

ESG EXECUTIVE
MBA Cybersécurité et Management Stratégique
des Risques de l'Information



Note de contribution

Ingénierie cognitive & cybersécurité :
nos fonctions cérébrales à la merci des cyber-attaques

par Clément Donzel

Date de soutenance : Janvier 2025

Sous la direction de :

Olivier Feix

Michel Juvin

« Nous héritons d'émotions qui n'ont pas évolué depuis le paléolithique, d'institutions médiévales et de technologies divines ». C'est ainsi qu'Edward O. Wilson, père de la sociobiologie, résume le triple défi auquel sont confrontées nos sociétés modernes¹.

Nos connaissances actuelles sur les mécanismes du fonctionnement cérébral auraient dû nous permettre de nous émanciper de nos vulnérabilités intrinsèques telles que nos biais cognitifs, nos perceptions du risque, la gestion de nos émotions et nos dissonances cognitives. Au lieu de cela, tirant profit du narratif commercial de la révolution technologique permanente prônée par les acteurs du numérique, des entités malveillantes, attirées par l'appât du gain ou la volonté de déstabilisation se saisissent de la numérisation à marche forcée de nos sociétés pour exploiter les failles humaines et technologiques. Face à cette course à l'innovation, les institutions publiques et les législateurs semblent dépassés et peinent à repenser le cadre légal.

Le cerveau humain devient une commodité que l'on peut contrôler pour influencer nos décisions et manipuler nos émotions. Cette emprise n'est pas seulement un risque qui érode notre vie privée et notre libre arbitre, c'est aussi une menace pour nos démocraties dont la stabilité et le vivre-ensemble sont compromis par des logiques économiques qui tendent à fragiliser nos mécanismes de défense, à abaisser notre conscience sociale et individuelle et à appauvrir notre sphère informationnelle.

Chaque jour apporte son lot de plateformes numériques piratées par des cyberattaquants emportant avec eux toujours plus de données confidentielles et de salariés manipulés par des hackers ingénieux. Loin de se limiter à la sphère commerciale, l'ingénierie cognitive est exploitée par des groupes terroristes et des organisations mafieuses, parfois sponsorisées par des États (Métézeau, 2024²). Ces attaques ne cessent de se perfectionner à mesure que l'augmentation de l'étendue de nos connaissances et que la meilleure maîtrise des technologies permettent d'améliorer l'efficacité des techniques de persuasion, d'influence ou de manipulation.

Loin d'être le « problème situé entre la chaise et le clavier » comme le dit l'adage informatique, l'humain, acteur de l'interface numérique, est le dernier rempart contre les bandits modernes. Mieux formé, plus conscient des enjeux et des techniques utilisées par les délinquants cybernétiques, il

¹ Edward Osborn Wilson, *The origins of Creativity*, Penguin (2017), p.90.

² Frédéric Métézeau (2024), Quand les puissances étrangères ciblent les outre-mer français, Radiofrance.fr [Consulté le 16 mai 2024], adresse URL : <https://www.radiofrance.fr/franceinter/quand-des-puissances-etrangeres-ciblent-les-outre-mer-francais-5403867>

pourra, aidé par la technologie, non seulement s'en prémunir mais participer activement à détecter des anomalies et proposer des remédiations aux entités dont il dépend.

Les solutions existent. En développant par exemple l'intelligence émotionnelle qui doit rejoindre l'arsenal de la cybersécurité. Les capacités à faire preuve de pleine conscience et de métacognition³, à maintenir un état de bonheur stable, à exercer l'empathie envers les autres et à démontrer une résilience face aux adversités, sont cruciales pour créer des environnements numériques sécurisés.

Développer un regard analytique et un esprit critique adapté à l'évolution de nos sociétés est essentiel pour évoluer dans un monde VUCA⁴. En éduquant et en sensibilisant aux différents risques cyber, en régulant les atteintes à nos mécanismes cérébraux, en favorisant la transparence algorithmique, en réinstaurant le rôle clé des *gatekeepers*⁵ et en protégeant nos mécanismes d'autocorrection, nous pouvons remettre l'humain au centre du jeu numérique.

Favoriser une forme d'agentivité⁶ et de réflexivité⁷, intégrer le facteur l'humain dans le développement des outils numériques et des interfaces cerveau-machine, tenir compte de nos vulnérabilités, sont non seulement souhaitables mais seront déterminants pour assurer un avenir stable pour les générations à venir. Ce mémoire vise à livrer une contribution dans le but de mieux cerner les défis actuels et futurs et propose des pistes de réflexion pour que nos fonctions cognitives ne soient plus à la merci des cyberattaques.

³ La métacognition consiste à avoir une activité mentale sur ses propres processus mentaux.

⁴ VUCA: Volatility, Uncertainty, Complexity & Ambiguity. Acronyme basé sur les théories de Bennis & Nanus.

⁵ Les *gatekeepers* sont des professionnels de l'information, journalistes, médias indépendants, chargés de hiérarchiser et gérer l'accès à une information.

⁶ L'agentivité correspond à la capacité à agir sur le monde, donc à produire des effets causaux sur lui.

⁷ Éléments internes, externes et collectifs qui favorisent chez l'utilisateur une prise de recul.