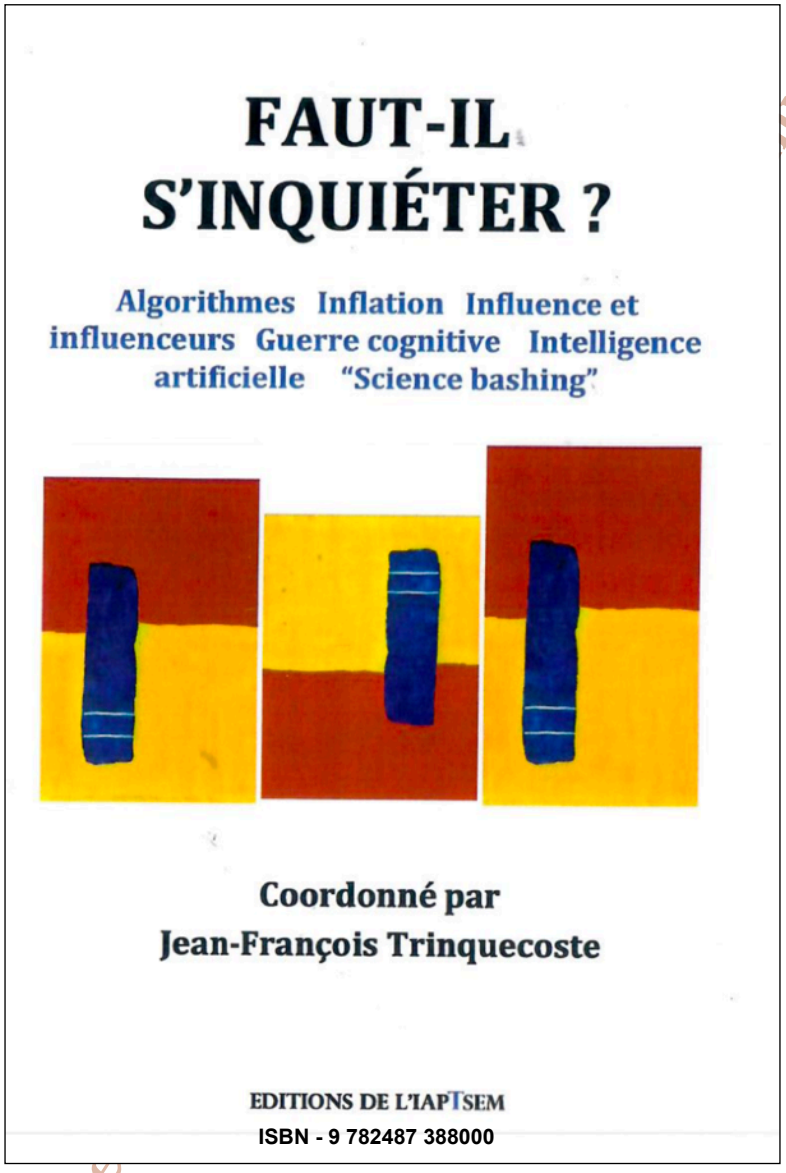
# “Cognitive Warfare” – Une guerre invisible qui s’attaque à notre pensée

Bernard Claverie

# “COGNITIVE WARFARE” UNE GUERRE INVISIBLE QUI S’ATTAQUE À NOTRE PENSÉE




Bernard Claverie

Professeur des universités à l’Institut Polytechnique de Bordeaux

*La pensée est une faculté fragile, sujette à l'erreur et au mensonge.*

Emmanuel Kant

**D**epuis toujours les guerres invisibles préparent, empêchent ou accompagnent l'action kinétique, celle des armes sur le champ de bataille, pour la défense, la conquête ou la soumission des territoires et des peuples à vaincre. Une des plus anciennes est celle de l'information ; elle a toujours accompagné les conflits, faisant part entière de la politique, de la diplomatie et de l'art militaire. Mais depuis la seconde guerre mondiale, avec l'avènement de l'électronique puis de l'informatique, et avec leur pervasion à la fin du siècle dernier, le « monde cyber » est devenu un autre moyen de la dominance et des conflits.

**N**ée de la guerre de l'information, la guerre cybernétique s'en est détachée pour avoir recours au concret des machines et des réseaux mais également à l'impalpable des programmes, des virus et des bots qui assaillent le monde moderne. Ces deux mondes, guerre informationnelle et cyberguerre, ont tissé des liens étroits, entretenant certaines superpositions dans ce qu'il est convenu d'appeler le champ « virtuel » superposé au champ du « matériel ». L'une utilise souvent les outils de l'autre, et vice versa ; ainsi les frontières disparaissent-elles entre les domaines pour n'être qu'une différence de point de vue.

**C**ette double caractéristique de convergence et de différence contribue à l'augmentation du « brouillard » cher aux adeptes de Clausewitz. Elle lui donne une teinte renouvelée, celle des ambiguïtés, des fausse-tés et des manipulations de masse ou ciblées sur tel ou tel individu. C'est au domaine du temps que la caractéristique est redoutable : les guerres de l'information et de la cybernétique ne s'arrêtent jamais.

**L**es sciences cognitives sont un domaine récent de la recherche sur l'esprit humain et la pensée. Elles de caractérisent par la complémentarité de différentes disciplines : linguistique, psychologie et philosophie analytique, biologie et neurosciences, informatique, IA et modélisation. À côté des champs du « matériel » et du « virtuel », elles ouvrent ainsi un nouveau champ de la guerre : le « cognitif ».

**L**a guerre cognitique est l'application des sciences cognitives au domaine de la guerre.

## UNE GUERRE D'ALTÉRATION DE LA PENSÉE

Les progrès des neurosciences comme ceux des sciences du comportement, ont amené à l'émergence des sciences cognitives. Elles constituent un répertoire nouveau des connaissances sur le cerveau et les processus de production, d'organisation et d'adaptation des phénomènes de pensée. Les politiciens et militaires s'en sont évidemment saisis. Comme avant eux les spécialistes de l'information puis ceux des technologies notamment numériques l'avaient fait, ils ont théorisé, mis en doctrine puis en pratique les applications de la dominance cognitive. Ce ne sont alors plus le comportement des individus ou leurs outils et programmes qui deviennent le moyen et l'objectif des acteurs de la défense ou de l'attaque, mais directement la pensée, ses formes et ses moyens, ainsi que les conditions de l'esprit devenu ainsi la cible. Telle est définie la « guerre cognitive » (guerre cognitique [1]) ou la *« cognitive warfare »*.

Elle est une démarche agressive utilisant de manière rationnelle et précise les connaissances des sciences cognitives, modifiant les informations et utilisant les nouvelles technologies pour agir sur le cerveau, l'intelligence et la pensée. De manière conséquente, elle agit ainsi sur les individus ciblés mais également sur les processus sociaux qui permettent leur vie commune. C'est une autre guerre silencieuse, continue, et personne n'en sort indemne. Les différentes attaques tentent de changer les processus de la rationalité pour entraîner les victimes dans le doute et l'anxiété, souvent dans le déni et l'incohérence, parfois dans le trouble de l'esprit pour le malheur des victimes.

Cette guerre efficace fait l'objet d'une pratique précise établie par de grands pays, notamment quelques états totalitaires actuellement au-

[1] Comme il est absurde de qualifier les sciences et techniques de l'information d'informatives, toute science ou technique l'étant, on a utilisé le mot « informatique » en France – pour abandonner l'idée d'une science du seul calcul (computer science). Par analogie on devrait utiliser « cognitique » pour désigner ce qui est relatif aux sciences et technologies de la cognition, mais l'usage n'ayant pas peur des absurdités, la pratique est bien celle d'utiliser le qualificatif « cognitif ». On prend dans ce texte le parti d'adopter la notion de « cognitique » lorsqu'il s'agit de signifier la dimension scientifique, instrumentale et d'application des technologies ciblées sur le cerveau et de garder « cognitive » lorsqu'on se rapproche des domaines plus familiers aux « sciences politiques ».

devant de la scène internationale. La doctrine européenne est en train de s'écrire, avec tant de retard qu'on comprend mal que la France soit dans les dernières nations avancées à s'intéresser au domaine. La guerre cognitive se heurte paradoxalement là à l'ignorance et au désintérêt surprenants des citoyens comme des responsables nationaux : les Français ont longtemps cultivé le scotome. Pourtant, et à l'étonnement renouvelé de certains, cette guerre préside d'évidence aux attaques qui ont récemment transformé la civilisation. Elle est à la préparation de tous les grands conflits de l'actualité et probablement déjà à celle de nombreux à venir.

Le Monde moderne a radicalement évolué avec l'apparition des produits et services numériques et des techniques de l'électronique et des rayonnements à la portée de presque tous. Cette évolution a transformé à la fois les sociétés de ce début de siècle, et les hommes qui les composent ; plus personne n'admettrait de se priver de son *smartphone*, de son micro-ondes, de son ordinateur ou de son navigateur *GPS*. Du détournement de leur usage orienté vers la nuisance est née la guerre cognitive. Le but est d'altérer ou de détruire la pensée rationnelle, les processus et la vie cognitive normale. Il s'agit de les altérer chez un ennemi ou une victime choisie tout en protégeant ceux de ses propres troupes ou citoyens, pour en tirer un bénéfice significatif, stratégique ou tactique. Ce champ de menace en émergence utilise de manière rationnelle et organisée tous les moyens technologiques d'action sur le cerveau et par là sur la cognition.

Cette pratique est aujourd'hui à la base de toute préparation d'action armée et du soutien à l'action kinétique des états belliqueux et de ceux qui veulent se prémunir. Ainsi, elle agit aussi en temps de paix, pour un suprémacisme masqué ou pour préparer les populations attaquées à leur future défaite et à leur soumission. On cherche des parades pour protéger ses propres acteurs et populations ; en ce sens, il s'agit d'une problématique de défense globale, à la fois militaire et civile, à l'endroit et au temps des conflits mais aussi ailleurs, voire partout où la menace peut se concrétiser. On en retrouve la doctrine sous différentes appellations selon les pays ou les disciplines qui l'abordent : « *cognitive warfare* », « *cognitive dominance* », « *cognitive superiority* », « *cognitive control* », « *réflexive control* », « influence cyber-psychologique », « *human cyberdefence* », « *maskirovka* numé-

rique », « ingénierie psychosociale orientée », « neuro-technologies », etc. Peu importe le mot, le but est toujours le même : l'altération cognitive quel qu'en soit le niveau de l'atteinte [2] et quels qu'en soient le nombre et le niveau d'organisation des cibles [3] ou des personnes à défendre et protéger.

Dans tous les cas, il s'agit d'utiliser trois champs de compétences. Les moyens vont de l'usage dirigé de *neuro-technologies* [4 & 5] à l'altération de la communication interpersonnelle, en passant par les pratiques de l'ingénierie sociale [6] ou du contrôle réflexif [7 & 8], souvent en combinaison et selon des méthodes amplifiées par les outils technologiques et cybernétiques. Après avoir dû faire le constat d'interventions négatives d'acteurs initialement anonymes mais aujourd'hui bien identifiés, les démocraties et les systèmes sociaux civilisés se sont inquiétés de cette réalité insidieuse et difficilement saisissable. Ainsi, les

---

[2] Claverie B. (2021). Qu'est-ce que la cognition ? Et comment en faire l'un des moyens de la guerre, in B. Claverie, F. du Cluzel, & B. Prébot (eds), *Cognitive Warfare : la Guerre Cognitique*. Neuilly: NATO-Collaboration Support Office, 4, 1-20, 2021.

[3] Adlakha-Hutcheon G., Dåbakk S. L., Danley L., Bērziņš J., & Blatny J. M. (2022). *Advancing Towards a Common Understanding of Cognitive Warfare for Science and Technology, and Identifying Future Research Trajectories*. Technical Evaluation Report: *Cognitive Warfare Workshop*, Kjeller (Norway): November 2022. Document ac/323-d(2023)0003 (inv), Neuilly: NATO-Collaboration Support Office.

[4] Walther G. (2015). Weaponization of Neuroscience, in J. Clausen & N. Levy (eds) *Handbook of Neuroethics.* Dordrecht: Springer.

[5] McCreight R. (2024). The war inside your mind: unprotected brain battlefields and neuro-vulnerability. *Academia Biology*, 2(6156), 1-9.

[6] Hadnagy C. (2010). *Social Engineering The Art of Human' Hacking*, Hoboken: John Wiley & Sons.

[7] Vasara A. (2020). *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy*. Helsinki: National Defence University.

[8] De Goeij M.W.R. (2023). Reflexive Control: Influencing Strategic Behavior, *Parameters*, 53(4), 97-108.

pratiques d'organisations ou de puissances hostiles [9 & 10] utilisant des moyens non conventionnels d'action sur la pensée des individus et des groupes [11] ont été percées à jour et sont en train d'être répertoriées. Aujourd'hui, elles deviennent une préoccupation de l'Alliance de défense atlantique qui, faute de savoir trop la contrer, entend étudier la guerre cognitive pour la détecter et former ses militaires et les citoyens des pays alliés à y résister et traiter ses effets.

Un problème reste celui de la qualification de l'attaque ; sa mise au jour est une chose, la reconnaître, l'objectiver et la nommer en sont d'autres. Elles entraîneraient la mise en œuvre de l'acte de solidarité de l'OTAN, désignant l'auteur comme ennemi déclaré, en projetant le Monde dans une aventure dont personne ne connaîtrait l'issue. Le scotome est donc installé : on sait ce qui se passe et l'on s'efforce de ne pas le voir.

## UN CONTEXTE TECHNOLOGIQUE POUR DES CONSÉQUENCES PSYCHOLOGIQUES

La théorisation de l'action cognitique a été développée par des Anglo-Saxons dont les travaux [12 & 13] ont rejoint ceux indépendamment menés, dès le début des années 2000, par le Département de la dé-

---

[9] Backes O., & Swab A. (2019). Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. *Paper, Belfer Center for Science and International Affairs*. Cambridge: Harvard University – Harvard Kennedy School, November 2019.

[10] Hung T.-C., & Hung T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars, *Journal of Global Security Studies*, 7(4), ogac016.

[11] Bērziņš J. (2023). The Cognitive Battlefield: Exploring the Western and Russian Views, *Centre for Security and Strategic Research papers*. CSSR Paper 05/23. Riga: National Defence Academy of Latvia, Centre for Security and Strategic Research editions.

[12] Giordano J., & Wurzman R. (2011). Neurotechnologies as weapons in national intelligence and defense – An overview, *Synesis*, T, 55-71.

[13] Giordano J. (2014). *Neurotechnology in National Security and Defense*. Boca Raton: CRC Press.

fense américaine [14] et par des politistes français [15]. Plus récemment, ces généralistes ont étudié la « domination cognitive » dans, une vision civile et de sécurité globale [16 & 17]. C'est dans ces toutes dernières années que le concept a pris une discrète importance en s'appuyant sur les progrès des neuro-technologies (*Neuro-weapons*), de la communication en réseaux (*Network Centric Warfare*) [18] et de l'intelligence artificielle (*Algorithmic Intelligent Systems*) [19].

De la biologie à la technique informatique, de l'électronique située à la pervasion ou à l'embarquement (y compris incarné), des rayonnements diffus à leur maîtrise focalisée, du calcul massif à la computation quantique, de l'Internet à l'interconnectivité globale, les révolutions technologiques s'accélèrent dans de nombreux domaines. Leurs conséquences merveilleusement utiles s'accompagnent pourtant de nouveaux dangers et de nouvelles pratiques mettant ces progrès souvent au service de la vénalité, et parfois à la disposition d'intentions nuisibles**.** Elles servent ainsi des ambitions illégitimes de domination ou de supériorité. Les acteurs sont souvent de médiocres pirates ou des malfaisants, mais l'organisation rationnelle des pratiques par des entrepreneurs aux manettes de sociétés prédatrices a très vite intéressé des leaders et idéologues qui ont trouvé là de quoi assumer leurs projets. C'est d'ailleurs dans une convergence curieuse que ces acteurs s'appuient sur les compétences et moyens de ces mêmes socié-

---

[14] Money A. L. (2001). *Report on Network Centric Warfare: Submitted to the Congress in partial fulfillment of Section 934 of the Defense Authorization Act for FY01*. Washington: Department of Defense, 2001.

[15] Harbulot C., & Lucas D. (eds) (2002). *La guerre cognitive, l'arme de la connaissance*. Paris: Éditions Lavauzelle.

[16] Hartley D.S., & Jobson, K.O. (2021). *Cognitive Superiority: Information to Power*, London: Springer.

[17] Harbulot C. (2024). La légitimité civile de la guerre cognitive, *Ingénierie Cognitique*. London: ISTE, 7(1), 14-17.

[18] Alberts D.S., Garstka J.J., Stein F.P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington: Department of Defence Command and Control Research Program.

[19] Leblanc B. (2024). Faut-il craindre l'Intelligence Artificielle ? In J.-F. Trinquecoste (ed.) *Faut-il avoir peur ?* Actes des conférences 2023 de l'IAPTSEM.

tés, toujours avec le concours d'individus pathologiques cachés derrière leurs écrans. Des porosités et des perméabilités sont d'ailleurs à l'œuvre pour contribuer à un état de « menace globale ».

Le domaine des technologies généralisées est dans ce contexte devenu l'un des moyens et le champ de jeu des suprémacistes et des « idiots utiles » ou contraints qui les servent. Et la menace repose à la fois et curieusement sur la conscience que chacun a souvent du danger, mais aussi sur son incapacité à imaginer pouvoir se passer de l'usage des armes mêmes de l'effraction cognitive. Le numérique joue ici un rôle bien particulier. Comme l'imprimerie a fait du papier et de l'encre les moyens de l'influence de l'époque, le numérique est devenu celui de la transformation des esprits.

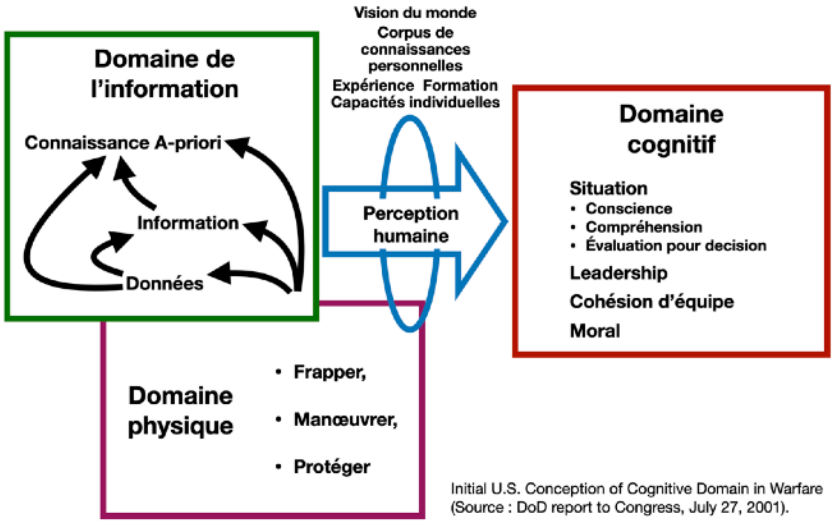



*Figure n° 1 Modèle de domaines de la guerre selon les travaux du Département de la défense américaine en 2001* [23].

La doctrine américaine détermine aujourd'hui trois champs de l'action : physique, virtuel, et cognitif. Le premier est celui des moyens techniques, de la performance des artefacts et de leur robustesse ou fragilité permettant l'effraction des systèmes ; c'est le domaine des informaticiens, électroniciens et intrumentateurs de l'information « de base ». Le second est celui de l'information structurée ou dirigée, et des contenus ; c'est celui de la diffusion et de la transformation des informations pour avoir des conséquences cérébrales ou en faire des connaissances permettant des effets facilitateurs, amplificateurs ou disruptifs. Le troisième est celui qui, grâce aux deux précédents, pro-

duit l'altération des processus de pensée [20]. C'est notamment la conscience de situation et la capacité de décision qui sont ciblées, soit pour les altérer, les empêcher ou en annihiler l'intention, soit pour les conduire sans conscience vers l'attente de l'agresseur [21]. Telle est donc l'ambition de la « guerre cognitive » qui, dans les champs civil et militaire, entend s'appuyer sur des moyens et des méthodes technologiques pour manipuler des informations et assurer ainsi une « supériorité cognitive » [22].

Ces occurrences sont complémentaires [23]. Elles posent chacune les redoutables problèmes du droit et de l'éthique [24], ceux de la légitimité des pratiques, mais aussi ceux de la réponse interdite par les valeurs occidentales. Quant à l'étude expérimentale pour la prévention, elle échappe aux règles de protection des personnes dans la recherche. Aujourd'hui, l'Occident ne peut ni répondre de la même manière ni réellement expérimenter pour se préparer et pouvoir prévenir.

## TROIS COMPARTIMENTS DE L'ACTION COGNITIQUE

Les trois champs de l'action cognitique ont pour objectif trois niveaux de ciblage. On parle de « compartiments ». Ce sont ceux, que la

---

[20] Desclaux G., Marion D., & Claverie B. (2019). Reading the mind of the enemy through an augmented multi-domain Commander's Critical Information Requirements (CCIR) process, *Proceedings of the 24th international Command and Control Research & Technology Symposium*, October 29-31, 2019, Laurel (Maryland): Johns Hopkins Applied Physics Laboratory.

[21] Masakowski Y.R., & Blatny J.M. (eds) (2023). *Mitigating and Responding to Cognitive Warfare*. STO Technical Report TR-HFM-ET-356 – AC/323(HFM-356)TP/1120. Neuilly: Nato Collaboration Support Office.

[22] Claverie B., & du Cluzel F. (2021). Le « Cognitive Warfare » et l'avènement du concept de « guerre cognitique, in B. Claverie, F. du Cluzel, B., & Prébot (eds), *Cognitive Warfare : la Guerre Cognitique*. Neuilly: NATO-CSO Collaboration Support Office, 1, 1-8.

[23] Beauchamp-Mustafaga, N. (2019). Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations, *China Brief*. Washington: The Jamestown Foundation, 19(16), September 6th.

[24] Miller S. (2023). Cognitive warfare: an ethical analysis, *Ethics and Information Technology*, 25, a46.

théorie nous donne de la pensée humaine [2] ; on peut inventorier certains exemples maintenant bien documentés. Le compartiment biologique est globalement celui des cerveaux, supports de la cognition ; l'attaque utilise leur vulnérabilité en les altérant ou en manipulant leurs automatismes [25]. Le compartiment psychologique ou comportemental est celui des productions cognitives et des conséquences comportementales des influences [26 & 27], au niveau individuel, en ce qui concerne l'atteinte des contenus mentaux structurés, ou à l'échelle des petits groupes pour ce qui relève de la destruction de la cohésion – par exemple celle d'un équipage ou d'une cellule décisionnelle. Le troisième compartiment est sociologique [28] ; l'influence est plus indirecte et globale, par exemple sur une catégorie professionnelle, une structure de revendication identitaire, un groupe de pensée ou religieux, une partie ciblée de la société, de telle ou telle nation, de telle ou telle culture…

À bas niveau, la guerre cognitive agit directement sur le cerveau. Un exemple connu est celui du « syndrome de La Havane » ; l'altération cérébrale directe par émission de rayonnements dirigés cible les possibilités de concentration et de décision des victimes [29]. Elle peut être brève ou durable et alors handicaper les victimes pour longtemps. Mais d'autres *neural weapons* [4 & 5] plus ou moins ciblées sont aujourd'hui inventoriés : lasers pour l'atteinte des capacités visuelles [30], intoxi-

---

[25] Claverie B., & Prebot B. (2024). La guerre cognitive de bas niveau : la guerre des cerveaux, *Ingénierie Cognitique*. London: ISTE, 7(1), 69-77.

[26] Claverie B., & Trinquecoste J.-F. (2024). Guerre cognitive et influence psychologique, I*ngénierie Cognitique*. London: ISTE, 7(1), 49-58.

[27] Janin P. (2024). Influence des réseaux sociaux sur la résilience cognitive des jeunes – impact sur les combattants, *Ingénierie Cognitique*. London: ISTE, 7(1), 101-110.

[28] Mucchielli A. (2005). *L'Art d'influencer : analyse des techniques de manipulation*, Paris: Armand Colin.

[29] McCreight R. (2022). Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat. *Small Wars Journal*, online September 16th.

[30] Nakagawara V., & Montgomery R.W. (2000). Laser pointers and aviation safety, *Aviation and Space Environnemental Medicine*, 71, 1060-1062.

cations chimiques ayant des conséquences cognitives [31], manipulations de facteurs d'ambiance tels que les bruits impulsionnels, vibrations, etc. La liste n'est pas close et l'inventivité des nuisibles est probablement sans limite. On peut associer à ce compartiment visant l'étage de base de la cognition certaines technologies utilisant des phénomènes par ailleurs connus, comme l'influence subliminale [32] réglée sur l'atteinte d'automatismes cognitifs (procédures) ou la saturation attentionnelle avec des lumières ou images, des rythmes sonores ou des musiques répétitives [33], etc. Des tels moyens, autrefois réservés à la torture mentale, peuvent être ciblés, de manière individuelle ou généralisée, faisant de cette question une préoccupation de certains spécialistes de santé. On les retrouve sous le terme de « contrôle réflexif » qui englobe des notions de cybernétique de second ordre et de métacognition [34].

Moins physiquement intrusive, l'obsession d'imagerie des pratiquants de jeux vidéo ou de certains programmes addictifs est un autre exemple d'effraction neurophysiologique. Les usagers de systèmes informatiques deviennent dépendants des programmes ou des réseaux [35] et littéralement se droguent au numérique : jeu, lecture en ligne, séries vidéos, permanence de l'information… Les conséquences sont multiples : le besoin et le manque, l'altération de la pensée, l'intolérance, la désespérance et le repliement sur soi ou en petits groupes identitaires, souvent fragiles, élitistes ou violents.

---

[31] Karimi M.A., Avakh F., Abdollahi M., Nikoozadeh E.K., & Golaghaei A (2023). Effects of Chemical Warfare Throughout Time on Mental DisorderSymptoms and Brain Executive Functions of Veterans Exposed toChemical Weapons, *Military Health Science Research*, 21(1), e138012.

[32] Jiang B., Bin Z., & Fujun L. (2013). Research on Subliminal Message Technology and Its Application in Psychological War, *National Defense Technology* (China), 34(4), August 3th.

[33] Schäfer T., Fachner J., & Smukalla M. (2013). Changes in the representation of space and time while listening to music, *Frontiers in Psychology*, 4, 508.

[34] Thomas T.L. (2004). Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies*. 17(2), 237–256.

[35] Cegarra J. (2024). Guerre cognitive et dépendance technologique, *Ingénierie Cognitique*. London: ISTE, 7(1), 59-63.

Plus près de l'émotion et du trouble de la pensée, l'altération de la construction des représentations de son environnement physique ou social, celles des objets et des êtres et de leurs relations présentes, passées et futures, entraîne des réadaptations cognitives qui peuvent être facilement détectées et exploitées. Les dangers sont ceux de l'action sur les phénomènes nécessaires à la construction des représentations : attention, perception et apprentissage, mémoire, capacités d'anticipation, de programmation motrice, etc. On retrouve là les grandes catégories de la neuropsychologie dont la caractéristique fondamentale est celle d'une atteinte focalisée qui se répercute sur l'ensemble cognitif et handicape les personnes et leur milieu. La guerre cognitive est ici une forme de neuropsychologie expérimentale. Les conséquences altèrent l'émotion, l'affectivité, les sentiments et la personnalité des victimes. On rejoint là le domaine des *« psy-ops »* (opérations psychologiques) aujourd'hui armées par le numérique et l'IA, et on connaît la théorisation de la *maskirovka* numérique qui transforme souvent les personnes ciblées en meilleurs avocats des acteurs de leur propre agression [36 & 37].

La confusion réel/virtuel amène de plus en plus de personnes à l'incapacité de distinguer les informations réelles ou légitimes de celles créées et manipulées, notamment grâce à l'ingénierie sociale et aux IA génératives. On constate évidemment cette incapacité dans les systèmes d'information, mais aussi, de plus en plus, dans les films et séries, les podcasts, les jeux ou la réalité virtuelle et autres *métavers* au sein desquels les conséquences sont cognitives et affectives, avec des retentissements sociaux mal maîtrisables.

Le compartiment de l'action sociale est en effet l'un des domaines de prédilection des agresseurs. Les outils ciblés sont eux-mêmes à double objectif, agir sur des individus mais aussi sur des groupes ou des organisations sociales. L'exemple de « Cambridge Analytics » n'est pas le seul, et la désinformation, l'induction et l'influence généralisées sont à

[36] McKenzie I.K. (2004). The Stockholm Syndrome Revisited: Hostages, Relationships, Prediction, Control and Psychological Science, *Journal of police crisis negotiations*, 4(1), 5-21.

[37] Claverie B. (2023). Les opérations d'influence psychologiques russes et la Maskirovka comme état d'esprit, *Ingénierie Cognitique*. London: ISTE, 6(1).

l'œuvre chez les jeunes comme chez les adultes qui se dressent ainsi les uns contre les autres. Les cibles sont souvent des relais sociaux, parfois des idiots utiles, afin d'influer en retour sur d'autres personnes. Ces phénomènes psychosociaux sont, dans ce bouclage, envahis d'affectivité et d'émotion altérant d'autant plus la rationalité des individus avec des effets de groupe. Les conséquences sociales et culturelles [28] sont elles-mêmes à l'origine de dimensions relationnelles et de confiance de niveau psychosocial, transformant les individus.

## LE MODÈLE CROISÉ DE L'OTAN : LES TROIS NIVEAUX DE L'ACTION

La *Science and Technology Organization*, organe de recherche de l'Alliance atlantique, considère que la guerre cognitive consiste, grâce aux moyens technologiques, à « altérer à la fois la cognition et les émotions, souvent dans un environnement modifié, en agissant sur un ou plusieurs de leurs processus afin d'amener à de fausses perceptions ou convictions, d'entraver et fausser la pensée, d'inhiber ou empêcher la prise de décision », et d'amener à une décision erronée, culpabilisée ou mal contextualisée. C'est l'ensemble des « activités menées en synchronisation avec d'autres instruments de pouvoir, afin d'affecter les attitudes et les comportements en influençant, en protégeant et/ou en perturbant les cognitions des individus et des groupes afin d'obtenir un avantage. » et en cela « comme pour d'autres menaces hybrides, nos adversaires mènent une guerre cognitive tout au long du continuum du conflit, et visent à rester dans la "zone grise", en dessous du seuil du conflit armé. » [21].

La guerre cognitive intègre, comme on l'a vu, un « armement » (*weaponization*) de trois domaines : les neurosciences, la psychologie et l'ingénierie sociale. La STO les distingue en trois domaines : la connaissance et sa fausseté, la compréhension et son altération, et la décision et son empêchement [38]. Un modèle conceptuel croisé des compartiments et des niveaux de l'action a été publié sous le titre de « *house model* » (cf. figure n° 2).

Le processus de connaissance est le premier niveau de la cognition.

[38] Paulauskas K. (2024). Why cognitive superiority is an imperative, *NATO Review*, online February 6th.

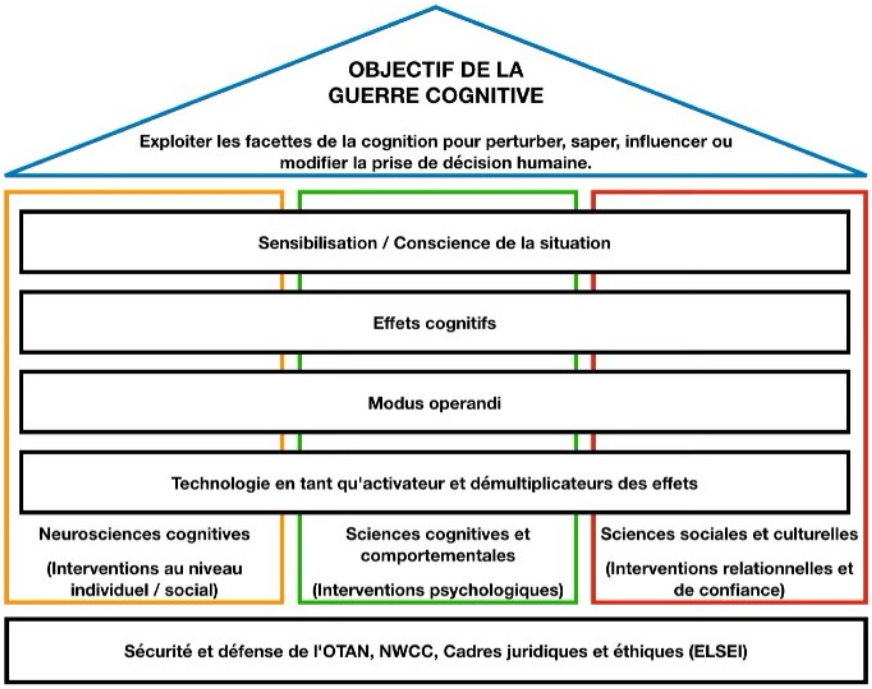



*Figure n° 2 : Le « house model » développé par la NATO-STO - HFM 356: Mitigating and responding to cognitive warfare. On remarquera la complémentarité des sciences et des méthodes, neuro-, psycho- et sociologiques (NWCC: NATO Warfighting Capstone Concept; ELSEI : ethical, legal, social and environmental implication).*

Une de ses dimensions principales est la contextualisation. Le processus cognitif est ce que l'on appelle la « conscience de la situation » (*situation awareness*) ; il concerne la détection, la prise d'information, son organisation, son stockage et l'exploitation des données issues de l'environnement et de l'expérience même de chaque individu en interaction avec les autres [39]. En termes stratégiques, la connaissance consiste à « connaître » ses adversaires et concurrents, en rapport avec ses propres forces et celles de ses alliés. En termes tactiques, il s'agit de connaître instrumentalement les « quand, comment et combien » ; le but est, au-delà de donner des fausses informations, de faire mal penser. Le travail porte aujourd'hui sur la conception d'aides numériques « dignes de confiance » permettant de faciliter et de sécuri-

[39] Prébot B. (2021). Le partage de conscience de situation est un lien de fragilité cognitive, in B. Claverie, F. du Cluzel & B. Prébot (eds), *Cognitive Warfare : la Guerre Cognitique*. Neuilly: NATO-CSO Collaboration Support Office, 10, 1-7.

ser la connaissance [40] grâce à des outils numériques appropriés.

La compréhension de la situation consiste, au-delà de la perception et de la conscience, à donner du sens à la situation [20] en s'y situant spatialement, temporellement, affectivement et intellectuellement. Cet étage cognitif est en charge de transformer la connaissance en un objet mental de compréhension globale. Autant le niveau précédent peut être délégué ou aidé par des machines de supervision et de contrôle de l'erreur humaine, autant la compréhension est personnelle : la machine ne comprend pas. Il s'agit de comprendre ce que les différents intervenants prévoient ou sont susceptibles de faire, comment ils pensent et organisent leurs propres stratégies cognitives, comment ils décident, programment, commandent et contrôlent leurs opérations. L'atteinte cognitive porte sur des processus de reconfiguration, complétion, substitution…

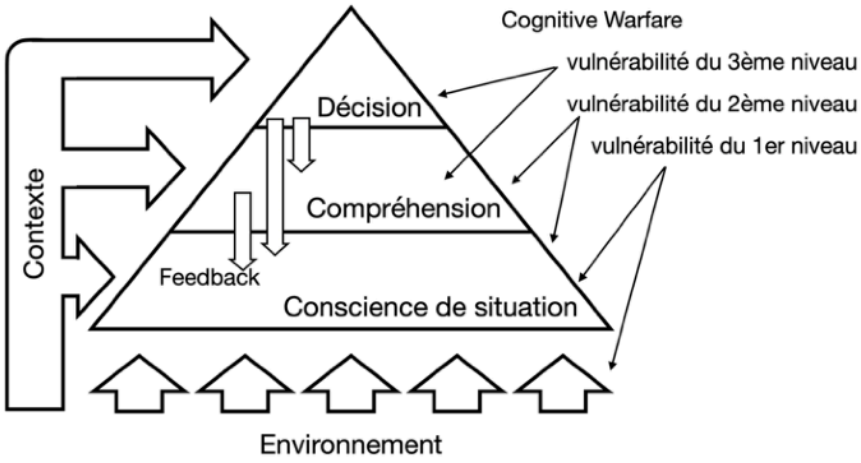



*Figure n° 3 : Trois niveaux de traitement cognitif de l'information et niveaux de vulnérabilité et de l'action cognitique (OTAN/STO). Les informations traitées sont issues de l'environnement (situation et contexte) et réévaluées par feedback positif (facilitateur), négatif (modulateur) ou correctif (adaptatif).*

Le niveau supérieur est celui de la décision et de la conduite de l'action. L'avantage cognitif correspond à cet étage : c'est l'aptitude à pouvoir et savoir décider, à agir et à contrôler son action de manière supérieure à celle d'un concurrent ou d'un adversaire. Pour cela, leurs ca-

[40] Desclaux G. (2021). Communication et confiance entre les humains et les machines intelligentes dotées de fonctions autonomes, *Hermès,* Paris: CNRS Éditions, 88, 192-196.

pacités doivent être diminuées. En ce qui concerne la guerre cognitive, les deux moyens sont associés : (i) aide à la décision par les moyens numériques, (ii) altération de l'information, des moyens de connaissance, et des processus de compréhension. Les outils à l'œuvre sont la distorsion cognitive et l'inhibition, pour une mauvaise ou une non-prise de décision. Ils correspondent à l'altération du raisonnement, la fausse certitude, le doute et la peur de l'erreur.

On documente différents niveaux de vulnérabilité [41] : lorsqu'il y a surabondance d'informations, lorsqu'il n'y a pas assez de sens et que la compréhension est impossible, la réaction n'est ni suffisante, ni rapide, ni efficace voire erronée. Lorsque le décideur se remémore par induction et lorsque l'écart référentiel est grand entre le souvenu et l'oublié, l'émergence incontrôlée des souvenirs inhibe la décision. L'histoire politique internationale récente est, à ce propos, un exemple typique des inhibitions, des délais et des fuites de responsabilité.

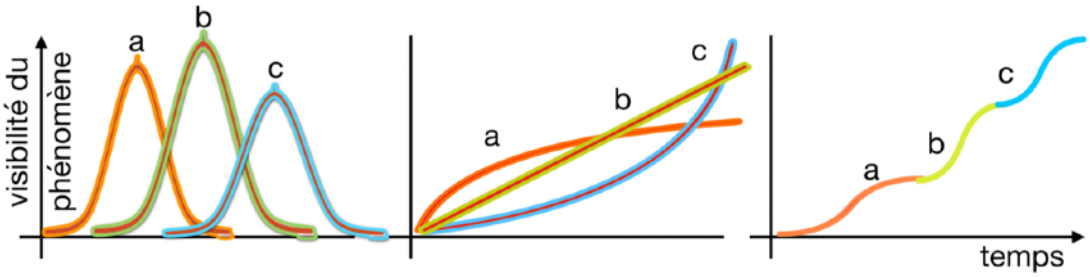



*Figure n° 4 : Les différents temps de l'action cognitique (RAND NSRD 2023) : a en temps de paix, b pendant la crise, c en période guerre. La compréhension spontanée se rapproche du schéma en cascade e en succession (à droite) alors que les formes probable de l'action sont combinées en recouvrement (à gauche), ou en parallèle (au centre).*

Ces trois étages couplés des trois domaines s'échelonnent selon les temps de la guerre cognitive. La RAND Corporation, organisme de recherche non gouvernemental américain, s'étant saisie de la problématique de la guerre cognitive menée par la Chine envers les États-Unis, a défini un ensemble de cas génériques à partir de la doctrine chinoise de l'Armée populaire de libération (*PLA : People's Liberation Army*). Elle distingue trois phases temporelles : les actions en temps de paix,

[41] Danyk Y., & Briggs C.M. (2023). Modern Cognitive Operations and Hybrid Warfare, *Journal of Strategic Security*, 16(1), 35-50.

celles pendant la crise, celles du temps de la guerre militaire [42] (cf. figure n° 4). La théorisation apparaît d'ailleurs dans d'autres supports, saisie par les auteurs des essais d'anticipation exploratoires [43] financés par les armées (type *Red-team*) [44].

| Répartition de l'action adaptée de guerre cognitive par la PLA | | | | | |
|---|---|---|---|---|---|
| Phase opérationnelle | Cible opérationnelle | Tactiques | Type de l'information | Vecteur | But operationnel |
| Temps de paix | Population nationale (masses et alliés) | Plan national de programme | Vérité | | Renforcer la confiance intérieure |
| | Société internationale | | | | Obtenir le soutien de l'opinion internationale |
| Temps de guerre | Élites de l'adversaire | Création de contenus vidéo | Vérité et désinformation | Interférence par guerre électronique | Opposition à la guerre par les élites |
| | Troupes et militaires à la bataille | Diffusez de manière sélective des informations | Vérité traumatisante | Pénétration par Internet | Pression psychologique |
| | Masses populaires et cibles spécifiques | Désinformation pure | Information fausse ou douteuse | | Inciter les commandants à des erreurs |

*Tableau n° 1 : Doctrine chinoise de guerre cognitive en fonction des temps de l'action (a et c - le temps de crise b est inclus dans les lignes du temps de guerre (selon la RANC Corporation). Reproduction d'un tableau de Jiang et al. (2011 ; traduction du chinois par Beauchamp-Mustafaga, 2019 - selon le traducteur, le tableau semble recouper en partie la thèse de doctorat de Bu Jiang sur l'effet psychologique des informations suggestives par superposition vidéo.*

La compétition en temps de paix (a) repose sur la collecte de données, le façonnage des perceptions des adversaires, la dégradation de leur motivation à combattre et la sape des volontés. Ces actions permettent d'aborder favorablement l'épisode de crise (b), avec le soutien de la dissuasion et la menace, la dégradation de la volonté de réaction

[42] Beauchamp-Mustafaga N. (2023). *Chinese Next-Generation Psychological Warfare - The Military Applications of Emerging Technologies and Implications for the USA*. Santa Monica: RAND National Security Research Division.

[43] Le Guyader H. (2023). Termites, fourmis, frelons : les trois temporalités d'un conflit moderne. In *Black Trends – un Monde en Rupture*. Paris: Equateurs.

[44] Red Team (2023). *Ces guerres qui nous attendent (2030-2060)*. Paris: Les Équateurs / Humensis.

ainsi que la maîtrise négative du soutien public et l'affaiblissement de toutes les forces morales de l'intérieur. Le temps de la guerre (c), dans la même veine, s'accompagne de la dégradation des conditions de la prise de décision, tant en matière de leadership que des moyens de sa mise en œuvre et de la conduite des opérations. Il s'agit d'altérer la combativité et la volonté de l'adversaire en détruisant le plus possible le soutien public à la guerre et de l'affaiblir « de l'intérieur » en s'attaquant notamment à l'imaginaire et l'espoir.

## CIBLAGE, BIAIS COGNITIFS ET THÉORIE TERNAIRE DES CIBLES

L'inventaire des modalités dont dispose l'acteur étant établi, se pose alors la question de la relation de ces niveaux d'action. Un premier type d'actions peut-être orienté à tous les niveaux, postulant un effet d'interaction entre individus (a), groupes (b) et sociétés ou cultures (b). Un second type vise spécifiquement l'un des éléments, c'est-à-dire tel ou tels individus (a), tel ou tels groupes – dont les dimensions peuvent varier de l'équipage à la structure d'organisation de travail (b), de collaboration, d'échange… – ou des structures sociales supérieures (c). Enfin, l'action peut concerner tous les niveaux (a, b, c) en en exploitant la contamination. L'exploitation des bais cognitifs selon leurs types détermine ou est déterminée par la pratique du « ciblage ».

Les biais cognitifs sont une sorte de distorsions de la pensée qui peut être utilisée dans chacun des trois dimensions, compartiments et temps de l'action, selon un mode lui-même ternaire. La notion de biais est née de la psychologie et de l'économie dans les années 1970 [45] pour comprendre certaines décisions irrationnelles de gestionnaires ou de consommateurs. C'est une forme de déviation ou d'altération systématique de la logique rationnelle menant, le plus souvent spontanément ou dans un contexte d'influence, à un écart entre réalité objective (données de la réalité) et réalité subjective (vues de l'esprit). C'est cette dernière qui emporte la conviction des victimes [46].

Il s'agit donc d'exploiter les limites à la fois structurelles et fonction-

[45] Kahneman D., Slovic P., & Tversky A. (eds.) (1982). *Judgment Under Uncertainty : Heuristics and Biases*. Cambridge: Cambridge University Press.

[46] Guéguen N. (2002). Psychologie de la manipulation et de la soumission, Paris: Dunod.

nelles des individus (capacités mentales, limitations psychophysiologiques, convictions et croyances…) pour transformer la pensée. On évoque là les notions de rationalité limitée (*bounded rationality*) [47] et de logique spontanée ou naturelle [48], convoquant plus une « pensée magique » que logique [49]. Et c'est ce côté irrationnel qui, dans le cadre de la guerre cognitive, est exploité afin d'amener des individus et des groupes ciblés à des choix comportementaux inadéquats, des décisions inadaptées ou des conduites stabilisées qui conduisent la cible à une forme programmée de l'erreur ou de l'inhibition de l'action.

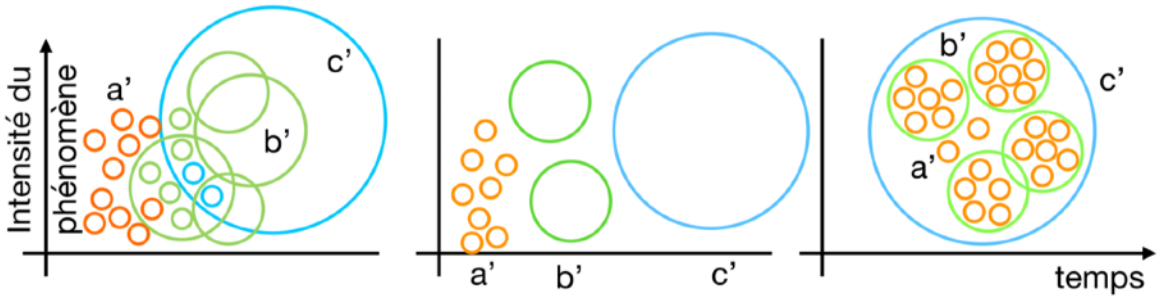



*Figure n° 5 : Trois types de ciblage, directe de l'individu (a') au groupe (b') et à la société (c') et vice versa (à gauche), spécifique à l'un des niveaux (au centre), et indirecte par contamination (à droite).*

Ces biais peuvent être classés selon l'implication des compartiments cognitifs concernés (*cf. supra*), c'est-à-dire des étages de l'appareil mental qu'ils mobilisent. Les biais sensori-moteurs, les habitudes et les automatismes perceptifs permettent le recours à des méthodes d'altération de base du traitement de l'information : bruitage, automatismes, habitudes ou préférences cognitives (procédures), menant à la non-détection, à la négation ou à l'illusion. Ils exploitent la fatigue, la chronobiologie, les capacités limitées des canaux attentionnels, la saturation de l'attention, l'inhibition du contrôle de l'action… et même l'atteinte biologique. Les biais mnémoniques concernent les caracté-

[47] Simon H.A. (1997). *Models of Bounded Rationality – Vol. 3: Emperically Grounded Economic Reason*. Cambridge: Massachusetts Institute of Technology Press.

[48] Grize J.-B. (2009). Logique Naturelle, in R. Doron & F. Parot (eds) *Dictionnaire de Psychologie.* Paris: Presses Universitaires de Frances, 424-425.

[49] de Brabandère L. (2008). *Pensée Magique, Pensée Logique*. Paris: Éditions Le Pommier.

ristiques dynamiques de la mémoire (mémoire à court terme vs. à long terme, mémoire procédurale vs. déclarative, mémoire implicite vs. sémantique…) et de l'apprentissage (conflits cognitifs, effet de primauté, de récence…).

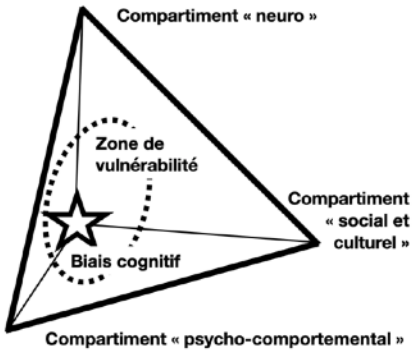



*Figure n° 6 : Théorie du micro-ciblage – exemple de concordance opérationnelle entre vulnérabilité individuelle de la cible (en pointillés) et orientation de biais cognitif qui lui est adapté (représenté par une étoile).*

Les moyens de documentation découlent de la rencontre des techniques traditionnelles du renseignement augmentées par les outils du numérique et du big data : habitudes, pratique sportive ou artistique, voyages, vie familiale et extra-familiale, activités associatives, informations de santé… mais également traceurs GPS, comportements en ligne, sites consultés et temps d'écran, réseaux sociaux, acceptation des *cookies*, rythmes de sommeil, consommations électriques… Des programmes statistiques et d'intelligence artificielle permettent à la fois le raccourcissement des temps d'analyse et l'explosion du champ des données utiles. Des exemples de tels programmes ont récemment défrayé la chronique (programme *Pegasus* et autres moyens d'intrusion numérique à la portée de tous sur le *darknet*).

Le ciblage porte plus sur les « quantités comportementales » que sur les contenus qui sont ultérieurement traités par des *analytics* d'IA sémantique. On peut ainsi dresser des descriptions de vulnérabilités et repérer de plus en plus finement des biais adéquats. La procédure est bien établie et connue sous le nom de « microciblage » [50]. La guerre

[50] Debidour J., & Pelletier P. (2024). De l'analyse d'audience au microciblage : outil comportemental pour la guerre cognitive", *Ingénierie Cognitique*. London: ISTE, 7(1), 96-100.

cognitive peut alors être interprétée comme une théorie offensive et une pratique ciblée des biais cognitifs induits après analyse comportementale numérique. Ces dimensions, si elles sont exploitées pour des actions d'ingérence cognitique, doivent être sérieusement prises en compte dans les procédures de prévention, de formation, de protection et d'anticipation des menaces.

## FORMER ET PROTÉGER FACE À L'INGÉRENCE COGNITIQUE

Les préoccupations liées à la guerre cognitive sont suffisamment sérieuses pour que les organismes internationaux (Commandement pour la transformation de l'OTAN), américains (Department de la défense, RAND Corporation) et aujourd'hui français (Cellule d'Anticipation stratégique et orientation de l'État-major des armées, Agence Innovation-Défense de la Direction générale de l'armement) souhaitent aborder cette menace à différents niveaux d'expertise, politique, sociale, psychologique et biologique. De manière générale, et au-delà des limitations instrumentales et réglementaires spécifiques à la défense et la sécurité, le spectre connu n'en est qu'au tout début. Certaines études commencent à aborder la vulnérabilité multidimensionnelle des *C2-air* [51] ou celle des personnels politiques [52]. Elle ne concerne cependant que des milieux très fermés où il n'est pas facile d'expérimenter. Par ailleurs l'éthique impose une grande prudence et le respect des caractéristiques intimes ainsi que de la potentielle fragilité des personnes.

On peut néanmoins tracer une feuille de route pour de futurs travaux et pour l'information et la formation. L'envahissement des outils numériques dans les tâches assurées par les personnes ciblées ouvre tant de vulnérabilités, dont la dépendance cybernétique et le refus de la prise de conscience. Toute attaque, pour peu qu'elle soit repérée, demande pourtant une reconfiguration cognitive rapide, le plus

[51] Claverie B., du Cluzel F., & Desclaux G. (2022). Cognitive Warfare and C2: Operationalizing the Concept of Cognitive Warfare, paper presented at the *2nd Scientific and Strategic Workshop on "Cognitive Warfare"*. West Point (New-York): US Military Academy - March 4th.

[52] Valette M., Harbulot C. & Hardouin A. (2024). Guerre Cognitive : avant-propos au numéro spécial, *Ingénierie Cognitique*. London: ISTE, 7(1), 4-5.

souvent aidée, vers des procédures plus traditionnelles que de nouvelles générations ne maîtrisent plus. La sensibilisation et la formation sont alors des nécessités loin d'être comprises ni parfois envisagées ou même acceptées. La résilience des représentations partagées entre décideurs, entre décideurs et opérateurs et entre opérateurs eux-mêmes doit être réexaminée à l'aune des fragilités. Par exemple, la saturation attentionnelle, la distraction orientée, l'usure motivationnelle, la banalisation et l'induction de l'incertitude sur les analyses et sur les jugements, peuvent être exploitées d'un côté en ayant pour but l'effraction cognitique d'un autre, etc.

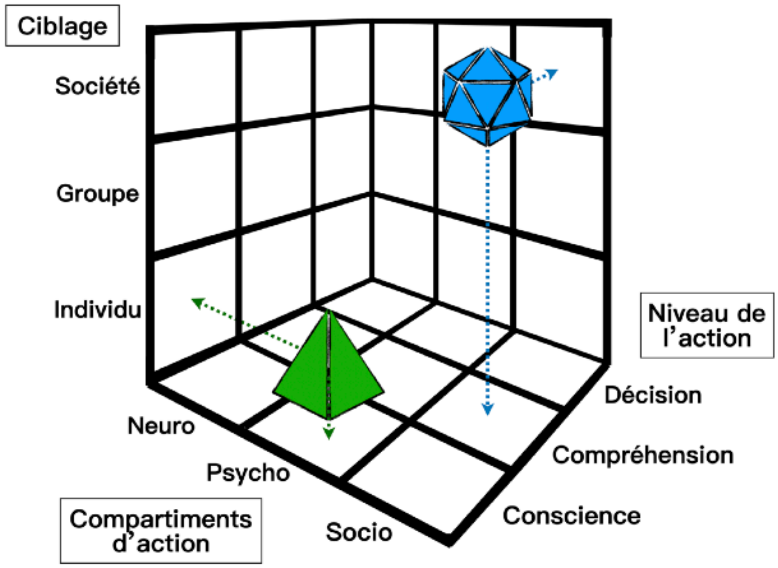



*Figure n°7 : Espace factoriel synthétique des actions ciblées en fonction des compartiments de l'action (neuro, psycho-comportemental, social), du niveau de l'action (conscience situation, compréhension, capacité de décision)à, et de la typicité de la cible (individu choisi, groupe ou équipe, ensemble social). Ici la pyramide représente un ciblage psycho-comportemental altérant la conscience situation d'un individu, le polygone une action de démoralisation (e.g.: maskirovka) d'une société par absence de compréhension d'évènements. Cet espace permet d'établir les stratégies de formation et prévention des actions d'ingérence cognitique selon la théorisation qui en est donnée dans l'article.*

Cette feuille de route doit aborder différentes dimensions (cf. figure 7), celle du développement technologique pour la surveillance, l'évaluation et l'amélioration de capacités cognitives ainsi « augmentées », et de méthodes de supervision de l'état cognitif des opérateurs, pilotes, contrôleurs ou commandeurs. Le but est de sauvegarder les performances de prise de décision, d'améliorer les capacités mentales des individus, et de construire de futures contre-mesures.

Si de discrets efforts ont été entrepris quant à la robustesse affective de certains personnels militaires, rien ne l'est dans le civil. La supervision et la détection par des IA (HAT pour *Human-Autonomy Teaming* [53]) sont une piste proposée par certains auteurs, mais restent pour l'heure bien négligées. La normalisation devrait, en termes doctrinaux, permettre ainsi l'évaluation continue par de tels systèmes adaptatifs, par une nouvelle génération d'IHM enrichies par IA de confiance, c'est-à-dire de technologies robustes de surveillance, d'évaluation, d'alertes et de modulation dans les trois compartiments, et cela pour les trois étages de vulnérabilité et pour les trois temps déjà évoqués. Pour cela, on imagine des simulateurs ou « *design labs* » [54] afin d'enrichir, à la fois, les dimensions d'enseignement et de recherche. Ce type de dispositifs, bien que leur conceptualisation n'en soit qu'à ses débuts, doit prendre une place centrale pour une véritable pédagogie de la menace.

## ÉTHIQUE DES VULNÉRABILITÉS ET PÉDAGOGIE DE LA MENACE

Les limites éthiques de l'action de supériorité cognitive percutent de plein fouet les valeurs morales des états et sociétés occidentales. Un exemple maintenant célèbre est celui qui consiste à interférer dans le processus démocratique en s'immisçant dans les élections ou à manipuler un dirigeant politique pour obtenir des avantages économiques ou stratégiques. Un autre exemple a été celui du microciblage de parlementaires recevant des messages personnalisés en pleine session de vote. De nombreux cas ont été identifiés pour amener des opérateurs à des erreurs ciblées. Face à de telles situations, les institutions ou industries occidentales ne peuvent pas compromettre leurs valeurs pour se défendre contre un acteur souvent dissimulé ayant des valeurs différentes. Au contraire, elles doivent trouver les moyens de mieux comprendre, expliquer, former, expérimenter, et sensibiliser les cibles potentielles et proposer des protocoles de défense.

---

[53] Lyons J.B., Sycara K., Lewis M., Capiola A. (2024). Human–Autonomy Teaming (HAT) – Équipe entre humain et autonomie : définitions, débats et orientations. *Ingénierie Cognitique*. London: ISTE, 7(2), 1-26.

[54] Ducourneau A. (2024). Un "design lab". pour la sécurité cognitive, *Ingénierie Cognitique*. London: ISTE, 7(1), 90-95.

Les technologies d'attaque utilisées ont ceci de particulier qu'elles sont toujours intrusives, et cela sans apparence et sans trace immédiate ou concrète. Une question éthique est posée : comment protéger des personnes qui, parfois, sont elles-mêmes demandeuses de l'usage des technologies nocives, comment protéger des adeptes de la fréquentation de dispositifs dangereux, comment protéger les personnes fragiles face à la complexité de procédures, les travailleurs postés lassés des éléments de méthode, les opérateurs dans les moments de fatigue et d'inattention, etc. ? Tous ces publics sont des cibles faciles. L'influence librement consentie, par exemple dans la pratique de réseaux sociaux pourtant connus comme nocifs, dans l'acceptation des cookies dans la navigation internet ou le refus des contraintes de élémentaires de cybersécurité, ou encore l'exhibitionnisme numérique en ligne sont à ce propos significatifs de la complexité d'un domaine où tout le monde se sent expert ou au contraire dépassé.

La question de la responsabilité de la cible est alors posée : la faille cognitive s'apparente-t-elle à une faute professionnelle et le fait de l'ignorer ou de la cacher à une circonstance aggravante ? La capacité d'objectivité et celle d'autocritique ne sont pas, en la matière, à la portée de chacun. L'effort pédagogique doit s'accompagner de tolérance institutionnelle dans le difficile équilibre du droit à l'erreur et de la responsabilité engagée. Il s'agit là d'un retard naturel du droit, puisque la jurisprudence n'a pas eu le temps de s'établir. Un troisième niveau est relatif à la redoutable question : comment prévenir ou protéger ceux qui ne le veulent pas ? Faut-il pénaliser le domaine ? C'est un fait : une caractéristique commune de ces actions d'effraction cognitive est qu'elles mobilisent des processus inconscients peu contrôlables et qu'ils transforment toujours la personnalité des individus. Cette atteinte est d'ailleurs souvent niée par les victimes elles-mêmes, par refoulement ou par dissimulation et l'on ne peut que difficilement aider des personnes qui le refusent. La conséquence en est souvent chez elle la construction argumentative justificative qui peut aller jusqu'à l'hallucination ou au délire, voire à l'agression du « porteur de mauvaise nouvelle » ou même parfois de celui qui n'y est pour rien. Dans tous les cas, elle participe à l'augmentation de l'effet nocif, lui donnant une forme d'amplification.

La dimension psychopathologique des conséquences de l'influence

orientée ou des armes neuroniques n'est pas à négliger et reste bien peu étudiée au niveau individuel comme à celui des groupes. On ne peut que constater l'indéniable résistance des décideurs ou des managers, peut-être même des lecteurs de ces lignes, pourtant eux-mêmes cibles potentielles. Minimiser le risque pour soi-même contribue *de facto* à accroître la regrettable efficacité du ciblage hostile. Ici encore l'effort doit être celui de la sensibilisation et de la formation, mais aussi celui de la démonstration dans une culture généralisée de sécurité globale [55] et de prévention [56].

## POUR CONCLURE

La révolution technologique des cinquante dernières années a donné des moyens et méthodes permettant à des acteurs malveillants, étatiques ou non, pour mener une nouvelle forme de guerre silencieuse, invisible mais bien concrète. Cette guerre contre la pensée rationnelle et l'intelligence éclairée est la guerre cognitive.

Si elle a été initialement utilisée par des entreprises internationales très vite confrontées aux limites de la Loi et de l'éthique, elle a été perfectionnée et standardisée comme pratique généralisée par certains pays, parfois des dictatures ou des états parias qui s'affranchissent de ces limites en appliquant l'attaque des individus et des systèmes sociaux démocratiques. Aujourd'hui, la guerre cognitive est probablement anti-occidentale, et elle peut cibler tous les domaines économiques et industriels, de culture et d'éducation, de défense ou de sécurité. Le risque est partout, en Europe, dans les pays anglo-saxons et dans les autres nations démocratiques de l'Indo-Pacifique ou de l'extrême orient qui sont devenus le terrain de jeu des acteurs agressifs. L'OTAN engage les alliés à s'y confronter et à réagir, prévenir et peut-être agir. Dans ses principes, elle sépare les trois dimensions de l'ac-

---

[55] Claverie B., & Hamacher H. W. (2018). Education and Information towards a Shared Culture on Global and Civil Security, Topic 5 of the Global Security / Civil Security Session. *6th French-German Research Forum in Scientific Research – 6° Forum de la coopération franco-allemande en recherche scientifique*, Berlin (Germany) 19 June 2018. Official r*eport*. Paris: La Documentation Française.

[56] Van der Linden S. (2023). *Why Misinformation Infects Our Minds and How to Build Immunity*. London: W.W. Norton & Company.

tion et de la défense en un premier volet du concret et du physique, un autre de l'information et un troisième cognitif, ; et c'est celui-là qui est le lieu de nouvelles vulnérabilités. Alors que le risque du réel est évident, avec récemment des technologues qui s'en sont saisies dans le domaine cybernétique [57], que le risque de l'information [58] commence à poindre son nez, le domaine cognitif reste le parent pauvre de l'intérêt des responsables politiques et des polémologues.

Comment réagir face à ce désintérêt des élites ? Mais comment aussi faire face à des personnes informées du risque et qui le refusent, ou qui flirtent avec lui ou décident de le négliger par rapport aux bénéfices qu'ils pensent trouver dans des pratiques dangereuses ? Le cadre éthique actuel n'est évidemment ni suffisant ni satisfaisant. Des efforts commencent à être faits. On a cité plus haut les travaux de l'OTAN et on peut signaler l'Organisation de coopération et de développement économiques (OCDE) qui a récemment proposé un encadrement des neuro-technologies [59] et alerte sur les effets cognitifs des fausses informations [60]. Au niveau doctrinal militaire, le cadre de l'emploi de ces technologies ne fait pas encore l'objet de texte précis ; ils sont en rédaction.

La doctrine peut-elle prévoir de telles agressions non armées justifiant la légitime défense, selon les principes universels de distinction, de proportionnalité et de précaution ? Comment objectiver et mesurer des actions cognitiques, souvent menées sous le seuil de détection, et comment répondre puisque le *modus operandi* est interdit et l'action incommensurable ? Le domaine est complexe et mêle moralité, subjectivité et incapacité au grand bénéfice des acteurs de la guerre cognitive, dans un désintérêt presque passif de leurs prochaines victimes.

---

[57] Comité national pilote d'éthique du numérique (CNPEN) (2019). *Manifeste pour une éthique du numérique*. Paris: Conseil Consultatif National d'Éthique.

[58] Colon D. (2023). *La Guerre de l'information – Les États à la conquête de nos esprits*. Paris: Le Taillandier.

[59] OCDE (2022). *Recommandation du Conseil sur l'innovation responsable dans le domaine des neurotechnologies*, OECD/LEGAL/0457, Paris: Instruments juridiques de l'OCDE.

[60] OCDE (2024). *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*. Paris: Éditions OCDE.