Neuralink : derrière la science-fiction, la « neurosécurité »

Thibault RENARD
Senior advisor - CyberCercle
Expert – Comptoir Prospectiviste

Les investissements dans les « neurotechs » se multiplient. Une course mondiale avec pour ligne d'arrivée la connexion directe à notre cerveau est lancée. Côté américain sont en lice NeuraLink dirigée par l'emblématique Elon Musk, Synchron, soutenue par ses rivaux Bill Gates et Jeff Bezos, Blackrock Neurotech, Motif Neurotech ou encore BrainGate. En France, on trouve les équipes de CEA Clinatec. Quant à la Chine, son ministère de l'industrie et des technologies de l'information a affiché son objectif de mettre des produits sur le marché dès 2025…

Sur cette thématique des Interfaces Cerveau-Ordinateur (ou Brain Computer Interface - BCI) à visée pour l'instant thérapeutique il semble que, concernant les implants cérébraux d'interfaces directes neuronales, Neuralink ait pris l'avantage. Après l'obtention d'une autorisation en septembre 2023, Neuralink a procédé à l'implantation d'une puce cérébrale sur son premier patient humain en janvier 2024. Fidèle à ses coups de communication et ses excès d'optimisme, ravi du bilan concluant et espérant que la stabilité du patient soit pérenne, Elon Musk avait déclaré à l'occasion avoir pour objectif *« de traiter des pathologies ou handicaps comme l'obésité, l'autisme, la dépression ou encore la schizophrénie »*. La fonction première de ces puces étant de capter les schémas de pensée associés au mouvement, fin mars 2024 Neuralink diffusait une vidéo de Noland Arbaugh, 29 ans et tétraplégique, alias "P1" (le "1er patient" implanté). Grâce à un implant cérébral lui permettant de contrôler la souris d'un ordinateur, ce dernier racontait jouer aux échecs, aux jeux vidéo Mario Kart et Civilization VI, ou encore prendre des cours de japonais et de français. Synchron de son côté se déclarait en avril 2024 prête pour mener à grande échelle un essai clinique de sa propre puce cérébrale.

Et la cybersécurité ?

Dans ce contexte d'annonces tonitruantes, les débats et questionnements sont nombreux sur ce nouveau sujet de société des cerveaux « augmentés », quand bien même ce serait à visée thérapeutique. Cette forme de transhumanisme, soutenue par les leaders de la Silicon Valley, entre en résonnance avec un imaginaire collectif marquée par le « cyberpunk » et la crainte de l'avènement d'un monde dystopique. Soupçonnée de masquer sa démarche commerciale derrière une approche humaniste, elle se voit souvent condamnée dans le monde intellectuel ou technologique pour des raisons philosophiques, morales ou politiques. S'y ajoutent les questions de bioéthique, de la nécessité ou non d'être invasif, de maltraitance animale

concernant les cobayes (ayant conduit au lancement d'une enquête fédérale contre Neuralink). Mais parmi les milliers d'articles sur le sujet, les questions de cybersécurité sont rarement évoquées. Le « brainjacking », soit la prise de contrôle de l'implant électronique cérébral d'une tierce personne, n'est-il un fantasme de geek ? Ou faut-il s'attendre à des scénarii de science-fiction devenant réalité à base de piratage de « cyber-cerveaux » comme dans le manga *The Ghost in the Shell* ? Rapide tour d'horizon des enjeux de cybersécurité pointés par les experts, autour d'un sujet qui, s'il tient de la prouesse d'un point de vue médical, s'avère inversement d'une certaine rusticité du point de vue sécurité.

Vers des *« cyberattaques neurales »* ?

Une première évidence s'impose : une puce cérébrale n'est jamais qu'un objet connecté comme un autre. Intuitivement, le risque le plus évident et spectaculaire est donc le piratage de la puce. Cela demeurerait un véritable défi pour le pirate, car il devra comprendre son système d'exploitation, disposer d'une proximité physique, d'une connaissance approfondie de son fonctionnement... mais rien de techniquement irréalisable. Avoir un objet connecté lié à notre cœur ayant sans doute autant d'enjeux symboliques et médicaux que relié au cerveau, il suffit de se pencher sur le cas des défibrillateurs cardiaques connectés, dont la « piratabilité » était pointée dès les débuts des années 2010, avec même des démonstrations en 2018. L'ancien vice-président américain Dick Cheney avait même reconnu, lors d'une interview accordée à l'émission 60 Minutes, avoir dû désactiver la fonction sans fil de son défibrillateur pour éviter les tentatives de piratage. Les indentifications de vulnérabilités accompagnées de mises à jour dans le domaine sont donc déjà régulières, comme récemment le 20 septembre 2022 où la Food & Drug Administration (FDA) avait par exemple publié un bulletin d'alerte concernant une vulnérabilité dans le système de pompe à insuline Medtronic MiniMed. Par ailleurs, sans même avoir besoin de causer des dommages physiques ou tromper l'interface, un piratage permettrait d'accéder à des informations médicales personnelles, voir même accéder à « l'historique » des activités d'un utilisateur. Et même si cette première puce de Neuralink ne joue qu'un rôle d'émetteur vers un ordinateur, que des puces influencent directement notre cerveau n'est qu'une question de temps. Des *« cyberattaques neurales »* sont donc d'ores et déjà envisagées par les chercheurs…

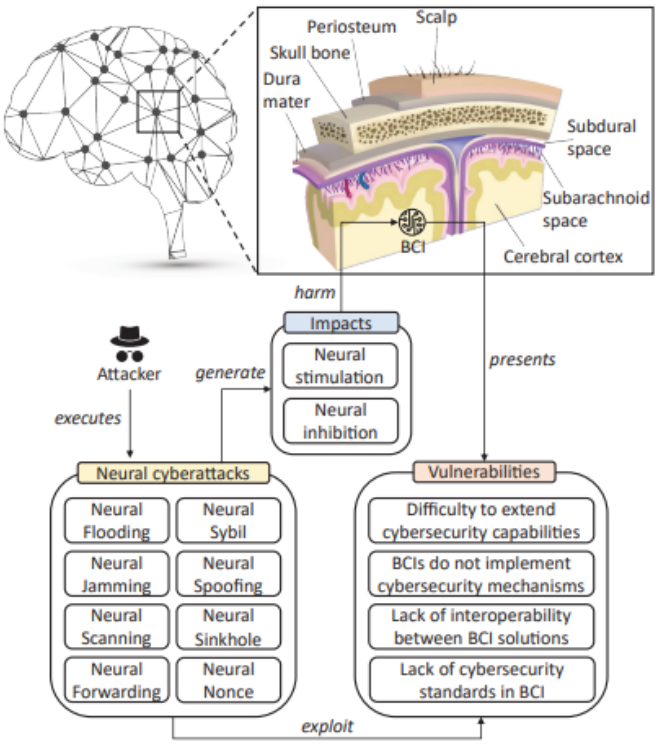


Figure 1: Attacker executing the proposed neuronal cyberattacks that exploit vulnerabilities of invasive neuromodulation BCIs and generate particular impacts on the BCI.

Extrait de Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity, *Communications of the ACM Volume 66 Issue 4pp 68–78* https://doi.org/10.1145/3535509

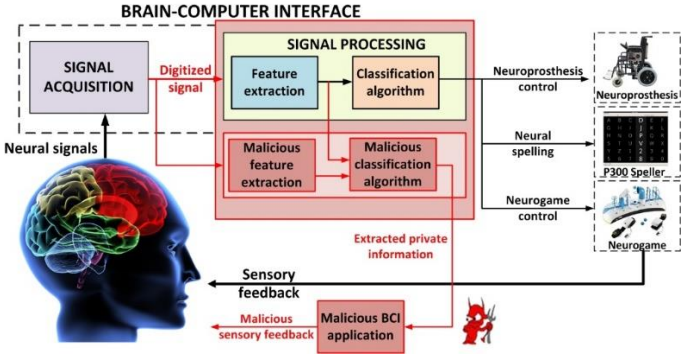
Vers une *neurosécurité* ?

Mais au-delà de la puce elle même et de la fascination qu'elle exerce, et quand bien même le dispositif ne serait pas invasif, c'est finalement d'une interface cerveau-ordinateur dont il s'agit. L'autre faille peut

donc venir de l'interface avec laquelle interagit la puce. De nombreux experts estiment que le talon d'Achille résidera plutôt dans un piratage de l'API (Application Programming Interface, ou interface de programmation d'application) de l'ordinateur connecté, permettant de donner l'impression que l'utilisateur émet des commandes qu'il n'émet pas, ou inversement un jour de manipuler la puce elle-même.

Par ailleurs, de manière bien plus triviale, le concept dans sa dimension thérapeutique étant de rendre de l'autonomie à l'utilisateur, Neuralink elle-même communique sur la perspective que ses patients pourront un jour interagir avec leur ordinateur, mais aussi leur propre smartphone. Elon Musk, jamais avare de promesses, promet par exemple que les applications liées à Neuralink seront compatibles avec Apple iOS ou encore Google Android. Mais qui dit interaction entre votre smartphone et un objet, quand bien même ce serait une puce dans votre cerveau, le plus probable sera de passer par exemple par une connexion Bluetooth. Et si le protocole Bluetooth est considéré comme sûr, à nouveau son piratage n'a rien d'insurmontable…

Quel que soit l'angle d'attaque, connexion ou API, la cybersécurité des Brain-Computer Interfaces (BCI) sera donc la « nouvelle frontière » des pirates. Il s'agit désormais d'un champ de recherche à part entière, au sein de ce que certains appellent la « neurosécurité ».



BCI Security, par l'UW BioRobotics Laboratory
https://wp.ece.uw.edu/brl/neural-engineering/bci-security/

Quid des données ?

Se posera également immanquablement la question des données, qui ne seront vraisemblablement ni stockées sur la puce, ni dans votre smartphone ou votre ordinateur, mais bien sur le cloud. Que deviendront ces données ? Neuralink et ses rivaux n'ayant pas vocation à être éternellement des œuvres philanthropiques mais bien commerciales, elles seront un jour partagées ou revendues. Le piratage, la falsification ou les leaks des bases de données elles-mêmes sont donc parfaitement envisageables, ce type de données ayant une forte valeur, ne serait-ce que symbolique. Et bien sûr, l'usage de ces données par les IA fera partie intégrante de la problématique.

Comme on peut le voir, les pistes de réflexions autour de la sécurité ne manquent pas, et aucune ne relève de la science-fiction.

Le magazine Futur Hebdo s'était amusé à dater la première faille de neuro-sécurité avérée au 5 octobre 2065. Les Interfaces Cerveau-Ordinateur, quelles que soient leurs formes, vont néanmoins et de toute évidence intégrer et envahir notre quotidien bien plus tôt que nous le pensions. Etrangement, cette date elle-même de 2065 apparait désormais comme particulièrement optimiste. Mais les réflexions autour de la neurosécurité restent cantonnés aux experts. Le côté presque anecdotique du débat autour de la dimension cybersécurité des avancées de Neuralink et de ses consœurs est révélateur, comme si ces questions relevaient soit toujours de l'imaginaire et de la science-fiction, soit seront de toute façon in fine prises en compte au moment de la commercialisation, et pas en amont. Les leçons issues des dégâts que l'on constate seulement aujourd'hui des *« technologies persuasives »* inventées il y a déjà 20 ans, n'ont de toute évidence pas été tirées. Mais il n'est pas trop tard pour éviter que la neurosécurité, et notamment sa dimension

cyber, demeure le parent pauvre des débats autour du design de nos cerveaux, actuels ou bientôt « augmentés ».

Une *« neurosecurity by design »* reste à inventer.

Aller plus loin *:*

Une première faille de neuro-sécurité avérée ?, FuturHebdo, 05/10/2065
https://www.futurhebdo.fr/05102065-premiere-faille-de-neuro-securite-averee/
Can Neuralink Be Hacked? Cybersecurity Experts Weigh-In, Compass IR Compliance 04/02/2024
https://www.compassitc.com/blog/can-neuralink-be-hacked-cybersecurity-experts-discuss-potential-risks
Mindhacker: Security & Privacy Risks of Brain-Computer Interfaces, Journal of High Technology Law, 12/11/2020
https://sites.suffolk.edu/jhtl/2020/11/12/mindhacker-security-privacy-risks-of-brain-computer-interfaces/
What are the security implications of Elon Musk's Neuralink ?, CSO 01/08/2019
https://www.csoonline.com/article/567573/what-are-the-security-implications-of-elon-musks-neuralink.html
Hacking Humans: How Neuralink May Give AI The Keys To Our Brains, Forbes, 28/11/2020
https://www.forbes.com/sites/forbestechcouncil/2020/11/18/hacking-humans-how-neuralink-may-give-ai-the-keys-to-our-brains/?sh=21e3bc25791d
Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics Inf Technol 18, 117–129 (2016).
https://doi.org/10.1007/s10676-016-9398-9