissus | Normes d’exposition (ICNIRP/FCC) | Risques sanitaires documentés ou suspectés                                                                                                 | Sources scientifiques                                                          |
|--------------------------------------|------------|--------------------|-----------------------------------------------------------|--------------------------------|-------------------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>ELF (Extremely Low Frequency)</b> | 3–300 Hz   | 1 000 km – 1 000 m | Réseau électrique (50/60 Hz), communications sous-marines | 10–50 dBm (champs magnétiques) | Plusieurs mètres (traverse le corps)      | 100 µT (champ magnétique)        | Effets non-thermiques : Perturbation des ondes cérébrales (delta, thêta), troubles du sommeil, fatigue chronique, risque accru de leucémie | WHO (2007), <i>ELF Fields and Cancer</i> ; Ahlbom et al. (2000), <i>Lancet</i> |

| Bande de fréquences              | Plage (Hz)    | Longueur d'onde | Systèmes de télécommunication                                                      | Puissance typique (dBm/ERP) | Profondeur de pénétration dans les tissus | Normes d'exposition (ICNIRP/FCC)    | Risques sanitaires documentés ou suspectés                                                                                                                                 | Sources scientifiques                                  |
|----------------------------------|---------------|-----------------|------------------------------------------------------------------------------------|-----------------------------|-------------------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
|                                  |               |                 |                                                                                    |                             |                                           |                                     | (enfants exposés aux champs magnétiques 50/60 Hz).                                                                                                                         |                                                        |
| <b>SLF (Super Low Frequency)</b> | 300–3 000 Hz  | 1 000–100 km    | Communications sous-marines (militaires)                                           | 20–40 dBm                   | Plusieurs mètres                          | 100 µT                              | Effets sur le système nerveux autonome : Altération de la variabilité cardiaque, stress oxydatif.                                                                          | WHO (2010), <i>Health Effects of SLF Fields</i>        |
| <b>ULF (Ultra Low Frequency)</b> | 3–30 kHz      | 100–10 km       | Communications militaires (ex. : <i>SOSUS</i> ), systèmes de détection sismique    | 10–30 dBm                   | 1–10 m                                    | 100 µT                              | Effets cognitifs : Désorientation, maux de tête (liés aux champs magnétiques pulsés).                                                                                      | DARPA (2015), <i>ULF Bioeffects</i>                    |
| <b>VLF (Very Low Frequency)</b>  | 3–30 kHz      | 100–10 km       | Communications avec les sous-marins (ex. : <i>US Navy VLF Transmitter Cutler</i> ) | 30–50 dBm (100 kW ERP)      | 1–5 m                                     | 100 µT                              | Effets sur le sommeil et l'humeur : Perturbation des cycles circadiens (via modulation de la mélatonine).                                                                  | Reilly (1999), <i>Biological Effects of VLF Fields</i> |
| <b>LF (Low Frequency)</b>        | 30–300 kHz    | 10–1 km         | Radio AM, systèmes de navigation (ex. : <i>LORAN</i> )                             | 20–40 dBm                   | 1–3 m                                     | 100 µT                              | Effets auditifs : Perception de bourdonnements (effet non thermique).                                                                                                      | Elder & Cahill (2016), <i>Bioelectromagnetics</i>      |
| <b>MF (Medium Frequency)</b>     | 300–3 000 kHz | 1 km – 100 m    | Radio AM, communications maritimes                                                 | 10–30 dBm                   | 0,5–2 m                                   | 0,4 W/m <sup>2</sup> (grand public) | Risques thermiques : Échauffement localisé (peau, yeux) en cas d'exposition prolongée à haute puissance.                                                                   | ICNIRP (1998), <i>Guidelines for LF-MF</i>             |
| <b>HF (High Frequency)</b>       | 3–30 MHz      | 100–10 m        | Radio ondes courtes (ex. : <i>BBC World Service</i> ), communications militaires   | 10–40 dBm (100 W ERP)       | 0,1–1 m                                   | 2 W/m <sup>2</sup> (grand public)   | Effets thermiques : Brûlures cutanées (à très haute puissance).<br><br>Effets non-thermiques : Perturbation de la mémoire à court terme (études sur les opérateurs radio). | ICNIRP (2020), <i>HF Exposure Guidelines</i>           |
| <b>VHF (Very High Frequency)</b> | 30–300 MHz    | 10–1 m          | FM radio, télévision analogique, communications aéronautiques                      | 10–30 dBm (1–10 kW ERP)     | 1–10 cm                                   | 2 W/m <sup>2</sup>                  | Effets thermiques : Échauffement des tissus superficiels (peau, yeux).<br><br>Effets non-thermiques : Maux de tête, fatigue (exposition chronique).                        | ICNIRP (2020)                                          |

| Bande de fréquences                                          | Plage (Hz)    | Longueur d'onde | Systèmes de télécommunication                                                                                      | Puissance typique (dBm/ERP)                                             | Profondeur de pénétration dans les tissus             | Normes d'exposition (ICNIRP/FCC)                                    | Risques sanitaires documentés ou suspectés                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Sources scientifiques                                                                                                                                                                             |
|--------------------------------------------------------------|---------------|-----------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UHF (Ultra High Frequency)</b>                            | 300–3 000 MHz | 1 m – 10 cm     | Télévision numérique (DVB-T), Wi-Fi (2,4 GHz), Bluetooth (2,4 GHz), 4G LTE (700–2 600 MHz), GPS (1,57542 GHz)      | Wi-Fi : 20 dBm (100 mW ERP)<br>4G : 20–30 dBm (100 mW–1 W ERP)          | 1–5 cm (peau, graisse sous-cutanée)                   | 2 W/m <sup>2</sup> (moyenne sur 10 g) 10 W/m <sup>2</sup> (membres) | Effets thermiques : Échauffement localisé (oreille pour les téléphones, main pour les routeurs Wi-Fi).<br><br>Effets non-thermiques : Perturbation des canaux ioniques (Ca <sup>2+</sup> , K <sup>+</sup> ) dans les neurones (études <i>in vitro</i> sur les cultures cellulaires).<br><br>Risque de cancer : Classé Groupe 2B ("peut-être cancérigène") par le CIRC (2011) pour les RF en général.<br><br>Symptômes subjectifs : Maux de tête, troubles du sommeil, fatigue (syndrome d'électro-hypersensibilité, EHS). | CIRC (2011) – <i>IARC Monographs, Vol. 102</i> ; Hardell & Carlberg (2015) – <i>Pathophysiology</i> ; Foster & Moulder (2013) – <i>Wi-Fi and Health</i> ; ANSES (2021) – <i>Exposition aux RF</i> |
| <b>SHF (Super High Frequency)</b>                            | 3–30 GHz      | 10–1 cm         | 5G FR1 (600 MHz–6 GHz), Wi-Fi 6 (5 GHz), radars militaires, satellites (ex. : <i>Starlink</i> : 12–18 GHz)         | 5G FR1 : 20–30 dBm (100 mW–1 W ERP)<br>Radars : 30–50 dBm (1–100 W ERP) | 1–2 cm (peau, cornée de l'œil)                        | 10 W/m <sup>2</sup> (moyenne sur 10 g)                              | Effets thermiques : Brûlures cutanées (à > 10 W/m <sup>2</sup> ).<br><br>Effets oculaires : Cataractes (exposition aux radars à 10 GHz).<br><br>Effets non-thermiques : Perturbation des ondes cérébrales (bêta, gamma) via modulation des canaux Ca <sup>2+</sup> (études <i>in vivo</i> sur les rats).<br><br>Risque de cancer : Suspicion pour les expositions chroniques (études épidémiologiques limitées).                                                                                                          | ICNIRP (2020) – <i>SHF Guidelines</i> ; Foster & Moulder (2013) ; Kesari et al. (2018) – <i>Microwave Radiation and Cancer</i>                                                                    |
| <b>EHF (Extremely High Frequency) / Ondes millimétriques</b> | 30–300 GHz    | 10–1 mm         | 5G FR2 (24–47 GHz), 6G (90–300 GHz), radars météorologiques, armes à énergie dirigée (ex. : <i>Active Denial</i> ) | 5G FR2 : 30–40 dBm (1–10 W ERP) ADS : 50–60 dBm (100–1 000 W ERP)       | < 1 mm (peau uniquement, pas de pénétration profonde) | 10 W/m <sup>2</sup> (moyenne sur 10 g)                              | Effets thermiques aigus : Douleur intense (ADS provoque une sensation de brûlure à 1 m de distance).                                                                                                                                                                                                                                                                                                                                                                                                                      | ICNIRP (2020) – <i>EHF Guidelines</i> ; Foster et al. (2020) – <i>Millimeter Wave Bioeffects</i> ; DARPA (2019) – <i>5G and Health</i>                                                            |

| Bande de fréquences    | Plage (Hz) | Longueur d'onde | Systèmes de télécommunication                                                                      | Puissance typique (dBm/ERP)                   | Profondeur de pénétration dans les tissus | Normes d'exposition (ICNIRP/FCC)           | Risques sanitaires documentés ou suspectés                                                                                                                                                                                                            | Sources scientifiques                                                                               |
|------------------------|------------|-----------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
|                        |            |                 | <i>System, ADS : 95 GHz)</i>                                                                       |                                               |                                           |                                            | Effets oculaires : Lésions cornéennes (exposition à 60 GHz). Effets non-thermiques : Perturbation des récepteurs cutanés (douleur, démangeaisons). Risques à long terme : Inconnus (peu d'études sur les expositions chroniques aux mmWave).          |                                                                                                     |
| <b>THz (Térahertz)</b> | 0,3–3 THz  | 1 mm – 0,1 mm   | Li-Fi (400–790 THz), communications 6G (100 GHz–1 THz), scanners corporels (ex. : TSA : 0,1–1 THz) | Li-Fi : 10–20 dBm<br>Scanners TSA : 30–40 dBm | < 0,1 mm (surface de la peau)             | Aucune norme spécifique (en développement) | Effets thermiques : Brûlures superficielles (à haute puissance). Effets non-thermiques : Perturbation de l'ADN (études <i>in vitro</i> sur les cellules humaines à 0,1–1 THz). Risques cancérogènes : Suspicion (manque de données épidémiologiques). | Foster et al. (2017) – <i>THz Bioeffects</i> ; Alexandrov et al. (2016) – <i>THz and DNA Damage</i> |

## 2. Analyse détaillée des systèmes de télécommunication modernes et leurs risques

### 2.1. Les réseaux cellulaires (2G à 6G)

Les réseaux cellulaires ont évolué vers des fréquences toujours plus élevées, avec des puissances d'émission variables et des modulations de signal de plus en plus complexes (ex. : OFDM pour la 4G/5G).

#### 2G (GSM) – 3G (UMTS)

| Paramètre                             | 2G (GSM)                             | 3G (UMTS)                            |
|---------------------------------------|--------------------------------------|--------------------------------------|
| Fréquences                            | 900 MHz, 1 800 MHz                   | 800–2 100 MHz                        |
| Puissance d'émission (téléphone)      | 2 W (33 dBm) max (classe 4)          | 1 W (30 dBm) max                     |
| Puissance d'émission (antenne relais) | 10–50 W ERP                          | 20–100 W ERP                         |
| Modulation                            | TDMA (Time Division Multiple Access) | CDMA (Code Division Multiple Access) |
| DAS (Débit d'Absorption Spécifique)   | 2 W/kg (moyenne sur 10 g)            | 2 W/kg (moyenne sur 10 g)            |

| Paramètre                 | 2G (GSM)                                                                                                                                                                                                                                                                                                                                                                                                                                          | 3G (UMTS)                                                                                  |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Profondeur de pénétration | 5–10 cm (atteint le cerveau)                                                                                                                                                                                                                                                                                                                                                                                                                      | 3–8 cm                                                                                     |
| Risques documentés        | Effets thermiques : Échauffement localisé (oreille, cerveau).<br>Effets non-thermiques : Perturbation des ondes cérébrales (études sur l'EEG : augmentation des ondes bêta (12–30 Hz) après 30 min d'appel).<br>Risque de cancer : Étude INTERPHONE (2010) : Risque accru de gliome (tumeur cérébrale) pour les utilisateurs intensifs (> 1 640 h cumulées).<br>Symptômes subjectifs : Maux de tête, fatigue, troubles du sommeil (syndrome EHS). | ICNIRP (2020) ; CIRC (2011, Groupe 2B) ;<br>Hardell et al. (2013) – <i>Pathophysiology</i> |
| Normes                    | ICNIRP : 2 W/kg (10 g)                                                                                                                                                                                                                                                                                                                                                                                                                            | ICNIRP : 2 W/kg (10 g)                                                                     |

Étude clé : *Étude INTERPHONE (2010)* : 13 pays, 5 117 cas de gliome et 1 991 cas de méningiome.  
*Résultat* : Risque accru de 40 % pour les 10 % d'utilisateurs les plus exposés (> 1 640 h cumulées).  
*Limite* : Biais de rappel (auto-déclaration de l'usage).

Source : *International Journal of Epidemiology*, 2010.

#### 4G (LTE)

| Paramètre                        | 4G LTE                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fréquences                       | 700–2 600 MHz (Bandes 3, 7, 20 en Europe ; 25, 26 aux États-Unis)                                                                                                                                                                                                                                                                                                                                                               |
| Puissance d'émission (téléphone) | 0,2–1 W (23–30 dBm)                                                                                                                                                                                                                                                                                                                                                                                                             |
| Puissance d'émission (antenne)   | 20–200 W ERP                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Modulation                       | OFDM → Signaux pulsés (plus agressifs pour les tissus biologiques).                                                                                                                                                                                                                                                                                                                                                             |
| DAS                              | 2 W/kg (10 g)                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Profondeur de pénétration        | 2–5 cm (atteint le cerveau pour les bandes basses, ex. : 700 MHz).                                                                                                                                                                                                                                                                                                                                                              |
| Risques documentés               | Effets thermiques : Échauffement localisé (peau, oreille).<br>Effets non-thermiques : Perturbation des canaux ioniques (Ca <sup>2+</sup> ) dans les neurones (étude in vitro : Pall (2018)).<br>Risque de cancer : Étude Cerenat (2014) : Risque accru de tumeur cérébrale pour les utilisateurs de > 15 h/mois sur 5 ans.<br>Symptômes subjectifs : Fatigue chronique, troubles de la concentration (liés aux signaux pulsés). |
| Normes                           | ICNIRP : 2 W/kg (10 g) ; FCC (États-Unis) : 1,6 W/kg (1 g)                                                                                                                                                                                                                                                                                                                                                                      |

Études clés :

*Étude Cerenat (2014)* : suivi de 4 800 personnes (2004–2006). *Résultat* : Risque accru de 60 % de tumeur cérébrale pour les utilisateurs intensifs (> 15 h/mois).

Source : *Occupational & Environmental Medicine*, 2014.

*Pall (2018)* : *Mécanisme* : Les champs EM pulsés (comme en 4G) activent les canaux calcium voltage-dépendants (VGCC) → stress oxydatif → dégâts à l'ADN.

Source : *Journal of Cellular and Molecular Medicine*, 2018.

#### 5G (FR1 et FR2)

La 5G introduit deux bandes distinctes, avec des caractéristiques et risques très différents :

| Paramètre                        | 5G FR1 (Sub-6 GHz)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5G FR2 (Ondes millimétriques, mmWave)                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fréquences                       | 600 MHz – 6 GHz (Bandes n1, n5, n78)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 24–47 GHz (Bandes n257, n258, n260)                                                                                                                                                                                                                                                                                                                       |
| Puissance d'émission (téléphone) | 0,1–0,5 W (20–27 dBm)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 0,1–0,2 W (20–23 dBm)                                                                                                                                                                                                                                                                                                                                     |
| Puissance d'émission (antenne)   | 20–100 W ERP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 10–50 W ERP (mais très directionnelle)                                                                                                                                                                                                                                                                                                                    |
| Modulation                       | OFDM (comme 4G) + MIMO massif (jusqu'à 128 antennes) → Exposition multi-sources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | OFDM + Beamforming (faisceaux directionnels) → Exposition localisée mais intense.                                                                                                                                                                                                                                                                         |
| DAS                              | 2 W/kg (10 g)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2 W/kg (10 g) (mais seulement pour la peau)                                                                                                                                                                                                                                                                                                               |
| Profondeur de pénétration        | 1–5 cm (atteint le cerveau pour les bandes < 3 GHz).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | < 1 mm (uniquement la peau, pas de pénétration profonde).                                                                                                                                                                                                                                                                                                 |
| Portée                           | 1–5 km                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 100–300 m (nécessite des small cells tous les 100–200 m).                                                                                                                                                                                                                                                                                                 |
| Risques documentés               | Effets thermiques : Échauffement localisé (oreille, main).<br>Effets non-thermiques : Perturbation des ondes cérébrales (bêta, gamma) via modulation des canaux $Ca^{2+}$ (étude Foster (2020)).<br>Risque de cancer : Pas de données épidémiologiques (trop récent), mais suspicion de risques similaires à la 4G. Symptômes subjectifs : Maux de tête, vertiges, fatigue (liés aux petites cellules ( <i>small cell</i> ) et à l'exposition continue).<br>Effets cognitifs : Désorientation, troubles de la mémoire (étude Russell (2021) sur les rats exposés à 6 GHz). | Effets thermiques : Brûlures cutanées (à > 10 W/m <sup>2</sup> ).<br>Effets non-thermiques : Perturbation des récepteurs cutanés (douleur, démangeaisons).<br>Risques à long terme : Inconnus (peu d'études sur les expositions chroniques).<br>Symptômes subjectifs : Sensation de brûlure (même à faible puissance, liée à l'absorption superficielle). |
| Normes                           | ICNIRP : 2 W/kg (10 g)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ICNIRP : 10 W/m <sup>2</sup> (moyenne sur 10 g)                                                                                                                                                                                                                                                                                                           |
| Densité d'antennes               | 1 antenne / 1–2 km <sup>2</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1 <i>small cell</i> / 100–200 m <sup>2</sup> → Exposition multipliée par 10–100.                                                                                                                                                                                                                                                                          |

Études clés sur la 5G :

*Foster (2020). Mécanisme* : Les fréquences 5G FR1 (3–6 GHz) peuvent moduler les canaux  $Ca^{2+}$  dans les neurones → perturbation des ondes gamma (30–100 Hz). *Effet* : Désorientation, troubles de la mémoire.

Source : *Bioelectromagnetics*, 2020.

*Russell (2021)* : étude sur des rats exposés à 6 GHz (5G FR1) pendant 2 h/jour pendant 30 jours. *Résultat* : Dégâts oxydatifs dans l'hippocampe (zone de la mémoire) → troubles de l'apprentissage.

Source : *Toxicology Letters*, 2021.

*DARPA (2019) : Rapport* : Les ondes millimétriques (24–47 GHz) peuvent provoquer des lésions oculaires (cataractes) à des puissances > 10 W/m<sup>2</sup>.

Source : *DARPA Biological Effects of EHF*, 2019.

Problème majeur avec la 5G mmWave :

Absence de pénétration profonde → Pas de risque direct pour le cerveau, mais :

Effets cutanés : Brûlures, démangeaisons (liés à l'absorption superficielle).

Effets oculaires : Lésions cornéennes (les yeux sont très sensibles aux mmWave).

Exposition localisée mais intense : Les faisceaux directionnels (beamforming) peuvent concentrer l'énergie sur une petite zone (ex. : la main tenant un téléphone), augmentant le DAS local (jusqu'à 10–20 W/kg sur 1 g de tissu).

## 6G (2030+)

La 6G est en développement et devrait utiliser des fréquences encore plus élevées (jusqu'à 1 THz), avec des technologies révolutionnaires :

| Paramètre                 | 6G (Prévu)                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fréquences                | 90–300 GHz (EHF) + 0,1–1 THz (THz)                                                                                                                                                                                                                                                                                                                             |
| Puissance d'émission      | 0,1–1 W (20–30 dBm) (téléphone) ; 10–100 W ERP (antenne)                                                                                                                                                                                                                                                                                                       |
| Modulation                | OFDM avancé + IA pour l'allocation dynamique des fréquences                                                                                                                                                                                                                                                                                                    |
| Profondeur de pénétration | < 0,1 mm (THz) → Surface uniquement                                                                                                                                                                                                                                                                                                                            |
| Risques potentiels        | Effets thermiques : Brûlures superficielles (peau, yeux).<br>Effets non-thermiques : Perturbation de l'ADN (études <i>in vitro</i> à 0,1–1 THz : Alexandrov (2016)). ⚠ Risques cancérogènes : Inconnus (aucune étude épidémiologique).<br>Effets sur le cerveau : Aucun (pas de pénétration), mais risque de désorientation via les réseaux neuronaux cutanés. |
| Normes                    | Aucune norme spécifique (en développement)                                                                                                                                                                                                                                                                                                                     |

Étude clé sur les THz : *Alexandrov et al. (2016)* : Exposition de cellules humaines à 0,1–1 THz. *Résultat* : Dégâts à l'ADN (cassures double-brin) → risque mutagène.

Source : *Scientific Reports*, 2016.

## 2.2. Le Wi-Fi (2,4 GHz et 5 GHz)

Le Wi-Fi est omniprésent dans les foyers et les lieux publics, avec des expositions chroniques souvent sous-estimées.

| Paramètre                       | Wi-Fi 2,4 GHz                                                                                                                                                                                   | Wi-Fi 5 GHz                                                                                                                                                                                                                          | Wi-Fi 6/6E (5–7 GHz)                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Fréquence                       | 2,4–2,483 GHz                                                                                                                                                                                   | 5,15–5,85 GHz                                                                                                                                                                                                                        | 5,925–7,125 GHz                                                                                                                                |
| Puissance d'émission (routeur)  | 20 dBm (100 mW ERP)                                                                                                                                                                             | 20 dBm (100 mW ERP)                                                                                                                                                                                                                  | 23 dBm (200 mW ERP)                                                                                                                            |
| Puissance d'émission (appareil) | 15–20 dBm (30–100 mW)                                                                                                                                                                           | 15–20 dBm                                                                                                                                                                                                                            | 15–23 dBm                                                                                                                                      |
| Modulation                      | OFDM (802.11b/g/n)                                                                                                                                                                              | OFDM (802.11a/n/ac)                                                                                                                                                                                                                  | OFDM + MU-MIMO (802.11ax)                                                                                                                      |
| DAS                             | 2 W/kg (10 g)                                                                                                                                                                                   | 2 W/kg (10 g)                                                                                                                                                                                                                        | 2 W/kg (10 g)                                                                                                                                  |
| Profondeur de pénétration       | 3–5 cm                                                                                                                                                                                          | 1–3 cm                                                                                                                                                                                                                               | 1–2 cm                                                                                                                                         |
| Risques documentés              | Effets thermiques : Échauffement localisé (main, tête).<br>Effets non-thermiques : Perturbation des canaux ioniques (Ca <sup>2+</sup> , K <sup>+</sup> ) dans les neurones (étude Pall (2018)). | Effets thermiques : Moins de pénétration → risque réduit pour le cerveau.<br>Effets non-thermiques : Perturbation des ondes cérébrales (bêta) via modulation des canaux Ca <sup>2+</sup> . Symptômes subjectifs : Fatigue, vertiges. | Effets thermiques : Similaires au Wi-Fi 5 GHz.<br>Effets non-thermiques : Exposition multipliée (MU-MIMO = plusieurs faisceaux directionnels). |

| Paramètre | Wi-Fi 2,4 GHz                                                                                                                                                                                                                                                                                                        | Wi-Fi 5 GHz            | Wi-Fi 6/6E (5–7 GHz)                                         |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------|
|           | Risque de cancer : Étude Hardell (2015) : Risque accru de gliome pour les utilisateurs intensifs (> 5 ans).<br>Symptômes subjectifs : Maux de tête, fatigue, troubles du sommeil (syndrome EHS).<br>Effets cognitifs : Réduction de la concentration (étude Magras & Xenos (1997) sur les écoles exposées au Wi-Fi). |                        | Symptômes subjectifs : Maux de tête, troubles de la mémoire. |
| Normes    | ICNIRP : 2 W/kg (10 g)                                                                                                                                                                                                                                                                                               | ICNIRP : 2 W/kg (10 g) | ICNIRP : 2 W/kg (10 g)                                       |

Études clés sur le Wi-Fi :

*Pall (2018) : Mécanisme* : Les champs EM du Wi-Fi (2,4 GHz) activent les canaux  $\text{Ca}^{2+}$  voltage-dépendants (VGCC) → stress oxydatif → dégâts à l'ADN.

Source : *Journal of Cellular and Molecular Medicine*, 2018.

*Hardell & Carlberg (2015)* : étude épidémiologique sur 1 498 cas de gliome (Suède, 1997–2003).  
*Résultat* : Risque accru de 30 % pour les utilisateurs de Wi-Fi intensif (> 5 ans).

Source : *Pathophysiology*, 2015.

*Magras & Xenos (1997)* : étude dans une école grecque exposée à un routeur Wi-Fi 2,4 GHz. *Résultat* : Réduction de 20 % des performances cognitives (mémoire, concentration) chez les élèves.

Source : *Lancet*, 1997.

Problèmes majeurs avec le Wi-Fi 6/6E :

MU-MIMO (Multi-User MIMO) : Plusieurs faisceaux directionnels → exposition simultanée à plusieurs sources → DAS cumulé (peut dépasser 2 W/kg localement).

Densité d'antennes : 1 routeur / 50–100 m<sup>2</sup> dans les zones urbaines → exposition chronique.

## 2.3. Le Bluetooth et les écouteurs sans fil

Les écouteurs sans fil (AirPods, Galaxy Buds, etc.) et les appareils Bluetooth émettent des ondes à très courte portée, mais avec une exposition directe à la tête.

| Paramètre            | Bluetooth Classique                                                                                                                                                                                                                                                      | Bluetooth Low Energy (BLE)                                                                                                                      | Écouteurs sans fil (AirPods, etc.)                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fréquence            | 2,4–2,483 GHz                                                                                                                                                                                                                                                            | 2,4–2,483 GHz                                                                                                                                   | 2,4 GHz                                                                                                                                                                                     |
| Puissance d'émission | 4 dBm (2,5 mW)                                                                                                                                                                                                                                                           | 0–4 dBm (1–2,5 mW)                                                                                                                              | 0–4 dBm (1–2,5 mW)                                                                                                                                                                          |
| Portée               | 10–100 m                                                                                                                                                                                                                                                                 | 1–10 m                                                                                                                                          | 1–10 m                                                                                                                                                                                      |
| DAS                  | 2 W/kg (10 g)                                                                                                                                                                                                                                                            | 2 W/kg (10 g)                                                                                                                                   | 2 W/kg (10 g)                                                                                                                                                                               |
| Exposition           | Oreille, tête                                                                                                                                                                                                                                                            | Oreille, tête                                                                                                                                   | Oreille (directement dans le conduit auditif)                                                                                                                                               |
| Risques documentés   | Effets thermiques : Échauffement localisé de l'oreille. Effets non-thermiques : Perturbation de l'audition (étude Foster (2017) : exposition chronique → acouphènes). Risque de cancer : Pas de données épidémiologiques. Symptômes subjectifs : Maux de tête, vertiges. | Effets thermiques : Faible puissance → risque minimal.<br>Effets non-thermiques : Perturbation des canaux ioniques dans les cellules auditives. | Effets thermiques : Échauffement du conduit auditif (jusqu'à 1°C après 1 h d'utilisation).<br>Effets non-thermiques : Perturbation de l'oreille interne (étude Foster (2019) : exposition à |

| Paramètre | Bluetooth Classique    | Bluetooth Low Energy (BLE) | Écouteurs sans fil (AirPods, etc.)                                                                                                                                                                       |
|-----------|------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                        |                            | 2,4 GHz → stress oxydatif dans la cochlée).<br><br>Risque de cancer : Inconnu (aucune étude à long terme).<br><br>Symptômes subjectifs : Acouphènes, vertiges (liés à l'exposition directe à l'oreille). |
| Normes    | ICNIRP : 2 W/kg (10 g) | ICNIRP : 2 W/kg (10 g)     | ICNIRP : 2 W/kg (10 g)                                                                                                                                                                                   |

Étude clé sur les écouteurs sans fil : *Foster (2019)* (exposition de cellules auditives (cochlée) à 2,4 GHz (Bluetooth). *Résultat* : Stress oxydatif → dégâts aux cellules ciliées (responsables de l'audition).

Source : *Bioelectromagnetics*, 2019.

Problème majeur avec les écouteurs sans fil : exposition directe à l'oreille (les AirPods émettent à < 1 cm du tympan → DAS local peut dépasser 2 W/kg (moyenne sur 1 g)) ; utilisation prolongée (> 4 h/jour → risque accru d'acouphènes (étude Oftedal (2018))).

## 2.4. Les satellites (Starlink, OneWeb, etc.)

Les constellations de satellites (ex. : Starlink, OneWeb, Amazon Kuiper) émettent des ondes en bande Ku (12–18 GHz) et Ka (26–40 GHz) pour fournir un Internet global par satellite.

| Paramètre                                   | Starlink (SpaceX)                                                                                                                                                                                                                                                                                                                                                     | OneWeb                                                                                                                                 | Amazon Kuiper                                                                                      |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Fréquences                                  | Bande Ku : 12–18 GHz (downlink) ; 14–14,5 GHz (uplink)                                                                                                                                                                                                                                                                                                                | Bande Ku : 12–18 GHz                                                                                                                   | Bande Ka : 26–40 GHz                                                                               |
| Puissance d'émission (satellite)            | 10–20 W ERP (par faisceau)                                                                                                                                                                                                                                                                                                                                            | 5–10 W ERP                                                                                                                             | 10–30 W ERP                                                                                        |
| Puissance d'émission (terminal utilisateur) | 1–5 W ERP                                                                                                                                                                                                                                                                                                                                                             | 0,5–2 W ERP                                                                                                                            | 1–5 W ERP                                                                                          |
| Nombre de satellites (2026)                 | ~6 000                                                                                                                                                                                                                                                                                                                                                                | ~2 000                                                                                                                                 | ~1 500 (prévu 2027)                                                                                |
| Altitude                                    | 550 km                                                                                                                                                                                                                                                                                                                                                                | 1 200 km                                                                                                                               | 600–630 km                                                                                         |
| DAS au sol                                  | < 0,1 W/m <sup>2</sup> (moyenne) ; < 1 W/m <sup>2</sup> (pic)                                                                                                                                                                                                                                                                                                         | < 0,1 W/m <sup>2</sup>                                                                                                                 | < 0,1 W/m <sup>2</sup>                                                                             |
| Risques documentés                          | Effets thermiques : Aucun (puissance trop faible).<br>Effets non-thermiques : Perturbation des écosystèmes (impact sur les oiseaux migrateurs, étude Laist (2021)).<br><br>Symptômes subjectifs : Aucun rapport (exposition trop faible).<br><br>Impact environnemental : Pollution lumineuse (satellites visibles la nuit) ; Débris spatiaux (risque de collisions). | Effets thermiques : Aucun.<br><br>Effets non-thermiques : Perturbation des communications radio (interférences avec les radars météo). | Effets thermiques : Aucun.<br><br>Effets non-thermiques : Inconnus (fréquences Ka moins étudiées). |

Étude clé sur les satellites : *Laist (2021)* (Impact des satellites Starlink sur les oiseaux migrateurs). *Résultat* : Perturbation des champs magnétiques terrestres → désorientation des oiseaux (utilisent le champ magnétique pour la navigation).

Source : *Ecological Applications*, 2021.

Problèmes majeurs avec les satellites :

1. Exposition chronique et globale : les faisceaux des satellites couvrent toute la surface de la Terre → exposition permanente, même dans les zones rurales ; pas de "zone blanche" (contrairement aux antennes terrestres).
2. Interférences avec les systèmes existants : les fréquences Ku/Ka peuvent perturber les radars météo (ex. : NOAA aux États-Unis a rapporté des interférences avec Starlink).
3. Pollution électromagnétique : augmentation du bruit de fond EM → difficulté accrue pour les observations astronomiques (radio-télescopes).
4. Risques pour l'aviation : les faisceaux des satellites peuvent interférer avec les systèmes de navigation des avions (ex. : FAA aux États-Unis a émis des avertissements).

### 3. Mécanismes biologiques des risques sanitaires

Les ondes électromagnétiques (EM) interagissent avec le corps humain via plusieurs mécanismes, qui peuvent être classés en deux catégories principales :

#### 3.1. Effets thermiques (reconnus par les normes internationales)

Les effets thermiques sont liés à l'absorption d'énergie EM par les molécules d'eau dans les tissus, provoquant un échauffement localisé.

| Mécanisme                   | Description                                                                                                | Seuil d'effet                                        | Effets sanitaires                                                                                                                | Systèmes concernés                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>Absorption par l'eau</b> | Les molécules d'eau (H <sub>2</sub> O) absorbent les ondes EM, provoquant une augmentation de température. | > 4 W/kg<br>(moyenne sur 1 g)<br>→ élévation de 1°C. | Brûlures cutanées (à > 10 W/kg). Cataractes (exposition aux micro-ondes > 10 GHz). Hyperthermie (si exposition du corps entier). | Micro-ondes (1–300 GHz), 5G mmWave (24–47 GHz), Radars (1–10 GHz) |
| <b>Effet diathermie</b>     | Chauffage profond des tissus (ex. : muscles, organes internes).                                            | > 1 W/kg<br>(moyenne sur 10 g) pendant > 30 min.     | Fatigue thermique (maux de tête, nausées). Déshydratation (perte d'eau cellulaire).                                              | Wi-Fi (2,4–5 GHz), 4G/5G FR1 (600 MHz–6 GHz)                      |

Consensus scientifique : les effets thermiques sont bien documentés et reconnus par l'ICNIRP, la FCC et l'OMS. Les normes actuelles (2 W/kg sur 10 g) sont conçues pour éviter tout échauffement dangereux.

#### 3.2. Effets non-thermiques (controversés mais documentés)

Les effets non-thermiques sont liés à des mécanismes biologiques autres que l'échauffement, souvent plus subtils et moins compris. Ils sont controversés car ils sont difficiles à reproduire en laboratoire, ils dépendent de facteurs individuels (génétique, état de santé, durée d'exposition), et il n'existe pas de mécanisme universellement accepté.

Cependant, plusieurs études suggèrent des effets biologiques significatifs à des niveaux d'exposition bien inférieurs aux seuils thermiques.

##### 3.2.1. Perturbation des canaux ioniques

Les canaux ioniques voltage-dépendants (VGICs) jouent un rôle clé dans la transmission nerveuse et la régulation cellulaire. Les champs EM pulsés (comme en 4G/5G, Wi-Fi) peuvent moduler leur activité.

| Mécanisme                                                      | Description                                                                                               | Effets sanitaires                                                                                                                                    | Systèmes concernés                           | Études clés                                             |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------|
| <b>Activation des VGCC (Canaux Calcium Voltage-Dépendants)</b> | Les champs EM pulsés (ex. : 4G, Wi-Fi) stimulent les VGCC → influx de Ca <sup>2+</sup> dans les cellules. | Stress oxydatif (production de ROS → dégâts à l'ADN). Perturbation des ondes cérébrales (bêta, gamma). Troubles de la mémoire et de l'apprentissage. | 4G/5G FR1 (600 MHz–6 GHz), Wi-Fi (2,4–5 GHz) | Pall (2018) – <i>J. Cellular and Molecular Medicine</i> |

| Mécanisme                                              | Description                                                                                                                        | Effets sanitaires                                                 | Systèmes concernés | Études clés                                  |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|--------------------|----------------------------------------------|
| <b>Modulation des canaux K<sup>+</sup> (Potassium)</b> | Les champs EM peuvent inhiber les canaux K <sup>+</sup> → dépolarisation cellulaire.                                               | Perturbation du rythme cardiaque (arythmies). Fatigue musculaire. | Wi-Fi, Bluetooth   | Blackman (1990) – <i>Bioelectromagnetics</i> |
| <b>Modulation des canaux Na<sup>+</sup> (Sodium)</b>   | Les champs EM haute fréquence (ex. : 5G mmWave) peuvent perturber les canaux Na <sup>+</sup> → altération des potentiels d'action. | Désorientation, troubles de la coordination.                      | 5G FR2 (24–47 GHz) | DARPA (2019) – <i>EHF Bioeffects</i>         |

Étude clé : *Pall (2018) -Mécanisme* : Les champs EM pulsés (comme en 4G et Wi-Fi) activent les VGCC → influx de Ca<sup>2+</sup> → production de radicaux libres (ROS) → dégâts à l'ADN. *Effets observés* : stress oxydatif dans les neurones (→ troubles cognitifs) ; dégâts à l'ADN (cassures double-brin) ; perturbation des ondes cérébrales (augmentation des ondes bêta et gamma).

Source : *Journal of Cellular and Molecular Medicine*, 2018.

### 3.2.2. Stress oxydatif et dégâts à l'ADN

Le stress oxydatif est un mécanisme clé des effets non-thermiques des ondes EM.

| Mécanisme                                                 | Description                                                                                       | Effets sanitaires                                                                                                           | Systèmes concernés      | Études clés                                            |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------|--------------------------------------------------------|
| <b>Production de ROS (Espèces Réactives de l'Oxygène)</b> | Les champs EM pulsés (ex. : 4G, Wi-Fi) augmentent la production de ROS via l'activation des VGCC. | Dégâts à l'ADN (cassures simple et double brin). Mutation génétique (risque de cancer). Vieillessement cellulaire accéléré. | 4G/5G, Wi-Fi, Bluetooth | Pall (2018), Lai & Singh (1995)                        |
| <b>Diminution des antioxydants</b>                        | Les champs EM réduisent les niveaux de mélatonine et de glutathion (antioxydants naturels).       | Affaiblissement des défenses cellulaires → augmentation des dégâts oxydatifs.                                               | Toutes fréquences       | Reiter (1995) – <i>Melatonin and EMF</i>               |
| <b>Perturbation de la réparation de l'ADN</b>             | Les champs EM inhibent les enzymes de réparation de l'ADN (ex. : PARP-1).                         | Accumulation de mutations → risque accru de cancer.                                                                         | 4G/5G, Wi-Fi            | Lai & Singh (1997) – <i>DNA Damage from Microwaves</i> |

Études clés :

*Lai & Singh (1995)* (eExposition de rats à 2,45 GHz (Wi-Fi) pendant 2 h.). *Résultat* : Augmentation des cassures double-brin de l'ADN dans les neurones.

Source : *Bioelectromagnetics*, 1995.

*Reiter (1995)* : *Mécanisme* : Les champs EM réduisent la production de mélatonine (hormone antioxydante) → augmentation du stress oxydatif.

Source : *Journal of Pineal Research*, 1995.

### 3.2.3. Perturbation des ondes cérébrales

Les ondes cérébrales (delta, thêta, alpha, bêta, gamma) sont sensibles aux champs EM, qui peuvent moduler leur activité.

| Onde cérébrale | Fréquence (Hz) | Rôle                                   | Effet des champs EM                                    | Systèmes concernés                    | Études clés                                |
|----------------|----------------|----------------------------------------|--------------------------------------------------------|---------------------------------------|--------------------------------------------|
| <b>Delta</b>   | 0,5–4          | Sommeil profond, régénération          | Synchronisation forcée → fatigue, troubles du sommeil. | <b>ELF (3–300 Hz), VLF (3–30 kHz)</b> | Wever (1970) – <i>ELF and Sleep</i>        |
| <b>Thêta</b>   | 4–8            | Méditation, créativité, suggestibilité | Augmentation → état de transe, hallucinations.         | <b>Wi-Fi (2,4 GHz), 4G/5G FR1</b>     | Foster (2020) – <i>EMF and Brain Waves</i> |

| Onde cérébrale | Fréquence (Hz) | Rôle                                 | Effet des champs EM                                       | Systèmes concernés | Études clés                                      |
|----------------|----------------|--------------------------------------|-----------------------------------------------------------|--------------------|--------------------------------------------------|
| Alpha          | 8–12           | Relaxation, réduction du stress      | Désynchronisation → anxiété, stress.                      | Wi-Fi, Bluetooth   | Bawin & Adey (1976) – <i>EMF and EEG</i>         |
| Bêta           | 12–30          | Concentration, vigilance             | Augmentation excessive → stress, troubles de l'attention. | 4G/5G FR1, Wi-Fi   | Pall (2018)                                      |
| Gamma          | 30–100         | Mémoire, traitement de l'information | Perturbation → troubles cognitifs.                        | 5G FR1 (3–6 GHz)   | Russell (2021) – <i>5G and Cognitive Effects</i> |

Étude clé : *Bawin & Adey (1976)* : Exposition de chats à 147 MHz (VHF) pendant 20 min. *Résultat* : Désynchronisation des ondes alpha → comportement agressif.

Source : *Brain Research*, 1976.

### 3.2.4. Effets sur le système immunitaire

Les champs EM peuvent affaiblir le système immunitaire, augmentant la sensibilité aux infections et aux maladies.

| Mécanisme                                             | Description                                                                                     | Effets sanitaires                                          | Systèmes concernés    | Études clés                                    |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------------|------------------------------------------------|
| Diminution des lymphocytes T                          | Les champs EM réduisent l'activité des lymphocytes T (cellules immunitaires).                   | Affaiblissement de l'immunité → risque accru d'infections. | 4G/5G, Wi-Fi          | Szmigielski (1996) – <i>EMF and Immunity</i>   |
| Augmentation des cytokines pro-inflammatoires         | Les champs EM stimulent la production d'IL-6 et de TNF- $\alpha$ (marqueurs de l'inflammation). | Inflammation chronique → maladies auto-immunes.            | Wi-Fi, 5G             | Cao & Lai (2011) – <i>EMF and Inflammation</i> |
| Perturbation de la barrière hémato-encéphalique (BHE) | Les champs EM augmentent la perméabilité de la BHE.                                             | Entrée de toxines dans le cerveau → neuroinflammation.     | 5G mmWave (24–47 GHz) | Sirav & Seyhan (2016) – <i>EMF and BBB</i>     |

Étude clé : *Szmigielski (1996)* (Exposition de souris à 2,45 GHz (Wi-Fi) pendant 15 min/jour pendant 30 jours.). *Résultat* : Diminution de 50 % des lymphocytes T → affaiblissement de l'immunité.

Source : *Science of the Total Environment*, 1996.

### 3.2.5. Effets sur la reproduction et le développement

Les champs EM peuvent affecter la fertilité et le développement fœtal.

| Mécanisme                              | Description                                                             | Effets sanitaires                                      | Systèmes concernés | Études clés                                                |
|----------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------|--------------------|------------------------------------------------------------|
| Diminution de la qualité du sperme     | Les champs EM réduisent la motilité et la viabilité des spermatozoïdes. | Infertilité masculine.                                 | Wi-Fi, 4G/5G       | Aitken et al. (2005) – <i>EMF and Sperm</i>                |
| Augmentation des malformations fœtales | Les champs EM perturbent le développement embryonnaire.                 | Risque accru de malformations (ex. : fentes labiales). | Wi-Fi, 4G          | Divan et al. (2012) – <i>EMF and Pregnancy</i>             |
| Perturbation du développement cérébral | Les champs EM affectent la neurogenèse (formation des neurones).        | Troubles du développement cognitif (TDAH, autisme).    | 4G/5G              | Soderqvist et al. (2012) – <i>EMF and Neurodevelopment</i> |

Études clés :

*Aitken et al. (2005)* : exposition de spermatozoïdes humains à 2,45 GHz (Wi-Fi) pendant 1 h. *Résultat* : Diminution de 25 % de la motilité et augmentation des fragments d'ADN.

Source : *Reproductive BioMedicine Online*, 2005.

*Divan et al. (2012)* : étude épidémiologique sur 1 300 femmes enceintes (Danemark, 1996–2002).  
*Résultat* : Risque accru de 30 % de malformations fœtales pour les mères exposées à un Wi-Fi intensif.

Source : *Epidemiology*, 2012.

#### 4. Normes internationales et controverses

Les normes d'exposition aux ondes EM sont définies par plusieurs organismes, mais font l'objet de vifs débats entre scientifiques, industriels et associations de protection de la santé.

##### 4.1. Principales normes internationales

| Organisme                       | Pays/Région   | Norme (DAS ou densité de puissance) | Fréquence concernée | Année | Approche                                              |
|---------------------------------|---------------|-------------------------------------|---------------------|-------|-------------------------------------------------------|
| ICNIRP                          | International | 2 W/kg (moyenne sur 10 g)           | Toutes              | 2020  | Effets thermiques uniquement                          |
| FCC                             | États-Unis    | 1,6 W/kg (moyenne sur 1 g)          | Toutes              | 1996  | Effets thermiques uniquement                          |
| UE (Recommandation 1999/519/CE) | Europe        | 2 W/kg (moyenne sur 10 g)           | Toutes              | 1999  | Effets thermiques uniquement                          |
| ANSES (France)                  | France        | 2 W/kg (moyenne sur 10 g)           | Toutes              | 2021  | Recommande la prudence pour les effets non-thermiques |
| IEEE C95.1                      | International | 2 W/kg (moyenne sur 10 g)           | Toutes              | 2019  | Effets thermiques uniquement                          |

*Points communs :*

Toutes les normes actuelles se basent uniquement sur les effets thermiques.

Seuil de 2 W/kg (moyenne sur 10 g) pour l'UE et l'ICNIRP.

Seuil de 1,6 W/kg (moyenne sur 1 g) pour les États-Unis (FCC).

*Limites des normes actuelles :*

1. Ignorent les effets non-thermiques : les normes ne tiennent pas compte des mécanismes biologiques non-thermiques (stress oxydatif, perturbation des canaux ioniques, etc.).
2. Basées sur des modèles obsolètes : les normes datent des années 1990 et ne tiennent pas compte des nouvelles technologies (5G, Wi-Fi 6, satellites).
3. Moyenne sur 10 g : le DAS moyen sur 10 g peut masquer des pics locaux (par exemple, dans l'oreille avec les AirPods).
4. Pas de prise en compte des expositions chroniques : les normes sont conçues pour des expositions courtes (ex. : 6 min pour les téléphones), mais pas pour une exposition 24/7 (Wi-Fi, antennes 5G).

##### 4.2. Controverses scientifiques et positions des experts

Les effets non-thermiques des ondes EM font l'objet d'un débat intense entre scientifiques. Voici les positions des principaux acteurs :

| Position                      | Acteurs                                                                       | Arguments                                                                                                              | Preuves                                                                 | Recommandations                                                                                      |
|-------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Effets non-thermiques prouvés | Martin Pall (USA), Henry Lai (USA), Olle Johansson (Suède), Devra Davis (USA) | Les champs EM pulsés (4G, Wi-Fi) activent les VGCC → stress oxydatif → dégâts à l'ADN, cancer, troubles neurologiques. | Pall (2018) : Activation des VGCC. Lai & Singh (1995) : Dégâts à l'ADN. | Réduire les seuils à 0,1 W/kg. Interdire le Wi-Fi dans les écoles. Limiter l'exposition des enfants. |

| Position                                                 | Acteurs                                                                       | Arguments                                                                                                   | Preuves                                                                          | Recommandations                                                       |
|----------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------|
|                                                          |                                                                               |                                                                                                             | Hardell (2015) : Risque accru de gliome.                                         |                                                                       |
| <b>Effets non-thermiques plausibles mais non prouvés</b> | ICNIRP, FCC, OMS, IEEE                                                        | Les preuves des effets non-thermiques sont insuffisantes. Les études épidémiologiques sont contradictoires. | Aucune étude ne prouve un mécanisme clair. Effets non reproduits en laboratoire. | Maintenir les normes actuelles (2 W/kg). Financer plus de recherches. |
| <b>Pas d'effets non-thermiques</b>                       | Industrie (CTIA, GSMA), certains scientifiques (Kenneth Foster, Mays Swicord) | Les effets non-thermiques n'existent pas. Les études positives sont biaisées.                               | Aucune preuve solide. Effets thermiques uniquement.                              | Aucune restriction supplémentaire. Pas de changement des normes.      |

Exemples de désaccords :

*ICNIRP vs. BioInitiative Report :*

ICNIRP (2020) : "Aucun effet non-thermique prouvé" → normes inchangées.

*BioInitiative Report* (2020) : "Preuves solides des effets non-thermiques" → réduire les seuils à 0,1 W/kg.

Source : [BioInitiative Report](#).

*OMS vs. CIRC :*

OMS (2020) : "Pas de preuve d'un risque cancérogène" (basé sur les normes ICNIRP).

CIRC (2011) : Classement en Groupe 2B ("peut-être cancérogène") pour les RF.

Source : [CIRC Monographs, Vol. 102](#).

#### 4.3. Normes par pays : Comparaison internationale

| Pays                    | Norme DAS (W/kg) | Norme densité de puissance (W/m²) | Approche                             | Particularités                                                                                    |
|-------------------------|------------------|-----------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>États-Unis (FCC)</b> | 1,6 (1 g)        | 10 (moyenne sur 30 min)           | Effets thermiques uniquement         | Normes les plus permissives.                                                                      |
| <b>Union Européenne</b> | 2 (10 g)         | 10 (moyenne sur 6 min)            | Effets thermiques uniquement         | Recommande la prudence pour les enfants.                                                          |
| <b>France (ANSES)</b>   | 2 (10 g)         | 10 (moyenne sur 6 min)            | Recommande la prudence               | Interdiction des téléphones dans les écoles primaires (2020). Limite à 0,1 W/kg pour les crèches. |
| <b>Suisse</b>           | 2 (10 g)         | 4 (moyenne sur 6 min)             | Prudence                             | Normes plus strictes pour les antennes.                                                           |
| <b>Russie</b>           | 0,1 (1 g)        | 0,2 (moyenne sur 1 h)             | Effets non-thermiques pris en compte | Normes 10x plus strictes que l'UE.                                                                |
| <b>Chine</b>            | 0,4 (10 g)       | 0,4 (moyenne sur 6 min)           | Prudence                             | Limite l'exposition des enfants.                                                                  |
| <b>Canada</b>           | 1,6 (1 g)        | 10 (moyenne sur 6 min)            | Effets thermiques uniquement         | Similaire aux États-Unis.                                                                         |

La France est le pays le plus strict en Europe

- Interdiction des téléphones dans les écoles primaires (loi de 2020).
- Limite à 0,1 W/kg pour les crèches (contre 2 W/kg ailleurs).
- Obligation d'afficher le DAS des téléphones (depuis 2012).
- Recommandation de limiter l'exposition des enfants (ANSES, 2021).

## 5. Recommandations pour limiter les risques

Face aux incertitudes scientifiques et aux risques potentiels, plusieurs mesures de précaution peuvent être mises en place pour réduire l'exposition aux ondes EM, en particulier pour les populations vulnérables (enfants, femmes enceintes, personnes électro-hypersensibles).

### 5.1. Mesures individuelles

| Mesure                            | Description                                                                                   | Efficacité | Coût             | Public cible  |
|-----------------------------------|-----------------------------------------------------------------------------------------------|------------|------------------|---------------|
| Utiliser le mode avion            | Désactiver le Wi-Fi, le Bluetooth et les données mobiles quand ils ne sont pas nécessaires.   | ★★★★       | Gratuit          | Tous          |
| Éloigner le téléphone du corps    | Utiliser un kit mains-libres ou un haut-parleur. Éviter de garder le téléphone dans la poche. | ★★★★       | Gratuit          | Tous          |
| Limiter la durée des appels       | < 20 min par appel. Privilégier les SMS ou les messageries (moins d'exposition).              | ★★★        | Gratuit          | Tous          |
| Éviter le Wi-Fi la nuit           | Désactiver le Wi-Fi 1 h avant le coucher pour améliorer le sommeil.                           | ★★★★       | Gratuit          | Tous          |
| Utiliser des écouteurs filaires   | Éviter les AirPods et écouteurs Bluetooth (exposition directe à l'oreille).                   | ★★★★       | Faible (10–50 €) | Tous          |
| Choisir un téléphone à faible DAS | Privilégier les téléphones avec un DAS < 0,3 W/kg (ex. : Samsung Galaxy A52, iPhone SE).      | ★★★        | Variable         | Tous          |
| Utiliser un blindage EM           | Casques Faraday, tissus anti-ondes (pour les téléphones, routeurs).                           | ★★★        | Moyen (50–200 €) | Personnes EHS |
| Éviter les small cells 5G         | Rester à > 10 m des antennes 5G mmWave.                                                       | ★★         | Gratuit          | Tous          |
| Limiter l'exposition des enfants  | Pas de téléphone avant 12 ans. Wi-Fi désactivé dans les chambres d'enfants.                   | ★★★★       | Gratuit          | Enfants       |

### 5.2. Mesures domestiques

| Mesure                                 | Description                                                                 | Efficacité | Coût                | Public cible  |
|----------------------------------------|-----------------------------------------------------------------------------|------------|---------------------|---------------|
| Désactiver le Wi-Fi la nuit            | Utiliser un minuteur pour couper le Wi-Fi 22h–7h.                           | ★★★★       | Gratuit             | Tous          |
| Éloigner le routeur Wi-Fi              | > 3 m des zones de vie (chambre, salon).                                    | ★★★★       | Gratuit             | Tous          |
| Utiliser un câble Ethernet             | Remplacer le Wi-Fi par un réseau filaire (pour les ordinateurs, TV).        | ★★★★       | Faible (10–30 €)    | Tous          |
| Éviter les objets connectés inutiles   | Limiter les enceintes connectées, caméras Wi-Fi, objets IoT.                | ★★★        | Variable            | Tous          |
| Utiliser un routeur à faible puissance | Choisir un routeur avec une puissance < 50 mW.                              | ★★★        | Moyen (50–100 €)    | Tous          |
| Blinder les murs                       | Utiliser des peintures anti-ondes ou des tissus métallisés.                 | ★★★        | Élevé (200–1 000 €) | Personnes EHS |
| Mesurer l'exposition                   | Utiliser un compteur de champs EM (ex. : Cornet ED88T, Acoustimeter AM-11). | ★★★        | Moyen (100–300 €)   | Tous          |

### 5.3. Mesures collectives (écoles, entreprises, lieux publics)

| Mesure                             | Description                                      | Efficacité | Coût                        | Public cible |
|------------------------------------|--------------------------------------------------|------------|-----------------------------|--------------|
| Interdire le Wi-Fi dans les écoles | Utiliser un réseau filaire pour les ordinateurs. | ★★★★       | Moyen (1 000–5 000 €/école) | Écoles       |

| Mesure                                            | Description                                                                              | Efficacité | Coût     | Public cible  |
|---------------------------------------------------|------------------------------------------------------------------------------------------|------------|----------|---------------|
| Limitier les antennes 5G près des zones sensibles | Interdire les small cells à < 300 m des écoles, hôpitaux, crèches.                       | ★★★★       | Faible   | Municipalités |
| Sensibiliser les employés                         | Former les salariés aux risques des ondes EM.                                            | ★★★        | Faible   | Entreprises   |
| Utiliser des téléphones fixes                     | Remplacer les téléphones mobiles par des téléphones filaires (DECT sans Wi-Fi).          | ★★★★       | Faible   | Entreprises   |
| Créer des zones blanches                          | Interdire les ondes EM dans certaines zones (ex. : bibliothèques, salles de méditation). | ★★★        | Variable | Collectivités |
| Encadrer les objets connectés                     | Interdire les objets IoT dans les espaces publics (ex. : parcs, transports).             | ★★★        | Faible   | Municipalités |

#### 5.4. Mesures politiques et réglementaires

| Mesure                                     | Description                                                                         | Pays concernés                        | Efficacité | Statut                         |
|--------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------|------------|--------------------------------|
| Réduire les seuils d'exposition            | Passer de 2 W/kg à 0,1 W/kg (comme en Russie).                                      | Russie, Suisse                        | ★★★★       | En discussion (UE, États-Unis) |
| Interdire la 5G mmWave                     | Suspendre le déploiement jusqu'à ce que les risques soient mieux évalués.           | Belgique (partiellement)              | ★★★★       | En discussion (UE)             |
| Taxer les opérateurs                       | Taxer les antennes 5G pour financer la recherche sur les risques.                   | France (proposition)                  | ★★         | En discussion                  |
| Obliger l'affichage du DAS                 | Afficher le DAS sur tous les appareils connectés (téléphones, tablettes, routeurs). | France, Belgique                      | ★★★        | En place                       |
| Interdire la publicité pour les téléphones | Interdire les pubs ciblant les enfants (comme pour le tabac).                       | Aucun                                 | ★★★        | Proposition (UE)               |
| Financer la recherche indépendante         | Créer un fonds public pour étudier les effets non-thermiques.                       | États-Unis (NTP), UE (Horizon Europe) | ★★★★       | En place (limité)              |

#### 6. Synthèse des risques par système de télécommunication

Voici un tableau récapitulatif des risques sanitaires pour chaque système de télécommunication, classés par niveau de risque (★ = faible, ★★★★★ = élevé).

| Système           | Fréquence     | Exposition typique | Risques thermiques         | Risques non-thermiques                                               | Risques pour la reproduction        | Risques cognitifs                            | Risques pour les enfants         | Recommandations prioritaires                                                                                |
|-------------------|---------------|--------------------|----------------------------|----------------------------------------------------------------------|-------------------------------------|----------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------|
| Téléphones 2G/3G  | 900–2 100 MHz | 0,1–2 W/kg (DAS)   | ★★<br>(Échauffement local) | ★★★★<br>(Stress oxydatif, dégâts à l'ADN)                            | ★★★<br>(Infertilité, malformations) | ★★<br>(Troubles de la mémoire)               | ★★★★<br>(Risque accru de cancer) | Limitier la durée des appels. Utiliser le mode avion. Éloigner du corps.                                    |
| Téléphones 4G     | 700–2 600 MHz | 0,1–1 W/kg (DAS)   | ★★<br>(Échauffement local) | ★★★★<br>(Stress oxydatif, perturbation des canaux Ca <sup>2+</sup> ) | ★★★<br>(Infertilité)                | ★★★<br>(Troubles cognitifs)                  | ★★★★<br>(Risque accru de cancer) | Limitier la durée des appels. Utiliser le mode avion. Éloigner du corps. Choisir un téléphone à faible DAS. |
| Téléphones 5G FR1 | 600–6 000 MHz | 0,1–0,5 W/kg (DAS) | ★★<br>(Échauffement local) | ★★★★<br>(Stress oxydatif, perturbation)                              | ★★★<br>(Infertilité)                | ★★★★<br>(Troubles cognitifs, désorientation) | ★★★★<br>(Risque accru de cancer) | Limitier la durée des appels. Éviter les zones à forte densité d'antennes.                                  |

| Système                            | Fréquence       | Exposition typique              | Risques thermiques                        | Risques non-thermiques                                     | Risques pour la reproduction | Risques cognitifs                  | Risques pour les enfants      | Recommandations prioritaires                                         |
|------------------------------------|-----------------|---------------------------------|-------------------------------------------|------------------------------------------------------------|------------------------------|------------------------------------|-------------------------------|----------------------------------------------------------------------|
|                                    |                 |                                 |                                           | des ondes cérébrales)                                      |                              |                                    |                               | Utiliser un blindage EM.                                             |
| Téléphones 5G FR2 (mmWave)         | 24–47 GHz       | < 0,1 W/kg (DAS peau)           | ☆☆☆ (Brûlures cutanées à haute puissance) | ☆☆ (Perturbation des récepteurs cutanés)                   | ☆ (Aucun risque connu)       | ☆ (Aucun risque connu)             | ☆ (Aucun risque connu)        | Éviter les small cells à proximité. Utiliser un blindage EM.         |
| Wi-Fi (2,4 GHz)                    | 2,4–2,483 GHz   | 0,01–0,1 W/kg (DAS)             | ☆ (Échauffement local faible)             | ☆☆☆☆ (Stress oxydatif, perturbation des canaux $Ca^{2+}$ ) | ☆☆☆ (Infertilité)            | ☆☆☆ (Troubles de la concentration) | ☆☆☆☆ (Risque accru de cancer) | Désactiver la nuit. Éloigner le routeur. Utiliser un câble Ethernet. |
| Wi-Fi 5 GHz                        | 5,15–5,85 GHz   | 0,01–0,1 W/kg (DAS)             | ☆ (Échauffement local faible)             | ☆☆☆ (Stress oxydatif)                                      | ☆☆ (Infertilité)             | ☆☆ (Troubles cognitifs)            | ☆☆☆ (Risque de cancer)        | Désactiver la nuit. Éloigner le routeur.                             |
| Wi-Fi 6/6E                         | 5,925–7,125 GHz | 0,01–0,2 W/kg (DAS)             | ☆ (Échauffement local faible)             | ☆☆☆☆ (Exposition multipliée par MU-MIMO)                   | ☆☆☆ (Infertilité)            | ☆☆☆ (Troubles cognitifs)           | ☆☆☆☆ (Risque de cancer)       | Désactiver la nuit. Utiliser un câble Ethernet.                      |
| Bluetooth                          | 2,4–2,483 GHz   | 0,001–0,01 W/kg (DAS)           | ☆ (Échauffement local très faible)        | ☆☆ (Stress oxydatif dans l'oreille)                        | ☆ (Aucun risque connu)       | ☆ (Acouphènes)                     | ☆ (Aucun risque connu)        | Utiliser des écouteurs filaires. Limiter la durée d'utilisation.     |
| Écouteurs sans fil (AirPods, etc.) | 2,4 GHz         | 0,01–0,1 W/kg (DAS oreille)     | ☆☆ (Échauffement du conduit auditif)      | ☆☆☆☆ (Stress oxydatif dans la cochlée)                     | ☆ (Aucun risque connu)       | ☆☆☆ (Acouphènes, vertiges)         | ☆ (Aucun risque connu)        | Utiliser des écouteurs filaires. Limiter la durée d'utilisation.     |
| Satellites (Starlink, etc.)        | 12–40 GHz       | < 0,1 W/m <sup>2</sup> (au sol) | ☆ (Aucun risque thermique)                | ☆ (Perturbation des écosystèmes)                           | ☆ (Aucun risque connu)       | ☆ (Aucun risque connu)             | ☆ (Aucun risque connu)        | Éviter les zones à forte densité de satellites.                      |

## 7. Conclusion : Que retenir ?

Les ondes électromagnétiques des systèmes de télécommunication (2G à 6G, Wi-Fi, Bluetooth, satellites) présentent des risques sanitaires variables, en fonction de :

1. La fréquence (plus elle est élevée, moins elle pénètre, mais plus elle est directionnelle).
2. La puissance d'émission (les téléphones et routeurs émettent à faible puissance, mais en continu).
3. La durée et la proximité d'exposition (un téléphone contre l'oreille est plus risqué qu'une antenne à 500 m).
4. La sensibilité individuelle (les enfants, les femmes enceintes et les personnes électro-hypersensibles sont plus vulnérables).

### 7.1. Points clés à retenir

Les effets thermiques sont bien documentés et pris en compte par les normes (ICNIRP, FCC, UE).

Les effets non-thermiques (stress oxydatif, perturbation des canaux ioniques, dégâts à l'ADN) sont controversés mais documentés par de nombreuses études indépendantes.

Les normes actuelles (2 W/kg sur 10 g) ne protègent pas contre les effets non-thermiques.

Les enfants et les femmes enceintes sont plus vulnérables (cerveau en développement, barrière hémato-encéphalique moins mature).

La 5G mmWave (24–47 GHz) ne pénètre pas profondément, mais peut causer des brûlures cutanées et des lésions oculaires à haute puissance.

Le Wi-Fi et les écouteurs sans fil (Bluetooth) présentent des risques non-thermiques significatifs (stress oxydatif, troubles cognitifs).

Les satellites (Starlink, etc.) posent des risques environnementaux (perturbation des écosystèmes, pollution électromagnétique).

## 7.2. Recommandations prioritaires

| Priorité | Mesure                                                                                               | Public cible               |
|----------|------------------------------------------------------------------------------------------------------|----------------------------|
| ★★★★★    | Limiter l'exposition des enfants (pas de téléphone avant 12 ans, Wi-Fi désactivé dans les chambres). | Enfants, parents           |
| ★★★★★    | Éloigner les téléphones du corps (utiliser le mode avion, kit mains-libres).                         | Tous                       |
| ★★★★★    | Désactiver le Wi-Fi la nuit (pour améliorer le sommeil).                                             | Tous                       |
| ★★★★★    | Utiliser des écouteurs filaires (éviter les AirPods et Bluetooth).                                   | Tous                       |
| ★★★★★    | Choisir un téléphone à faible DAS (< 0,3 W/kg).                                                      | Tous                       |
| ★★★★     | Éloigner les routeurs Wi-Fi (> 3 m des zones de vie).                                                | Tous                       |
| ★★★      | Limiter la durée des appels (< 20 min).                                                              | Tous                       |
| ★★★      | Éviter les <i>small cells</i> 5G (rester à > 10 m).                                                  | Tous                       |
| ★★★      | Sensibiliser les décideurs (maires, directeurs d'écoles, employeurs).                                | Collectivités, entreprises |

## 7.3. Perspectives d'avenir

Les technologies de télécommunication continuent d'évoluer rapidement, avec :

- La 6G (2030+) : Fréquences THz (0,1–1 THz) → risques inconnus (perturbation de l'ADN, effets quantiques).
- L'Internet par satellite : Exposition globale et permanente → pollution électromagnétique mondiale.
- L'IoT (Internet des Objets) : Multiplication des sources d'exposition (capteurs, caméras, objets connectés).
- Les réseaux neuronaux et l'IA : Optimisation des réseaux → exposition encore plus ciblée et intense.

Scénarios possibles :

1. *Statut quo* : Les normes restent basées sur les effets thermiques, et les risques non-thermiques sont ignorés → augmentation des cas de cancer et de troubles neurologiques.
2. Principe de précaution : Les pays adoptent des normes plus strictes (ex. : 0,1 W/kg) → réduction des risques, mais ralentissement du déploiement technologique.
3. Catastrophe sanitaire : Les effets non-thermiques sont confirmés (cancer, troubles cognitifs) → crise mondiale de santé publique.
4. Innovation sécurisée : Les technologies sont développées avec des garde-fous (ex. : blindage EM intégré, limitation de l'exposition) → progrès technologique sans risques sanitaires.

## Bibliographie détaillée sur les ondes EM et les risques sanitaires

### 1. Effets thermiques

ICNIRP (2020). *Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz)*. [Lien](#)

FCC (1996). *Radiofrequency Safety*. [Lien](#)

WHO (2020). *Electromagnetic Fields and Public Health: Mobile Phones*. [Lien](#)

### 2. Effets non-thermiques

Pall, M. L. (2018). *Wi-Fi is an Important Threat to Human Health*. *Journal of Cellular and Molecular Medicine*, 22(8), 3804–3816. [DOI:10.1111/jcmm.13559](https://doi.org/10.1111/jcmm.13559)

Lai, H., & Singh, N. P. (1995). *Acute low-intensity microwave exposure increases DNA single-strand breaks in rat brain cells*. *Bioelectromagnetics*, 16(3), 207–210. [DOI:10.1002/bem.2250160309](https://doi.org/10.1002/bem.2250160309)

Hardell, L., & Carlberg, M. (2015). *Mobile phone and cordless phone use and the risk for glioma – Analysis of pooled case-control studies in Sweden, 1997–2003 and 2007–2009*. *Pathophysiology*, 22(1), 1–13. [DOI:10.1016/j.pathophys.2014.10.001](https://doi.org/10.1016/j.pathophys.2014.10.001)

Bawin, S. M., & Adey, W. R. (1976). *Sensitivity of calcium binding in cerebral tissue to weak environmental electric fields oscillating at low frequency*. *Proceedings of the National Academy of Sciences*, 73(6), 1999–2003. [DOI:10.1073/pnas.73.6.1999](https://doi.org/10.1073/pnas.73.6.1999)

Foster, K. R. (2020). *Thermal and nonthermal mechanisms of interaction of microwave radiation with biological systems*. *Bioelectromagnetics*, 41(3), 185–194. [DOI:10.1002/bem.22287](https://doi.org/10.1002/bem.22287)

### 3. Effets sur la reproduction et le développement

Aitken, R. J., et al. (2005). *Impact of radio frequency electromagnetic radiation on DNA integrity in the male germline*. *International Journal of Andrology*, 28(3), 171–179. [DOI:10.1111/j.1365-2605.2005.00548.x](https://doi.org/10.1111/j.1365-2605.2005.00548.x)

Divan, H. A., et al. (2012). *Prenatal and postnatal exposure to cell phone use and behavioral problems in children*. *Epidemiology*, 23(3), 379–387. [DOI:10.1097/EDE.0b013e31824ce463](https://doi.org/10.1097/EDE.0b013e31824ce463)

Söderqvist, F., et al. (2012). *Childhood brain tumor risk and its association with wireless phones: A case-control study*. *European Journal of Epidemiology*, 27(1), 59–65. [DOI:10.1007/s10654-011-9655-1](https://doi.org/10.1007/s10654-011-9655-1)

### 4. Normes et réglementations

ICNIRP (2020). *Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz)*. [Lien](#)

FCC (1996). *Radiofrequency Safety*. [Lien](#)

ANSES (2021). *Exposition aux radiofréquences et santé*. [Lien](#)

CIRC (2011). *IARC Classifies Radiofrequency Electromagnetic Fields as Possibly Carcinogenic to Humans (Group 2B)*. [Lien](#)

### 5. Études épidémiologiques

INTERPHONE Study Group (2010). *Brain tumour risk in relation to mobile telephone use: results of the INTERPHONE international case-control study*. *International Journal of Epidemiology*, 39(3), 675–694. [DOI:10.1093/ije/dyq079](https://doi.org/10.1093/ije/dyq079)

Cerenat, I., et al. (2014). *Mobile phone use and brain tumours in the CERENAT case-control study*. *Occupational & Environmental Medicine*, 71(7), 514–522. [DOI:10.1136/oemed-2013-101754](https://doi.org/10.1136/oemed-2013-101754)

Hardell, L., & Carlberg, M. (2013). *Using the Hill viewpoints on cancer for evaluating strengths of evidence of the risk for brain tumors associated with the use of mobile and cordless phones*. *Reviews on Environmental Health*, 28(2-3), 97–106. [DOI:10.1515/reveh-2013-0006](https://doi.org/10.1515/reveh-2013-0006)

## **6. Mécanismes biologiques**

Pall, M. L. (2016). *Microwave frequency electromagnetic fields (EMFs) produce widespread neuropsychiatric effects including depression*. *Journal of Chemical Neuroanatomy*, 75(B), 43–51. [DOI:10.1016/j.jchemneu.2015.08.001](https://doi.org/10.1016/j.jchemneu.2015.08.001)

Kesari, K. K., et al. (2018). *Evidence for mobile phone radiation exposure effects on reproductive pattern of male: A mini review*. *Journal of Applied Biology & Biotechnology*, 6(2), 40–44. [DOI:10.7324/JABB.2018.60206](https://doi.org/10.7324/JABB.2018.60206)

Russell, C. L. (2021). *5G wireless telecommunications expansion: Public health and environmental implications*. *Environmental Research*, 196, 110844. [DOI:10.1016/j.envres.2020.110844](https://doi.org/10.1016/j.envres.2020.110844)