Souveraineté cognitive : le maillon humain de la confiance numérique

Guillaume CHILLET
Psychologue
Responsable du domaine
sciences humaines et sociales
Agence de l'Innovation de Défense

Le pare-feu ne suffit plus

La cybersécurité a considérablement mûri ces dernières années. Les organisations investissent massivement dans la protection de leurs systèmes d'information : firewalls, SOC, détection d'intrusion, plans de continuité. Pourtant, malgré ces arsenaux techniques, les attaques informationnelles continuent de prospérer. Pourquoi ? Parce qu'elles ne visent pas les machines, mais les esprits qui les utilisent.

La désinformation, l'ingénierie sociale, les campagnes de manipulation, qu'elles soient le fait d'acteurs étatiques hostiles, de concurrents ou de groupes idéologiques, exploitent une vulnérabilité que nul antivirus ne peut corriger : les processus cognitifs humains. C'est le collaborateur qui clique sur le lien de phishing. C'est le décideur qui prend une mauvaise décision sur la base d'une information falsifiée. C'est le citoyen dont le vote est influencé par une campagne coordonnée.

La confiance numérique que nous cherchons à construire repose sur deux piliers indissociables : la sécurité des systèmes et la résilience des esprits qui les utilisent. Nous avons beaucoup investi sur le premier. Il est temps de nous intéresser sérieusement au second.

Le territoire mental : une métaphore opérationnelle

Pour rendre tangible cette dimension cognitive de la sécurité, je propose d'utiliser une métaphore que les professionnels de la défense et de la sécurité comprendront intuitivement tout autant que le grand public : celle du territoire.

Chaque individu possède un territoire mental, un espace où se forment ses jugements, ses décisions, ses convictions. Ce territoire a des frontières (ce que nous acceptons ou refusons de considérer), des voies d'accès (nos canaux d'information), des ressources (nos connaissances, notre esprit critique), et des vulnérabilités (nos biais cognitifs, nos émotions, notre fatigue attentionnelle).

Les opérations d'influence et de désinformation sont, dans cette perspective, des tentatives d'intrusion sur ce territoire. Elles cherchent à franchir nos frontières cognitives, à exploiter nos failles, à détourner nos ressources attentionnelles, et ultimement à prendre le contrôle de nos processus de décision.

Cette métaphore n'est pas qu'une figure de style. Elle

permet de transposer au domaine cognitif des concepts familiers aux professionnels de la sécurité : périmètre de défense, détection d'intrusion, analyse de menace, résilience.

Les « monstres informationnels » : taxonomie des menaces cognitives

Dans mon travail sur la résistance cognitive face à la désinformation, j'ai identifié cinq grandes catégories de menaces informationnelles, cinq « déguisements » que prennent les contenus manipulatoires pour franchir nos défenses :

L'Urgentiste exploite notre réactivité émotionnelle. Il se présente sous les traits de l'alerte, de la révélation exclusive, du « vous devez savoir maintenant ». Il court-circuite notre réflexion en activant nos réponses automatiques.

L'Expert autoproclamé usurpe les codes de l'autorité. Il mobilise un jargon technique, des références pseudo-scientifiques, des titres ronflants pour nous faire baisser notre vigilance critique.

Le Tribal joue sur notre besoin d'appartenance. Il divise le monde en « nous » et « eux », transforme toute nuance en trahison, et fait de l'adhésion émotionnelle un substitut à l'examen rationnel.

Le Séducteur flatte nos biais de confirmation. Il nous dit exactement ce que nous voulons entendre, renforce nos convictions existantes, et nous enferme progressivement dans des bulles informationnelles.

Le Brouilleur ne cherche pas à convaincre mais à saturer. Il multiplie les versions contradictoires, sème le doute systématique, jusqu'à ce que nous renoncions à distinguer le vrai du faux.

Reconnaître ces patterns est la première étape d'une défense cognitive efficace.

De la sensibilisation à l'entraînement : changer de paradigme

Face à ces menaces, la réponse dominante reste la « sensibilisation ». On informe les collaborateurs, on leur explique les risques, on leur montre des exemples. C'est nécessaire, mais insuffisant.

Vingt-cinq ans de pratique en sciences cognitive m'ont appris une chose : savoir n'est pas pouvoir. La preuve en est que nous connaissons tous les méfaits du tabac, et pourtant des millions de personnes fument. Nous savons que les biais cognitifs existent, et pourtant nous y succombons quotidiennement.

La différence entre la connaissance et la compétence, c'est l'entraînement. Un pilote de chasse ne se contente pas de lire le manuel de vol, il passe des centaines d'heures en simulateur pour que les bons réflexes deviennent automatiques.

C'est exactement ce dont nous avons besoin en matière de résilience cognitive : des protocoles d'entraînement qui permettent à chacun de développer des réflexes de vigilance, des routines de vérification, des automatismes de questionnement.

J'ai développé à cette fin un protocole simple, *le protocole STOP*, qui peut s'enseigner en quelques heures et se pratiquer très naturellement au quotidien :

- Suspendre : marquer une pause avant de réagir, partager, décider ;
- Tracer : identifier la source, remonter à l'origine de l'information ;
- Observer : examiner ses propres réactions émotionnelles comme des signaux d'alerte ;
- Prendre du recul : chercher des perspectives alternatives, consulter des sources contradictoires.

Ce n'est pas un rituel magique, mais de l'hygiène cognitive, aussi simple et aussi fondamentale que de se laver les mains.

Résistance individuelle, résilience collective : l'enjeu stratégique pour l'entreprise

Pour les organisations, la résistance cognitive individuelle n'est pas qu'une affaire de protection personnelle. Elle constitue le fondement même de la résilience collective dans un environnement concurrentiel saturé d'opérations d'influence.

Une entreprise fonctionne comme un organisme cognitif où chaque collaborateur joue le rôle d'un capteur et d'un processeur d'information. Lorsqu'un cadre dirigeant fonde sa stratégie sur des informations délibérément biaisées concernant un concurrent, lorsqu'un commercial se laisse influencer par des rumeurs orchestrées sur son propre produit, lorsqu'une équipe se déchire sur la base de fuites fabriquées, c'est toute l'intelligence collective qui se dégrade. Dans chacun de ces cas, ce n'est pas un système informatique qui a été compromis, mais un cerveau humain qui a été manipulé.

Cette vulnérabilité cognitive génère des coûts invisibles mais considérables : heures perdues à démêler le vrai du faux dans les flux informationnels, décisions stratégiques fondées sur des prémisses erronées dont les conséquences ne se révéleront que des mois plus tard, climat de défiance interne alimenté par des rumeurs circulant sans filtre, fuite des talents vers des environnements perçus comme plus sains informationnellement.

Inversement, lorsque les réflexes de résistance cognitive se généralisent dans une organisation, celle-ci développe une forme d'intelligence collective plus robuste, moins manipulable, plus capable de distinguer le signal du bruit. Chaque collaborateur doté d'une meilleure hygiène cognitive contribue à élever le niveau général de discernement. Les rumeurs circulent moins vite, les décisions se fondent sur des bases plus fiables, les crises provoquées par de fausses informations deviennent plus rares.

Plus encore, cette résistance cognitive crée une incitation sociale positive. Dans une organisation où chacun pratique le doute méthodique et la vérification des sources, celui qui propage une rumeur non vérifiée perd en crédibilité. Celui qui fonde une argumentation sur des sources douteuses voit sa légitimité s'éroder. La souveraineté cognitive cesse alors d'être une compétence individuelle pour devenir une norme collective, un standard de fonctionnement partagé.

Dans un environnement où l'information est simultanément l'arme principale et le terrain de bataille de la guerre économique, l'entreprise qui voit plus clair dispose d'un avantage décisif. Elle décide mieux parce qu'elle s'appuie sur des analyses moins polluées. Elle réagit plus justement parce qu'elle distingue les véritables menaces des alarmes fabriquées. Elle anticipe avec plus de précision parce qu'elle détecte les signaux faibles pertinents dans le bruit ambiant. Investir dans la résistance cognitive de ses collaborateurs, c'est investir dans le capital humain le plus précieux : la lucidité.

On peut oser un parallèle qui n’est pas anodin avec la crise sanitaire. Quand le COVID-19 a déferlé sur nos sociétés, nous avons collectivement appris à nous protéger. En quelques semaines, des gestes nouveaux sont devenus des réflexes : se laver les mains, porter un masque, maintenir une distance. Nous avons compris que notre comportement individuel avait un impact collectif, que protéger les autres, c'était aussi se protéger soi-même.

Face à la pandémie informationnelle, notre réaction a été tout autre. Nous avons contemplé la vague arriver et nous l'avons accueillie les bras ballants. Pas de gestes barrières, pas de distanciation critique, pas de réflexe de protection. Nous avons laissé les contenus toxiques circuler librement dans nos

esprits, les partager sans filtre, contaminer nos proches. Et nous continuons de le faire.

L'ironie est cruelle : le COVID lui-même a été l'un des plus grands vecteurs de désinformation de l'histoire récente. Nous avons su nous protéger du virus biologique, mais pas des rumeurs sur le virus. Nous avons appris à désinfecter nos mains, mais pas à filtrer ce qui entre dans nos têtes.

Il est temps d'appliquer à l'information la même rigueur que nous avons su mobiliser face au virus : des gestes simples, répétés, collectifs. Le *protocole STOP* est l'équivalent cognitif du lavage de mains, une routine d'hygiène mentale qui, pratiquée par chacun, protège tout le monde.

La souveraineté cognitive comme enjeu de sécurité nationale

Au-delà de la protection individuelle, la résistance cognitive des citoyens est un enjeu de souveraineté nationale. Les démocraties reposent sur la capacité des citoyens à former des jugements éclairés. Quand cette capacité est compromise, par la saturation informationnelle, par la manipulation émotionnelle, par l'érosion de la confiance dans les institutions, c'est le fondement même du contrat social qui vacille.

Les adversaires de nos démocraties l'ont bien compris. Les opérations d'influence étrangères ne cherchent plus seulement à promouvoir un narratif particulier, elles visent à fragmenter le débat public, à polariser les opinions, à rendre impossible tout consensus. L'objectif n'est plus de convaincre, mais de paralyser, d'empêcher.

Face à cette menace, la réponse ne peut pas être seulement technique ou institutionnelle. Elle doit mobiliser chaque citoyen comme acteur de sa propre défense cognitive. Non pas pour lui dire quoi penser, ce serait remplacer une manipulation par une autre, mais pour lui donner les moyens de penser par lui-même, de résister aux pressions informationnelles, d'exercer pleinement sa souveraineté sur son propre jugement.

Recommandations pour une stratégie de résilience cognitive

Pour les organisations, publiques comme privées, qui souhaitent intégrer cette dimension cognitive à leur stratégie de sécurité, je propose plusieurs axes de travail :

Cartographier les vulnérabilités cognitives de l'organisation, au même titre que les vulnérabilités techniques. Quels sont les processus de décision critiques ? Quels collaborateurs sont les plus exposés à l'influence ? Quels biais organisationnels peuvent être exploités ?

Former et entraîner, pas seulement sensibiliser. Intégrer des exercices pratiques de résistance cognitive aux programmes de formation existants. Simuler des attaques informationnelles comme on simule des incidents cyber.

Créer des processus de vérification pour les informations critiques. Instituer des délais de réflexion, des contre-analyses systématiques, des « red teams » informationnelles.

Cultiver la diversité cognitive dans les équipes de décision. Les groupes homogènes sont plus vulnérables aux biais de confirmation et aux bulles informationnelles.

Assumer la dimension humaine de la cybersécurité. Les fonctions RSSI et DRH doivent travailler ensemble. La sécurité des systèmes et la résistance des esprits sont les deux faces d'une même médaille.

Conclusion : défendre le territoire, tous les territoires

La confiance numérique que nous cherchons à construire ne sera jamais complète tant que nous protégerons les machines en oubliant les esprits. La cybersécurité du XXIe siècle doit intégrer pleinement

sa dimension cognitive, mais pas comme une notion abstraite.

Chaque collaborateur, chaque citoyen, chaque décideur est un maillon de cette chaîne de confiance. Leur donner les moyens de défendre leur territoire mental, c'est renforcer la résilience de l'ensemble de l'édifice.

La souveraineté cognitive n'est pas un luxe philosophique. C'est la condition de toutes les autres souverainetés, y compris numériques.

Guillaume CHILLET est l'auteur de l'ouvrage « Petit traité de souveraineté cognitive » (2026) - disponible sur Amazon.