

L'Intelligence Artificielle dans la guerre de l'information : vers la lutte informationnelle algorithmique



Colonel Bertrand BOYER

Chef de corps

Centre interarmées des actions sur l'environnement

Il est 1h52 dans la nuit du 28 août 2023, lorsque qu'une attaque informationnelle contre les armées françaises est lancée sur les réseaux sociaux. Cette action prend la forme d'un faux document de 12 pages, présenté comme une « fuite » et détaillant les préparatifs d'une prétendue opération militaire française contre la junte nigérienne. L'objectif de cette manipulation : attiser le sentiment antifrançais au Sahel, dans un climat tendu après le coup d'État du 26 juillet. Cette opération grossière est rapidement détectée et ses effets sont limités, mais qu'en serait-il si nos adversaires avaient eu recours massivement à des outils d'intelligence artificielle ? Et si la diffusion de ce faux avait été propulsée artificiellement en s'appuyant sur l'exploitation algorithmique des biais des auditoires cibles ?

De la guerre de l'information à la guerre cognitive

Depuis 2022 et l'introduction de l'influence au rang de sixième fonction stratégique dans La Revue nationale stratégique, les autorités françaises

structurent un domaine qui évolue plus vite que notre capacité à le circonscrire. Directement confrontés aux effets de la désinformation et de la manipulation de l'information, les Armées construisent et consolident une nouvelle aptitude interarmées : « influence et lutte informationnelle ».

Il s'agit dès lors de se doter d'une capacité à détecter, caractériser et agir face à ces menaces. Ce chantier s'inscrit dans un contexte où les évolutions technologiques constantes modifient profondément l'approche de ce type d'affrontement. La guerre de l'information aujourd'hui, ne se limite plus à diffuser un récit pour infléchir des perceptions sur un théâtre d'opérations, mais elle vise aujourd'hui directement nos processus cognitifs. Cet élargissement du domaine est rendu possible par la prédominance du fait technique dans notre relation à l'information. Cette part croissante de l'intermédiation technologique rend alors possible la création d'un véritable « marché » de la désinformation et l'émergence d'une économie de l'influence informationnelle.

Comme le souligne Samuel Henry dans son article sur "la matérialité de la désinformation"¹, nous assistons aujourd'hui à une industrialisation des processus de désinformation qui gomme la frontière entre manipulation et information et nous plonge dans l'ère de la post vérité.

Nous n'avons plus à faire à des séries d'actions isolées mais un écosystème complexe où la matérialité des techniques et des infrastructures joue un rôle déterminant. Dans ce cadre, la compréhension des mécanismes algorithmiques soutenant le modèle économique des plateformes de réseaux sociaux est un prérequis essentiel à l'action. Les acteurs étatiques et non-étatiques investissent massivement dans des dispositifs

¹ [La matérialité de la désinformation. Samuel HENRY](#)

techniques sophistiqués pour amplifier leur capacité d'influence, transformant la désinformation en une véritable infrastructure stratégique.

Ce que l'on qualifie aujourd'hui de « guerre de l'information » apparaît pourtant assez tôt dans l'histoire des conflits ; elle se fonde à l'origine sur la notion de ruse et agit sur les perceptions de l'adversaire. Sans définition établie, la guerre de l'information demeure un concept flou, propice aux interprétations divergentes. Le chercheur François-Bernard Huyghe la définissait en 2016 comme « l'ensemble des méthodes visant à infliger un dommage à un rival ou à se garantir une supériorité par l'acquisition d'information, par la dégradation de celle de l'adversaire ou par la propagation de messages favorables à ses desseins stratégiques ». Mais avec l'émergence des réseaux sociaux et des nouveaux opérateurs de l'information, le concept déborde du champ strictement militaire et devient un outil au service des stratégies de pouvoirs étatiques.

David Colon, historien et spécialiste de l'histoire de la propagande, définit pour sa part la guerre de l'information comme « le fait pour un État de recourir à l'information comme à une arme, à des fins militaires, politiques, économiques, culturelles ou diplomatiques. Elle repose sur l'usage de l'information non seulement comme une source de pouvoir, mais comme un pouvoir en soi, autrement dit comme un levier de puissance dans les relations internationales ». Cette forme d'affrontement se développe sur trois niveaux distincts, le politico-militaire et les opérations, l'économie et le volet socio-culturel.

Aujourd'hui, avec les possibilités offertes par les technologies de l'intelligence artificielle, nous assistons probablement à une nouvelle évolution majeure qui permet de façonner plus en profondeur des franges croissantes de la société. La guerre de l'information se mue en guerre cognitive et elle exploite les ressorts des algorithmes des plateformes.

Cette évolution conduit à explorer le concept de guerre cognitive algorithmique. Là où la guerre de l'information vise à modifier des comportements par l'action sur les perceptions, la guerre cognitive algorithmique va plus loin et cherche à influencer sur les croyances profondes et modifier notre « lecture du monde et des événements ». C'est le processus de traitement de l'information par l'individu via les plateformes qui est ainsi ciblé et les usages numériques rendent ces manipulations possibles à une variété d'acteurs.

L'émergence de la guerre cognitive algorithmique

Le concept de « guerre cognitive algorithmique » est principalement développé par des chercheurs chinois et il fait l'objet de nombreuses études dans le cadre de leçons tirées du conflit en Ukraine. En effet, l'invasion de l'Ukraine par la Russie en 2022 a marqué un tournant dans la manière dont certaines puissances conçoivent la guerre cognitive, notamment l'importance des algorithmes et de l'intelligence artificielle. La capacité de l'Ukraine à utiliser les réseaux sociaux pour établir un « récit alternatif » par rapport à la Russie a été identifiée comme un facteur clé de son succès, notamment sur des plateformes comme TikTok.

Un rapport du « Special Competitive Studies Project »² de novembre 2024, présente la guerre cognitive comme un agrégat de « guerre d'opinion publique, guerre psychologique, guerre juridique et commerciale, guerre diplomatique, guerre technologique et guerre idéologique ». Cette approche très large n'est pas sans rappeler les intuitions des colonels Qiao Liang et Wang Xiangsui dans leur ouvrage de référence « La guerre hors limites » publié en 1999. Cette continuité souligne l'importance, pour les stratèges chinois, de développer des outils afin de contrôler les croyances de l'ennemi par des messages ciblés.

Cette forme de contrôle sur l'adversaire est considérée par les théoriciens chinois comme « potentiellement plus bénéfique que de détruire par la puissance de feu, de prendre le contrôle des

² [Algorithmic Cognitive Warfare: The Next Frontier in China's Quest for Global Influence](#)

troupes ou de conquérir des villes et des territoires ».

Un aspect crucial de cette approche est son caractère permanent : les opérations cognitives sont réparties entre les agences militaires, de sécurité et de renseignement, gommant les frontières entre temps de paix et de guerre. Ainsi, la guerre cognitive est conçue comme un engagement continu et de temps long, bien avant que les premiers soldats ne soient mobilisés ou que les obus ne tombent. Cette continuité-là rend ainsi particulièrement difficile à identifier ou à contrer.

L'IA comme un catalyseur de la lutte informationnelle

Avec l'apparition des médias sociaux et le développement rapide de l'intelligence artificielle, les algorithmes sont devenus des outils capables de « créer un cadre cognitif flexible et de façonner les pensées et la cognition de l'adversaire sans qu'il ne le sache par la diffusion précise de messages tendancieux³».

Les algorithmes sont perçus comme des « contrôleurs », des « portiers » et des créateurs de « cocons d'information ». Cette notion est en réalité beaucoup plus puissante que la simple bulle de filtre car elle repose sur une stratégie de manipulation volontaire des algorithmes par les créateurs de contenus. Le cocon sémantique résulte d'une analyse de l'intention de recherche de l'utilisateur, une extrapolation de l'intention basée sur la sémantique.

L'infrastructure technique sous-jacente aux campagnes de désinformation comprend désormais à côtés des « usines à trolls » hautement organisées, des fermes de robots automatisés (bots), et des systèmes d'IA capables de générer du contenu trompeur à grande échelle. Ces infrastructures matérielles constituent le squelette invisible mais essentiel des opérations d'influence contemporaines et sont essentielles au développement de la guerre cognitive. Les apports

de l'IA sont alors doubles. Ils permettent d'une part d'automatiser un certain nombre de tâches qui auparavant incombaient à des opérateurs humains, simplifiant un aspect important de la guerre de l'information par la création de contenus. D'autre part l'IA permet surtout d'amplifier l'enfermement cognitif par un ciblage affiné des auditoires.

Agissant ainsi sur le ciblage, le développement de récit et l'automatisation de la diffusion, l'IA est aujourd'hui plus qu'un facteur de franchissement de seuil dans la guerre informationnelle mais potentiellement un élément de sa mutation vers la guerre cognitive algorithmique.

Quel modèle opérationnel de la guerre cognitive algorithmique ?

L'analyse des productions sur le domaine laisse entrevoir les apports de l'intelligence artificielle suivant un processus en six étapes :

1. Ciblage et « portrait de l'utilisateur » :

Le traitement algorithmique permet d'identifier les audiences cibles à grande échelle, et d'analyser l'état psychologique individuel comme les tendances sociales. Ce secteur est déjà exploité depuis de nombreuses années pour le marketing mais également dans le cadre des processus électoraux comme le scandale Cambridge Analytica a pu le mettre en lumière dès 2016. Il gagne pourtant en pertinence et change de nature, en particulier par la connexion permanente de nombreux capteurs et la captation continue de données personnelles.

2. « Attirer l'attention » : L'IA génère du contenu personnalisé, basé sur l'état psychologique en temps réel, afin de désarçonner le cadre cognitif existant de l'utilisateur. C'est ici que l'exploitation des biais cognitifs, couplée à un ciblage fin, se révèle particulièrement efficace. L'usage de plus en plus répandu des « chatbot émotionnels » témoigne ainsi de l'emprise potentielle de ces outils.

3. **Suggérer des références** : Une fois le cadre fixé, l'attention captée, l'approche de la guerre cognitive

³ Chen Changxiao, Lee Ho, Feng Mingyue, Shu Shuai,
<https://d.wanfangdata.com.cn/periodical/gfkj202401019>

algorithmique consiste à utiliser les mécanismes de diffusion pour faire apparaître la viralité de certains sujets comme naturelle. En exploitant ainsi certains biais informationnels, les cibles admettent progressivement un nouveau cadre de références.

4. Induire une réaction : Les algorithmes regroupent les individus dans de nouveaux "cocons d'information". En anticipant les recherches potentielles et en présentant des contenus, liens et produits statistiquement susceptibles d'intéresser les audiences et donc de les maintenir dans le « cocon ». On cherche ici, l'interaction avec le contenu, le clic, le « like », le commentaire.

5. Intervention opportune : Des messages spécifiques sont utilisés pour s'assurer que ces interactions évoluent dans la direction souhaitée, maintenant la cible dans son "cocon". C'est dans cette étape une sorte de recadrage de l'interaction qui permet le renforcement induit dans la phase suivante.

6. Superviser la gratification : L'algorithme mesure la gratification sociale des cibles et modèle les dynamiques internes de ces nouveaux regroupements, renforçant l'enfermement dans un cadre cognitif spécifique.

Au cœur de cette nouvelle forme de guerre se trouve les données. Celles-ci sont fondamentales à cette approche algorithmique, et il faut non seulement des données en masse mais des données précises et de qualité. Comme le souligne un chercheur chinois cité dans le rapport : « bien que les algorithmes soient le cœur [de la guerre cognitive algorithmique], l'information de renseignement est la clé ».

Le profilage algorithmique permet donc de concevoir des contenus sur mesure, adaptés à l'état cognitif et psychologique de chaque individu, mais cela implique la collecte et le traitement de vastes quantités de données personnelles : historique d'achat, données de voyage, données de santé, etc. Cette exigence explique en partie certaines

cyberattaques d'envergure attribuées à des acteurs étatiques, visant à alimenter leurs systèmes en données personnelles pour créer des profils complets de citoyens étrangers.

Cette infrastructure de données sophistiquée qui comprend des bases de données comportementales, des historiques de navigation, et des modèles prédictifs capables d'identifier les vulnérabilités cognitives et émotionnelles des populations ciblées est essentielle à ces opérations. La collecte massive de données personnelles n'est donc pas simplement un enjeu de vie privée, mais devient un véritable enjeu de sécurité nationale, transformant les plateformes numériques en potentielles armes informationnelles. Cette matérialité des infrastructures de données pose de nouvelles questions quant à la souveraineté numérique des États et leur capacité à protéger leurs populations des manipulations extérieures⁴.

Défis et perspectives

La propagande massive non ciblée et grossière, si elle n'a pas disparu, ne vise pas à produire les mêmes effets que l'approche cognitive algorithmique qui se développe. L'une cherche à diviser et s'impose comme un instrument des « ingénieurs du chaos », l'autre cherche à modifier les croyances en profondeur. C'est là une différence fondamentale. Ce mécanisme se nourrit par ailleurs, d'un modèle économique hybride où les techniques de persuasion sont autant utilisées pour vendre des produits que pour conduire une campagne d'ingérence lors d'une élection. De nouveaux opérateurs apparaissent, repoussant les limites éthiques et contournant les réglementations et proposent littéralement des services de désinformation.

Dans ce contexte d'affrontement permanent, où l'innovation technologique entraîne un renouvellement constant des pratiques, les forces armées doivent, pour garantir l'efficacité de leurs actions, intégrer une pluralité de facteurs au sein

⁴ Samuel Henry, Quelle matérialité de la désinformation ?
<https://www.diploweb.com/Quelle-materielite-de-la-desinformation.html>



d'une approche multichamps et multimilieux. La mobilisation résolue et massive de l'arme informationnelle par nos compétiteurs exige une refonte profonde de notre concept d'opérations d'information.

La structuration d'une capacité d'influence et de lutte informationnelle au sein des armées représente une occasion décisive de surmonter les résistances culturelles et techniques sans aucun renoncement à notre cadre légal et éthique. Il nous incombe dès lors de promouvoir une culture de l'hybridité, intégrant naturellement des actions indirectes et développant nos propres capacités d'action.

Pour peser dans ce système d'affrontement, plusieurs niveaux d'action sont possibles, mais le combat prioritaire semble être celui de la maîtrise des données. En s'inscrivant en complémentarité d'un dispositif interministériel éprouvé, les armées contribuent pleinement à la prise en compte de cet enjeu vital pour nos démocraties dans l'ère de l'intelligence artificielle.