# Un *design lab.* pour la sécurité cognitive

## Design lab for cognitive security

Axel Ducourneau[1]

[1] ASO - Etat-major des armées - Ministère des armées - France - axel.ducourneau@intradef.gouv.fr

**RÉSUMÉ.** Cet article plaide pour le développement pérenne d'un « *design lab* »sur la sécurité cognitive selon six grands principes : (1) un centrage de l'analyse sur l'acteur, (2) une attitude prospective, (3) une cohérence horizontale et verticale, (4) une agilité dans l'organisation des expérimentations, (5) une rapidité d'exécution et (6) une intégration itérative des résultats dans une perspective de prototypage de solution. Ces six principes combinés soulignent la nécessité pour les opérations cognitives d'être fondées sur une compréhension dynamique de la population ciblée (c'est-à-dire basée sur les concepts et le système de pensée propres aux personnes étudiées), appliquée de manière intégrée et synchronisée dans l'ensemble de « l'organisation » (et de ses partenaires) et dans une temporalité contrainte qui permettent la mise en place d'une stratégie de dissuasion adaptée.

**ABSTRACT.** This article argues for the sustainable development of a design lab for cognitive security based on six key principles: (1) society-centric analysis, (2) a prospective attitude, (3) horizontal and vertical coherence, (4) agility in the organisation of experiments, (5) speed of execution and (6) iterative integration of results with a view to prototyping solutions. These six principles combined underline the need for cognitive operations to be founded on an emic understanding of the target population (*i.e*. based on the concepts and thought systems specific to the people being studied), applied in an integrated and synchronised way throughout the 'organisation' (and its partners) and within a constrained timeframe that enables the implementation of an appropriate deterrence strategy.

**MOTS-CLÉS.** Sécurité cognitive, design lab, C2, prise de décision, ingénierie sociale, dissuasion cognitive.

**KEYWORDS.** Cognitive security, design lab, C2, decision-making, social engineering, cognitive deterrence.

La guerre cognitive recouvre une nouvelle polémologie centrée sur la société et les individus qui la composent et se fait à travers deux leviers principaux : la déstabilisation et l'influence à large échelle [TRI 24]. Le concept de « sécurité cognitive », tel qu'il est compris actuellement dans le monde occidental, est issu de la convergence des travaux portant sur les caractéristiques, limites et fragilités des individus, et sur les influences sociales, culturelles et leurs manipulations à des fins de guerre ou de suprématie [CLA 22].

### 1. la sécurité cognitive, un enjeu de sécurité nationale

D'un point de vue opérationnel, la sécurité cognitive, fait référence aux pratiques, méthodologies et efforts déployés par une nation pour se prémunir des tentatives d'ingénierie sociale - manipulations intentionnelles de la cognition et de la prise de décision, et perturbations de ces dernières par différentes formes d'ingérences étrangères.

Les fondements de la guerre cognitive telle qu'elle est développée dans la vision anglo-saxonne prennent racine dans divers courants issus du post-modernisme français, dont la post-vérité. Le terme est plus largement utilisé depuis 2017, notamment aux États-Unis d'Amérique où il désigne « les moyens d'action qu'un État ou un groupe d'influence utilisent pour manipuler les mécanismes spontanés de la cognition d'un ennemi ou de son peuple, pour l'affaiblir, le pénétrer, voire le soumettre ou le détruire » [GOL 17]. Ce concept de guerre cognitive s'ancre à la fois dans une réflexion historique sur l'évolution des doctrines de propagande, désinformation et de manipulation issues de la guerre froide (notamment des mesures actives soviétiques) et celles nées des deux dernières décennies d'affrontements contre-insurrectionnels et hybrides (en « zone grise »), ainsi que dans les travaux portant sur la militarisation des neurosciences. Il s'agit, dans cette acception, d'un champ disciplinaire nouveau, à la fois héritier de la « *political warfare* », des techniques de soft power, de l'« *information warfare* », et des « *psy-ops* », pour favoriser une présentation biaisée d'une réalité le plus souvent

 

orientée à des fins stratégiques. Ces travaux ont été largement facilités et ont pris une nouvelle dimension avec le développement et la généralisation des technologies numériques [BRO 20], notamment avec l'avènement de la numérisation de l'aide à la décision stratégique, celle de la connaissance des champs opérationnels et l'envahissement des flux massifs de données dans les procédures de C2 (*Command and Control*) civils comme militaires. Il concerne ainsi tout le champ de l'usage numérique et aborde aujourd'hui des dimensions d'ingérence et de contre-ingérence cybernétiques, d'attrition cognitive des individus comme des populations, et de la nécessaire préparation et défense de ceux qui y seraient soumis. Dans ce contexte, la « sécurité cognitive » est à considérer comme un nouveau champ de recherche opérationnelle à part entière [WAL 17].

## 2. La guerre cognitive comme système socio-technique multi-échelle

La difficulté à se représenter un environnement cognitif immatériel, constitué de réseaux d'acteurs, de concepts, d'idées et d'outils technologiques en interaction, nécessite d'en faire une représentation nouvelle, de cartographier cet environnement comme un domaine géographique du monde physique pour le rendre intelligible collectivement.

La guerre cognitive, constituée en système de controverses socio-technique, se mène au travers d'outils d'influence des organisations humaines interconnectées qui doivent prendre des décisions tactiques, opératives et stratégiques en situation d'incertitude et de rationalité limitée. Une particularité de la guerre cognitive réside dans son caractère multi-échelle (de l'individu aux ensembles sociaux les plus complexes, des citoyens aux décideurs étatiques, etc.) et multiculturel (nations, États, communautés identitaires, réseaux sociaux, etc.) s'immisçant à bas niveau dans toutes les strates des organisations sociales, et rendant son approche à la fois complexe, interdisciplinaire et par nature systémique. La guerre cognitive est basée sur une bonne connaissance des techniques d'ingénierie sociale.

L'ingénierie sociale est une expression générique qui englobe, dans une acceptation non normative, tous les dispositifs d'intervention civile et militaire planifiée, élaborés par des experts, visant à modifier des institutions et/ou des comportements dans des contextes variés. Envisager de modifier des organisations, des politiques publiques, des modes de gouvernance à l'échelle nationale, c'est faire de l'ingénierie sociale. Mais surtout, il s'agit d'observer et de s'adapter aux réactions des acteurs impliqués par ces interventions, en particulier ceux à qui elles sont destinées comme ceux qui doivent les exécuter.

Cette définition de l'ingénierie sociale, axée sur le contrôle à large échelle des institutions, est à mettre en regard avec celle définie dans le monde de la cybersécurité où les attaques d'ingénierie sociale visent à manipuler, non plus des institutions mais des individus qui compromettent leur sécurité personnelle ou celle de leur organisation. Selon cette définition, l'ingénierie sociale s'appuie sur la manipulation psychologique et exploite les erreurs ou les faiblesses humaines plutôt que les vulnérabilités techniques ou numériques des systèmes, elle est parfois appelée « piratage humain » (par l'induction de biais cognitifs, d'un sentiment de peur ou d'urgence à agir).

On peut ainsi utiliser, voire orienter ces systèmes socio-techniques, via par exemple la technique du nudge [TAL 09] qui va modifier le design de certains éléments du système. Le *design technique* (*persuasive technologies*) [FOG 99] crée des « affordances » [NOR 02] [GIB 79], c'est-à-dire des propriétés actionnables que l'être humain perçoit dans son environnement, et qui vont diriger ses actions et comportements de manière imperceptible ou peu perceptible, comme cela a été le cas sur des opérations menées par *Cambridge Analytica*, relevant du *dark nudging* et de l'*hyper nudging* [MAD 20] [BAK 20] [YEU 16].

La cartographie des systèmes socio-techniques est donc la première étape afin de créer, de maintenir et d'utiliser des réseaux permettant de mettre en oeuvre de l'ingénierie sociale à fin de guerre cognitive. Une caractéristique importante de ces systèmes est qu'ils changent constamment pour refléter la nature

dynamique de l'environnement. Ainsi, la constitution d'une cartographie réaliste de l'environnement organisationnel des prises de décision, avec la mise à disposition des moyens humains que cela implique, est la pierre angulaire de la résilience cognitive. [WAL 17].

### 2.1. *Guerre cognitive et facteur humain*

Le travail sur les facteurs humains et les relations anthropo-techniques, tout comme celui sur l'efficacité organisationnelle pour l'efficience stratégique et opérationnelle, sont des problématiques opérationnelles largement développées, en France, dans des centres ou écoles dépendants du Ministère des armées, tels que le CEAM (Centre d'Expertise aérienne militaire), le CREA (Centre de Recherche de l'Ecole de l'Air), le CDEC (Centre de Doctrine et d'Enseignement au Commandement, notamment son bureau « champs cognitifs »), ou l'IRSEM (Institut de Recherche stratégique de l'École militaire). Face aux nouvelles menaces cognitives amplifiées par le numérique, et qui ont des implications sur l'ensemble du spectre allant de la définition de l'axe de la recherche, au recueil et au traitement de l'information au renseignement, ou de la planification à la conduite d'opérations, la convergence entre facteur humain et efficacité organisationnelle s'avère une nécessité. L'enjeu majeur de la guerre cognitive pour les armées est de développer un système de compréhension et de visualisation d'environnement multi-domaine (MCM2 – multi-champs–multi-domaines) incluant pleinement le champ cognitif.

### 2.2. *Guerre cognitive, renseignement et planification des opérations*

La production de renseignement pour la guerre cognitive nécessite une capacité à se projeter dans l'environnement cible à long terme et nécessite une fusion considérable d'informations pour créer une image complète intelligible, partageable et sur laquelle s'appuient la décision et l'action. Cela implique de formuler un cadre conceptuel minimisant, voire maîtrisant les biais culturels et cognitifs qui influencent l'observation de la réalité, sa représentation et le partage de cette représentation [HEU 15]. Les analystes du renseignement utilisent une méthodologie pour décrire une réalité aussi précise, détaillée et complète que possible tout en indiquant les niveaux de fiabilité dans l'évaluation et l'examen de ces étapes opératoires, ainsi que les moyens de la partager de façon intelligible dans l'environnement source avec d'autres acteurs. Un effort majeur doit être fait sur la compréhension des failles sociétales que nos compétiteurs utilisent parfaitement pour nous déstabiliser. De même, un système de connaissance élargi aux sociétés (et non pas seulement à la connaissance de l'appareil militaire de nos compétiteurs) doit être organisé pour parer efficacement a la guerre cognitive dont la spécificité est d'être centrée sur la société dans son ensemble.

Une stratégie de sécurité cognitive implique une convergence en amont des phases opératives et tactiques entre les différents services dépendant de différents ministères en charge des opérateurs stratégiques (ministères chargés des Armées, des Affaires étrangères, de l'Intérieur…) ayant un volet influence de politique publique, ce qui implique un lien à définir entre stratégie et organisation interministérielle, voire à considérer la guerre cognitive comme un objet de politique publique globale. Il est alors nécessaire de doter les différents intervenant d'un même dispositif de détection, de formation et de résilience afin d'unifier une réponse unitaire à des menaces qui, par essence, peuvent être autant généralisées que certaines peuvent être ciblées dans des secteurs de fragilité qu'on ne soupçonne pas.

## 3. Créer des outils robustes de connaissance, de formation et d'entraînement pour l'action.

Un des enjeux de la résilience cognitive est de connaître et donc d'explorer différentes formes possibles de systèmes de renseignement, d'information pour la prise de décision stratégique (C2). Les retombées de la recherche pour la défense nationale sont évidentes, mais elles concernent l'ensemble des décideurs, fonctionnaires, élus… en ce sens qu'elles associent les dimensions individuelles et sociales dans tous les champs possibles de la guerre cognitive. Les outils de résilience ne sont pas nombreux, et la réalisation de *design labs* spécifiques aux menaces et à la mise en œuvre d'une sécurité

cognitive peut donc, par une approche multiniveaux et interdisciplinaire, fournir une approche outillée et validée à destination des opérationnel impliqués dans des situations de gestion de crises critiques complexes, réelles ou potentielles.

Les *design labs* pour l'innovation sociétale sont des dispositifs le plus souvent transitoires, permettant de créer un espace commun et fédérateur d'exploration et d'analyse d'un problème complexe à appréhender (en l'occurrence, les manifestations de la guerre cognitive et les modes de résilience associés). Ils sont pour partie une émanation du courant anthropologique porté à l'origine par Bronisław Malinowski à travers « l'observation participante » [PAN 72], méthode anthropologique qui engendra le *design thinking*, popularisé dans les milieux de l'innovation à partir des années 1990 [HAT 00]. Cette approche est depuis éprouvée dans les domaines de la technologie et largement répandue dans l'industrie, notamment pour la transformation des organisations et leur meilleure compétitivité ([BRO 17]; [MAR 09])

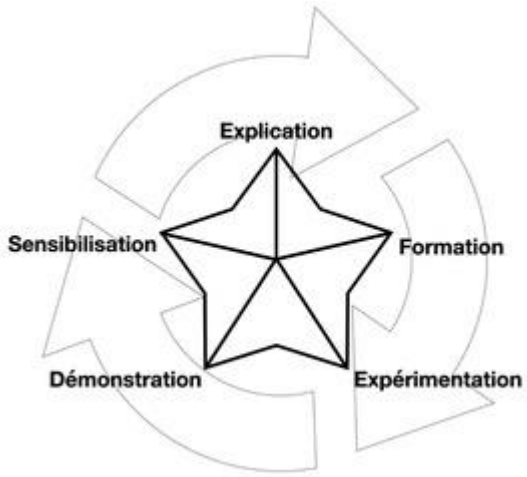


**Figure 1.** *représentation schématique du cycle itératif du* design lab*.*

La mise en oeuvre d'une approche opérationnelle du *design lab* permet d'assurer une complémentarité entre praticiens et chercheurs, selon un cycle itératif (figure 1) de sensibilisation, explication, formation, par la recherche et la démonstration des phénomènes mobilisés. Cela permet à la fois de disposer d'une plateforme dynamique pour la formation et la recherche appliquée.

La méthode utilisée permet d'appréhender des domaines en parallèle et en multi-échelle (de l'organisation d'un C2 à une réponse interministérielle de résilience sociétale). Cela favorise une progression continuelle dans les approches explorées par un raffinement itératif des techniques et méthodes employées. Une telle approche convient particulièrement bien aux systèmes complexes et dynamiques où l'incertitude domine.

Six principes de travail sont associés au *design lab* de guerre cognitive : (1) un centrage sur les acteurs qui permet de focaliser sur l'analyse de systèmes sociotechniques complexes, (2) une attitude prospective pour conserver une ouverture permanente dans la réflexion, (3) une cohérence horizontale d'idéation pour ouvrir le champ des possible et verticale pour recentrer l'analyse sur des solutions concrètes (4) une agilité dans l'organisation des expérimentations et des cas d'usages (5) une rapidité d'exécution qui permet l'adéquation à un contexte opérationnel dynamique (6) l'intégration itérative des résultats dans une perspective de prototypage de solution. Ces six principes combinés soulignent la nécessité pour les opérations cognitives d'être fondées sur une compréhension émique de la population ciblée, c'est-à-dire basée sur les concepts et le système de pensée propres aux personnes étudiées.

Ainsi, les opérations axées sur le comportement humain doivent être fondées sur une analyse complète de la population ciblée, de ses modes de communication et de la dynamique de son environnement. Une compréhension émique des acteurs est essentielle à une conception efficace des changements de comportement. Cela est dû au fait que tout individu ou tout groupe interprète toujours

les récits selon ses propres modèles mentaux, ses propres mythes fondateurs. Ceux-ci induisent des émotions spécifiques qui incitent les gens à agir ou à réagir de telle ou telle manière, d'où leur influence sur le cours et la réussite des opérations. Même si les « émotions » ne font pas partie de la collecte d'informations civiles militaires traditionnelles dans le cadre de la prise de décision, elles doivent être soigneusement analysées (sur le terrain et via les réseaux sociaux) pour comprendre si les interventions prévues seront entravées. Des opérations cognitives bien conçues, axées sur le comportement, doivent pouvoir reconnaître la diversité des populations cibles et leurs différentes motivations, intérêts et idées.

## Conclusion

La complexité de la guerre cognitive doit être abordée selon l'approche itérative du *design thinking* qui est pertinente pour explorer un large champ des possibles en utilisant trois axes : (1) créativité, (2) intelligence collective et (3) outils cognitifs, adaptés pour favoriser l'émergence dialectique (confrontation de la créativité avec le sens critique et la réflexivité). Il s'agit plus précisément de créer un environnement interdisciplinaire, exclusivement dédié à une approche opérationnelle, multi-sectorielle, multi-domaine et inter-ministérielle de la guerre cognitive, pour mettre en oeuvre une dissuasion propre au domaine cognitif, voire adopter une politique publique adaptée.

## Présentation de l'auteur

Axel Ducourneau est docteur en anthropologie, spécialiste de l'ingénierie sociale et officier supérieur de l'Armée de l'Air et de l'Espace au sein de la cellule "Anticipation Stratégique et Orientations" de l'État-major des armées françaises.

Les propos tenus dans cet article et les thèses qui y sont soutenues sont publiés sous la seule responsabilité de l'auteur, et n'engagent ni son institution d'appartenance, ni la revue qui les publie.

## Bibliographie

[BAK 20] BAKIR V., "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting", *Frontiers in Communication*, 3 September 2020.

[BRO 20] BROSE, C., *The kill chain: Defending America in the future of high-tech warfare*. New York (NY, USA): Hachette Books, 2020.

[BRO 17] BROWN T., Change by Design. How Design Thinking transforms Organizations and inspires Innovation. New York (NY, USA): Harper Collins Publishers, 2009.

[CLA 22] CLAVERIE B., DU CLUZEL F. "Cognitive Warfare: The Advent of the Concept of "Cognitics" in the Field of Warfare", in B. Claverie *et al.* (Eds.) *Cognitive Warfare : The Future of Cognitive Dominance.* Neuilly-sur-Seine (FR): NATO Collaboration Support Office, pp.2/1-2/7, 2022.

[FOG 99] FOGG B.J., "Persuasive Technologies", *Communications of the ACM*, vol.42, *n°5*, pp.26-29,1999.

[GIB 79] GIBSON, J.-J., *The Ecological Approach to Visual Perception*. Boston (MA, USA): Houghton Mifflin, 1979.

[GOL 17] GOLDFEIN D.. *General Goldfein Delivers Air Force Update. Air Force Association Air, Space and Cyber Conference*. National Harbor, Sept. 19, 2017.

[HAR 00] HATZFELD H., SPIEGELSTEIN J., *Méthodologie de l'observation sociale*, Paris (FR): Dunod, 2000.

[HUE 15] HEUER R.J., PHERSON R.H., S*tructured analytic techniques for intelligence analysis.* Washington (DC, USA): CQ Press, 2015.

[MAD 20] MADI M.A. *The Dark Side of Nudges*. New-York (NY, USA): Routledge, 2020.

[MAR 09] MARTIN R.L. The Design of Business: Why Design Thinking is the Next Competitive Advantage. Boston (MA: USA): Harvard Business Press, 2009.

[NOR 02] NORMAN D.A., *The design of everyday things*. New York (NY, USA): Basic Books, 2002.

[PAN 72] PANOFF M., *Bronislaw Malinowski*. Paris (FR): Payot, 1972.

[TAL 09] THALER R.H., SUNSTEIN C.R., *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New-York (NY, USA): Penguin Books, 2009.

[TRI 24] CLAVERIE B., TRINQUECOSTE J.-F., "Guerre cognitive et influence psychologique", *Ingénierie Cognitique*. Londres (UK): ISTE, vol.7, *n°1*, 2024.

[WAL 17] WALTZMAN R., *The weaponisation of information : the need for cognitive security*. Washington (DC, USA): Rand Corporation, 2017.

[YEU 17] YEUNG K., "Hypernudge: Big Data as a mode of regulation by design, *Information, Communication and Society*, vol.20, *n°1*, pp.118-136, 2017.