La Cybersécurité à l'ère de l'Augmentation Humaine

Auteur : Dr. Olivier BUCHHEIT, Sonopraxis

WG-3 EFCSE

EUROPEAN CYBER SECURITY MONTH

Be secure,

Be critical

A propos de l'auteur

Olivier BUCHHEIT

Généraliste en mécanique et matériaux, docteur en physique du solide, et musicien passionné. Ses formations académiques à Metz puis Nancy l'ont amené à travailler pendant 14 ans au sein du LIST (Luxembourg Institute of Science and Technology), dans les domaines des Matériaux, des Interactions Homme-Machine, de l'Intelligence Economique et de l'Innovation.

Actuellement médiateur technologique et scientifique dans l'enseignement secondaire et supérieur, ainsi qu'auprès d'instituts privés, publics, et du grand public, dans le domaine du digital (4.0, Intelligence Artificielle, Blockchain, Interaction Homme-Machine…).

Il est maintenant parfaitement établi que le digital est une (sinon *la*) modalité essentielle de notre développement socio-économique contemporain – et ce à l'échelle planétaire. Il aura fallu à peine quarante ans pour que la micro-informatique s'installe dans pratiquement la totalité des domaines de la connaissance et de l'action humaine, d'une manière ou d'une autre ; et un peu plus de vingt ans, pour qu'Internet connecte l'ensemble de la planète à tous les étages… allant jusqu'à se loger dans nos poches via les smartphones, nos poignets avec les montres connectées et nos yeux par les lunettes connectées. C'est ainsi l'ensemble des acteurs de la société (citoyens, professionnels, gouvernances et consommateurs de tous bords et de toute nation), et tout particulièrement des PME, ETI et organisations publiques, constituant un maillage fin au plus près des individus, qui composent maintenant quotidiennement avec ces technologies multi-usages (*general purpose technologies*[1]) que forment l'informatique et Internet.

Dans ce contexte de digitalisation ultra-galopante, la cybersécurité est devenue un enjeu *majeur* : de la protection des données personnelles de chaque individu dans le cadre d'une marchandisation frénétique de la data (véritable pétrole digital, alimentant un marketing chaque jour plus malin, ingénieux, intrusif ; nourriture première du Big Data, un des plus puissants piliers de la fameuse transformation 4.0 que nous vivons actuellement, et de l'Intelligence Artificielle), à l'espionnage industriel et étatique (voire le cas de Huawei et de la position américaine sur le sujet[2]), en passant par la cyberguerre (*cyberwarfare*[3]) comme nouveau terrain d'affrontement entre les nations, les diasporas d'activistes[4], ou encore les pirates isolés cherchant à détrousser l'internaute lambda au détour d'un clic sur la toile[5].

En parallèle de ce développement phénoménal du cyberespace avance un puissant courant de pensée, identifié depuis longtemps dans la littérature, le cinéma, et toutes autres formes de l'art de l'anticipation, et maintenant devenu une réalité parfaitement

[1] Bresnahan Timothy F., Trajtenberg, «General Purpose Technologies: Engines of Growth?», *Journal of Econometrics,* 65 (1995), 83-108
[2] https://www.theverge.com/2019/5/19/18631558/google-huawei-android-suspension
[3] https://searchsecurity.techtarget.com/definition/cyberwarfare
[4] https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-tokyo-narita-airport-whaling-protest-take-down-ddos-a6832481.html
[5] https://sensorstechforum.com/remove-jigsaw-ransomware-and-restore-fun-kkk-btc-encrypted-files/

tangible, très largement soutenue et développée par nombre d'acteurs et héros majeurs du Business comme par exemple Google, Facebook ou Elon Musk : le Transhumanisme.

Prenons le temps d'un petit tour d'horizon sur le sujet avant d'aller plus loin.

L'augmentation humaine *at a glance*

Philosophie de la technoscience au service du dépassement de la condition humaine (« l'amélioration humaine » via la modification sélective du génome humain, l'Internet-of-Things dans la chair, la fusion plus ou moins forte de l'humain et de la machine, ou encore, l'usage de puces informatiques dans le cerveau - le silicium comme dopage cognitif *in-situ*), ce courant est maintenant parfaitement installé dans notre réalité actuelle, et à venir. Il ne s'agit plus de simples fantasmes ou cauchemars Hollywoodiens, mais bien de puissantes lames de fond participant très activement à l'élaboration de notre société - et plus largement, à l'élaboration de la socio-économie à l'échelle planétaire.

Pour preuve, entre 2003 et 2009, plusieurs rapports d'analyse conséquents sur le sujet ont été produits par certaines des plus puissantes instances gouvernementales (la National Science Fondation[6] et le Conseil de Bioéthique aux USA[7], la Commission[8] et le Parlement[9] dans l'Union Européenne. Pour un aperçu global et concis, voir la publication de Gilbert Hottois sur le sujet[10]). Devenue alors sérieusement considérée par notre gouvernance, la pensée transhumaniste s'est depuis singulièrement concrétisée dans le champ du possible, voire même, pour nombre d'entre nous, dans le champ du *désirable et nécessaire* (comme dans le cas du rapport de la NSF par exemple, à la position largement technophile). Avec pour credo central, la convergence des Nanotechnologies, des Biotechnologies, des Technologies de l'Information et des Sciences

[6] Roco M.C., Baindridge W.S., « Converging Technologies for Improving Human Performance – Nanotechnology, Biotechnology, Information Technology and Cognitive Science », NSF, Juin 2002
[7] Fukuyama F. et al., « Beyond Therapy : Biotechology and the Pursuit of the Happiness", Council on Biotechics, Octobre 2003
[8] Nordmann A. et al., « Converging Technologies – Shaping the Future of European Societies", Commission Européenne, 2004
[9] Coenen C. et al., « Human Enhancement – Study », Parlement Européen, Mai 2009
[10] http://www.redalyc.org/pdf/1892/189230852011.pdf

cognitives (connues sous l'acronyme NBIC) – soit, l'utilisation symbiotique du fleuron de nos avancées technoscientifiques depuis le milieu du XXème siècle.

Ont suivi, pêle-mêle, l'Université de la Singularité co-fondée par Ray Kurzweil[11] et financée par notamment Google, CISCO, Nokia…[12], la mouvance du biohacking[13], l'émergence d'un parti politique aux USA en 2016[14] (aux résultats encore insignifiants, mais cela n'est à priori qu'une question de temps), ou encore la question du droit des cyborgs posée de plein fouet au juridique[15].

Dans le monde économique, Gartner[16], une des références s'il en est du *business intelligence* de la technoscience, plaçait en 2017 l'augmentation humaine comme une « technologie en début de hype » ; une année plus tard, ce courant a été segmenté en diverses technologies filles (preuve de sa maturité) et le fameux biohacking classé comme une des

> « 5 Technologies trends that will blur the lines between Human and Machine : 2018 is just the beginning of a "trans-human" age where hacking biology and "extending" humans will increase in popularity and availability"[17].

2019 poursuit naturellement la tendance.[18]

Notons enfin la présence du mouvement transhumaniste lors du sommet de Davos de cette année, dédié à la Transformation 4.0, par notamment la présence de WISeKey,

[11] Scientifique et entrepreneur de renom outre-Atlantique, une des premières figures du mouvement Transhumaniste - http://www.kurzweiltech.com/aboutray.html
[12] https://su.org/about/leadership/
[13] Ajout de nouvelles fonctionnalités au corps humain par modifications biologiques, implants électroniques, ou mécatroniques : la détection du Nord par un capteur vibrant accroché à la surface de la peau, le développement de la vision nocturne par injection de substances dans le globe oculaire, ou encore le puçage d'employés volontaires leur permettant d'ouvrir une porte ou de déclencher la photocopieuse par simple contact de la main.
[14] http://transhumanist-party.org/
[15] https://bodyhacks.com/rich-lee-first-victim-anti-transhumanism/
https://www.gofundme.com/f/cyborgdad
[16] gartner.com : "Gartner, Inc. is a global research and advisory firm providing insights, advice, and tools for leaders in IT, finance, HR, customer service and support, legal and compliance, marketing, sales, and supply chain functions across the world"
[17]https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

[18]https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/

acteur suisse de la cybersécurité, dont le CEO est auteur d'un livre pro- sur le sujet[19], et qui a animé sa seconde table annuelle (« transHuman Code meeting of Minds Roundtable ») sur « l'humain comme point de pivot de *l'Internet du Tout* ». Table ronde réunissant des techno-évangélistes divers et variés comme des collaborateurs du MIT, de l'ICANN, de la finance, de la Blockchain, de l'Intelligence Artificielle…[20]

Comme toute philosophie, il existe de nombreux courants à cette pensée, du plus soft (capteur à la surface de la peau) au plus hard (immortalité, mind-uploading, post-humanisme). Les questions posées par ce mouvement sont abyssales, les enjeux socio-économiques, vertigineux, et les deux premières puissances économiques mondiales dans l'arène, les USA et la Chine, parfaitement en course sur le sujet (la boite de Pandore du *designer baby* ouverte par Lulu, Nana et le CRISPR-Caas9[21], la suprématie militaire via le supersoldat en tête des études expérimentales[22]).

Il ne s'agit là que d'un infime tour d'horizon de cette philosophie du dépassement de la condition humaine, visant à poser rapidement le décor et à montrer que ce sujet est maintenant à considérer *avec le plus grand sérieux par l'ensemble de la société*.

Concentrons-nous maintenant sur l'objet de cette communication : la cybersécurité dans ce contexte.

[19] transhumancode.com : « Transhuman Code, Managing the future of humanity and technology towards the 4th Industrial Revolution »
[20] https://www.wisekey.com/press/wisekey-to-lead-groundbreaking-2019-davos-cybersecurity-and-transhuman-code-roundtables-focusing-on-the-human-as-the-fulcrum-of-the-internet-of-everything/
[21] https://www.apnews.com/4997bb7aa36c45449b488e19ac83e86d
Les USA ont communiqué sur leurs travaux au niveau du blastocyste : https://www.nationalgeographic.com/news/2017/08/human-embryos-gene-editing-crispr-us-health-science/
[22] https://www.popularmechanics.com/military/research/a23457329/augmented-super-soldiers-reversible/

Les enjeux de la cybersécurité dans un environnement transhumaniste : trois exemples

1. Le cas des IoT (Internet-of-Things)

Les objets connectés sont un des plus vastes marchés pour les années à venir[23]. Nous allons assister à une explosion de ces objets, et ce dans tous les secteurs : de la gamification de l'hygiène de vie par le self-monitoring (Fitbit-like) à la requête Internet en langage naturel dans le salon (« Ok Google, trouve… »), des frigos connectés au suivi des conditions d'acheminement des produits via la chaine d'approvisionnement elle aussi connectée (la Supply Chain 4.0), des Smart Cities comme politique d'urbanisation et de rayonnement international (l'avènement d'Athènes 4.0), en passant par le maintien de l'ordre dans les gouvernements pratiquants férocement la surveillance de masse (la police chinoise aux lunettes connectées profilant en temps réel les individus[24]), les exemples sont innombrables.

En plus d'apporter de nouvelles expériences aux utilisateurs, en déportant *in situ* des rudiments « d'intelligence » numérique en dehors des ordinateurs, les IoT permettent un maillage terrain extrêmement fin et puissant pour une véritable digitalisation du monde réel, physique ; et par-là, forment à leur tour une *general purpose technology* qui va permettre d'accélérer le développement de la prochaine révolution digitale encore dans l'œuf : l'Intelligence Artificielle, qui s'appuie fondamentalement sur la Data massive.

Il est probable que l'IoT sera, dans les décennies à venir, au moins significativement, sinon massivement embarqué dans le corps humain - faisant réellement de l'humain le point de pivot de *l'Internet du Tout*. D'ores et déjà en Union Européenne (Suède), plusieurs milliers de personnes ont implanté des puces « à champ proche » dans leur corps, pour des raisons non pas thérapeutiques, mais de confort, d'expérience d'une réalité augmentée. Ainsi le cas du hub Epicentre, avec ses employés déverrouillant portes et

[23] https://www.uktech.news/news/gartner-forecats-20-increase-in-iot-market-by-2020-20190829
[24] https://www.liberation.fr/planete/2018/02/09/en-chine-des-lunettes-connectees-au-service-de-la-police_1628425

imprimantes grâce à une puce de la taille d'un bon grain de riz implanté dans la main[25] ; mais également de Swedish Rail, compagnie ferroviaire nationale testant ce type de micropuces implantées dans le corps humain comme un moyen de fluidifier les guichets et autres bornes de validation[26]. Outre-Atlantique, c'est Three Square Markets et sa cinquantaine d'employés pucés RFID qui s'identifient à la porte d'entrée, sur leurs ordinateurs, et valident leur commande au distributeur de snacks. Il est prévu d'y ajouter des fonctions comme le GPS[27].

Et c'est là, en dehors de toute discussion philosophique, éthique et sociétale sur l'IoT dans la chair, que la cybersécurité devient un point central. L'IoT, aussi prometteur soit-il pour le business, est en effet tout aussi connu pour les immenses failles de sécurité qu'il comporte actuellement (le pacemaker[28] illustre parfaitement ce problème). Il n'existe pas de consensus suffisamment établi entre les différents acteurs de l'infrastructure IoT sur le point chaud de la sécurité, encore bien trop généralement reléguée au second plan (trop peu de *security by design)*. Ampoules[29], maisons[30] et pompes à essence[31] connectées ne sont que quelques exemples parmi la galaxie d'objets IoT pris pour cibles par les cybercriminels, avec pour objectifs nuisance locale, pénétration plus en avant dans un réseau, rançon ; ou encore l'établissement de botnets, véritables armées de systèmes connectés à Internet utilisés par exemple pour mettre à genoux un serveur informatique, en l'inondant massivement de requêtes superflues.

Ainsi donc, il y a fort à parier que nos PME, ETI et organisations publiques vont bientôt devoir composer avec une nouvelle forme de risque pour leurs systèmes informatiques : celui de l'implantation des IoT dans le corps de leurs employé(e)s… si ce n'est pas elles-mêmes qui encourageront cette pratique. Verra-t-on des entreprises refuser l'accès à certaines zones à des personnes implantées ? D'autres, au contraire, favoriser

[25] https://www.cnbc.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html
[26] https://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html
[27] https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html
[28] http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html
[29] https://www.lefigaro.fr/secteur/high-tech/2016/11/04/32001-20161104ARTFIG00007-pourquoi-les-ampoules-connectees-sont-une-cible-de-choix-pour-les-pirates.php
[30] https://www.forbes.fr/technologie/le-piratage-informatique-qui-menace-les-maisons-connectees/?cn-reloaded=1
[31] https://www.zdnet.com/article/iot-security-now-dark-web-hackers-are-targeting-internet-connected-gas-pumps/

(subventionner) les implants conformes à telle ou telle norme de sécurité « IT organiquement embarqué », encore à définir ? Si actuellement certaines chartes informatiques interdisent le recours au VPN, et que d'autres sont parfaitement laxistes sur l'usage de clouds et autres outils de partage de fichiers professionnels dans l'entreprise, comment sera traitée sur le terrain entrepreneurial quotidien la question de la fusion entre la chair et Internet ? Comment concilier le droit à jouir de son corps comme on l'entend, le devoir de sécurité dans une entreprise, et celui dans la sphère publique ? S'il est vrai qu'une clé USB a suffi à mettre à mal le programme nucléaire Iranien[32], *quid de multiples implants de la taille de grains de riz connectés à la vaste toile et à ses agents malveillants, en culotte courte comme en col blanc ?* Kasperski, lui, travaille déjà sur le sujet[33].

2. Le cas des biotechnologies

De part l'objet d'étude du Transhumanisme (l'humain), et le moyen de développement de cet objet (la technoscience), les biotechnologies occupent naturellement une place fondamentale dans cette pensée. En dehors de tout transhumanisme, la santé est une préoccupation majeure pour les individus, mais également pour les Etats (de la pérennité de la société qui les composent et qui leur permet donc de se maintenir, aux coûts engendrés pour assurer ce maintien). Le domaine des assurances, ou encore du prêt bancaire, sont eux aussi directement liés à la santé des individus ; une part essentielle de leur *business model*.

Quelques stratégies transhumanistes à ce niveau, certes à priori extrêmes, mais permettant de bien illustrer ce courant : l'usage de nanorobots circulants dans notre corps pour assurer un ensemble d'opérations de surveillance et de maintenance localisées[34], le rejet de la mortalité comme principe intrinsèque au vivant[35]. A plus court terme, déjà dans notre paysage, la génomique *prospective* est actuellement une des voies les plus en

[32] https://www.bbc.com/timelines/zc6fbk7
[33] https://usa.kaspersky.com/about/press-releases/2015_connected-phone-connected-house-connected-car-connected-body

[34] https://singularityhub.com/2016/05/16/nanorobots-where-we-are-today-and-why-their-future-has-amazing-potential/
[35] https://www.theguardian.com/technology/2019/feb/22/silicon-valley-immortality-blood-infusion-gene-therapy

vogue. L'établissement plus ou moins complet du génome de tout un chacun (pour quelques centaines à milliers d'euros), pour l'instant essentiellement cantonné pour le grand public dans la recherche généalogique (en dehors des usages thérapeutiques), est depuis peu utilisé pour réaliser du profilage d'embryon humain[36]. Genomic Prediction est une société permettant par exemple de trier des embryons sur base des risques à développer certaines maladies durant la vie future de l'individu[37]. Ce tri ne porte encore que sur des maladies à éviter, mais le marché fortement pressenti, autrement plus lucratif, est celui du *designer baby* – le choix des attributs physiques, biologiques et intellectuels du nouveau-né. Une autre approche propose de cumuler les données génomiques et « socio-étatiques » (impôts, niveau d'éducation, résultats de tests…) de chaque individu, en un vaste projet Big Data, pour développer à terme une sélection optimale des embryons dans le but du renforcement biologique et cognitif de notre espèce, et de son optimisation fonctionnelle[38]. Sur le chemin de ce parfait techno-eugénisme, encore long, citons aussi le cas du partage des données de 23andMe, une des sociétés les plus célèbres proposant d'aider à établir la filiation généalogique de n'importe quelle personne à l'aide d'un peu de salive, qui a récemment fait entrer dans son capital GlaxoSmithKline, géant pharmaceutique, en lui donnant accès aux données récoltées depuis son existence (données anonymisées). Il s'agit là de développer de nouveaux médicaments pour la Big Pharma, mais aussi bien sûr de maximiser les profits de la société 23andMe selon un processus parfaitement classique à l'ère d'Internet : la revente des données personnelles, *parfaitement personnelles* - celles de notre ADN[39]. Sachant de plus que ce type de données nous relient directement à nos enfants et nos aïeux, c'est en réalité une bonne partie de notre arbre qui est ici capitalisé gratuitement à travers quelques gouttes de notre salive. Nous rejoignons directement, et de manière parfaitement intime, la question du respect des données et de la vie privée des individus. Il est aussi aisé d'imaginer à quel point ces données intéresseront assurances et banquiers, dont le business est de pouvoir évaluer à long terme le risque sur les individus qu'ils couvrent[40]. Comme pour

[36] https://www.hfea.gov.uk/treatments/embryo-testing-and-treatments-for-disease/
[37] https://genomicprediction.com/epgt/
[38] https://nickbostrom.com/papers/embryo.pdf
[39] https://time.com/5349896/23andme-glaxo-smith-kline/
[40] http://www.slate.fr/story/158233/assureurs-genes

l'automobile, apparaitra probablement, dans un premier temps, la prime d'intéressement au profilage individuel (une réduction sur la cotisation si l'individu embarque un monitoring dans son véhicule, ou dans son corps). Dans un deuxième temps, renversement de la norme : pénalité pour la personne non monitorée.

Pour toutes organisations publiques et privées, les implications des biotechnologies pour l'humain augmenté sont multiples. Si nous acceptons le profilage des embryons, fort à parier que nous accepterons le profilage de l'employé. La propension à supporter des conditions de travail pénible peut certainement, pour partie, se retrouver dans nos gènes : résistance accrue à telle ou telle substance chimique, force physique, endurance intellectuelle, émotionnelle, sont à priori au moins partiellement définies par nos combinaisons GATTACA à la naissance. (L'hyper-)segmentation de l'humain devrait s'accélérer par cette métrique et ces modèles qui s'affineront chaque jour un peu plus grâce au Big Data et à l'IA. Le suivi fin des conditions de travail, in-situ, par des relevés biométriques (pression sanguine, température corporelle, sudation…) sera lui aussi boosté par les biotechnologies couplées aux IoT embarqués dans le corps ; la métrique de l'humain, sublimée dans le contexte du travail.

Et à nouveau, la cybersécurité est à placer au cœur de l'approche. Que ce soit dans le stockage des données, leur traitement, ou leur préservation (ne parlons plus de leur exploitation commerciale dérivée), les exemples de failles de sécurité sont déjà multiples en ce qui concerne la simple biométrie. Citons le cas de cette entreprise privée de reconnaissance faciale travaillant pour le gouvernement chinois, piratée, qui a laissé s'échapper dans la nature plus d'un million d'identités faciales[41] – le citoyen perdant le contrôle de son avatar facial suite à une politique gouvernementale. Ou celui de cette autre entreprise sud-coréenne en charge d'une vaste base de données biométriques (acquises par plus de 5000 entreprises mondiales, dont des banques et des polices nationales) ayant laissé cette dernière sur la toile parfaitement ouverte, données non chiffrées, accessibles sans difficulté pour le pirate lambda : à nouveau plus d'un million

[41] https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/

d'empreintes digitales, mots de passe, noms, prénoms, adresses[42]. Chine et Corée du Sud, pourtant perçus comme des génies du piratage, eux-mêmes piratés…

Ainsi donc, dans l'IoT comme dans la biométrie, les technologies se déploient *excessivement* plus vite que leur maîtrise en toute sécurité dans notre monde connecté. L'existence de référentiels solides, la nécessité de régulation des pratiques, le choix éclairé des fournisseurs, la réalisation des audits, la maitrise des responsabilités : autant de sujets intemporels dans l'activité humaine, qui peinent encore trop largement à être implémentés malgré les multiples disruptions quotidiennement affichées par nos industries et nos politiques. Imaginons donc maintenant la même approche sur les données du génome humain. La sacro-sainte disruption, appliquée au modèle des assurances et du prêt bancaire, assurément. Il sera bientôt véritablement risqué de laisser trainer ses poils en société…

Un autre point à prendre en compte pour la PME, les ETI et les organisations publiques est celui de l'espionnage industriel. Sony travaille à des lentilles connectées capables de prendre une photo en un clin d'œil ; Google envisage de les rendre éventuellement intra-oculaire, c'est-à-dire, implantées directement dans l'œil (de l'IoT à la biotechnologie transhumaine)[43]. Des projets encore bien loin d'être au point ; mais les brevets sont d'ores et déjà posés. Imaginons alors une entreprise diffusant à son insu des images en temps réel de son intérieur (écran comme bâtiment), ainsi que ses dialogues intra-muros. Espionnage industriel, ou dénonciation des conditions de travail.

En embarquant dans son corps la technologie à des fins de dépassement de soi, de nouvelles fonctionnalités, de fun, c'est toute la question de la cybersécurité que l'humain embarque avec lui. Cela exige un niveau de confiance maximal dans notre appareil technocratique – qui, en réalité, est extrêmement loin de pouvoir assurer le niveau de performance requis en termes de cybersécurité.

[42] https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms
[43] https://www.lesechos.fr/2016/05/google-imagine-des-lentilles-de-contact-implantables-dans-loeil-207027

3. Le cas des sciences cognitives

Continuons notre escapade dans le futur proche, et discutons quelque chose d'encore plus intime que notre génétique : notre esprit. Ici aussi nos avancées ont été fulgurantes grâce à notre technoscience : rétablissement de fonctions motrices par stimulation cérébrale intracrânienne, modélisations numériques poussées via plusieurs méta-projets de recherche sur cette ultime Machine à l'échelle du globe, création d'interfaces neuronales indirectes (casques posés sur le crâne, accessibles autour de 500 $ sur Internet, et mesurant une partie de l'activité cérébrale pour permettre de déplacer par la pensée le pointeur d'une souris à l'écran de l'ordinateur) et directes (implantations d'électrodes dans un cerveau, pour mesurer plus précisément l'activité neuronale et la relayer vers un bras mécanique par exemple). Citons également la DARPA[44], branche Recherche et Développement de l'armée américaine, cherchant à booster significativement les capacités cognitives de ses soldats grâce aux neurotechnologies (apprentissage rapide[45], restauration de la mémoire[46]…), Elon Musk craignant le développement d'une supra-intelligence artificielle à combattre via des implants cérébraux dopant l'esprit humain (et produits par sa société Neuralink[47]), la restauration de certaines fonctions cellulaires au sein de cerveaux de cochons morts depuis plusieurs heures[48], et bien plus troublant que tout le reste : les prémisses de la reconstruction d'images mentales sur base de signaux cérébraux traités par l'Intelligence Artificielle (voir à l'écran ce qu'une personne voit avec ses yeux en mesurant son activité cérébrale[49]).

La démocratisation des neurotechnologies, maintenant utilisées bien plus largement que pour le seul domaine médical[50], auprès des entreprises (via par exemple le neuromarketing, domaine en plein développement, permettant d'étudier finement les corrélations entre un contenu proposé – publicité papier, audio, vidéo, ou bande-

[44] https://www.darpa.mil/
[45] https://www.darpa.mil/program/targeted-neuroplasticity-training
[46] https://www.darpa.mil/program/restoring-active-memory
[47] https://www.lemonde.fr/pixels/article/2019/07/17/elon-musk-et-neuralink-presentent-leur-prototype-d-implants-cerebraux_5490344_4408996.html
[48] https://www.nature.com/articles/d41586-019-01168-9
[49] End-to-end deep image reconstruction from human brain activity, Guihua Shen et all., dx.doi.org/10.1101/272518
[50] http://dx.doi.org/10.1016/j.eij.2015.06.002

annonce d'un film, et le comportement cérébral de l'individu, pour par exemple chercher à mieux solliciter son comportement émotif) comme du grand public (monitoring des états cognitifs : relaxation, excitation, joie, tristesse ; jeu vidéo), pose déjà beaucoup de question sur la sécurité des données et le respect de la vie privée des individus soumis à ces expériences[51]. Pour une expérience donnée, qu'elle soit médicale, professionnelle ou personnelle, c'est en effet tout un ensemble de signaux neuronaux qui sont enregistrés, contenant une grande quantité d'informations dépassant *largement* le spectre des seules études pour lesquelles les expérimentations sont conduites ; par exemple, des marqueurs de troubles cérébraux de la personne. Ainsi l'individu se soumettant à ces essais donne énormément plus que requis, faisant de ces pratiques, une fois bien installées dans notre paysage, le nouveau Pactole[52] digital : imaginons nos BAXT et GAFA, notre employeur et nos employés, nos gouvernements, ayant accès à ce livre potentiellement ouvert sur notre personne. Potentiellement : l'exploitation des données reste encore délicate, et les mesures via des casques posés sur le crâne, plutôt fastidieuses (notamment dû au contact entre les points de mesure et le scalp par exemple). Mais les technologies et les algorithmes vont évoluer, d'autant plus que le marché est extrêmement porteur : une bonne part des professionnels et consommateurs en recherche de fluidité, de techno-fun et d'expérience utilisateur *seamless* seront probablement ravis de pouvoir interagir par leur seul esprit avec leur outil numérique et leur constellation d'IoT. Les implants cérébraux de Musk, pour une expérience de surf augmentée sur Facebook, Amazon, Google devraient permettre une *avalanche* de données cognitives, émotionnelles, individuelles plongées dans un déjà bien vaste Big Data, et précieusement minées par autant d'Intelligences Artificielles parfaitement dressées à cet effet. Neuro-éthique et cybersécurité sont déjà sur la table[53] : des essais de « neurohack / brain spyware » ont récemment fait leur preuve, un peu timides mais effectives, comme par exemple la détermination de l'adresse d'une personne, ou d'un code PIN[54].

[51] Ienca, M., Haselager, P., & Emanuel, E. J. (2018). Brain leaks and consumer neurotechnology. Nature Biotechnology, 36(9), 805–810. doi:10.1038/nbt.4240
[52] https://fr.wikipedia.org/wiki/Pactole
[53] http://www.theneuroethicsblog.com/2018/04/the-seven-principles-for-ethical.html
[54] https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

Nous avons encore un peu de temps devant nous avant que la population accepte d'être cérébralement augmentée par le silicium. Mais à nouveau, il y a fort à parier qu'une frange significative de la population soit séduite par ces technologies. PME, ETI et organisations publiques suivront naturellement : une fois que les first movers auront pris le train, il s'agira pour certains d'une simple question de compétitivité (nous n'avons parlé ici que de captation, de mesure d'ondes cérébrales ; il est évident que la stimulation cérébrale, le dopage cognitif, sera la v2), dans une société sous techno-acide en constante mutation. Et à nouveau se poseront sur ces données les problèmes désormais classiques dans notre monde digital : enregistrement, stockage, exploitation maitrisée ; partage de données entre services, partenaires, exploitation à des fins commerciales ; respect de la vie privée de l'employé, de l'employeur ; data leak, espionnage, malveillance… cependant cette fois-ci, il s'agira non pas d'un nom de famille, d'une adresse postale ou e-mail, mais de nos données cérébrales.

Conclusion : de l'importance de la compréhension des phénomènes, et donc de leur étude

Il est très intéressant de voir comment nos sociétés, c'est-à-dire, chacun d'entre nous, a dans un premier temps accordé une confiance quasi-complète, voire parfaitement aveugle, dans les technologies de communication digitale. Il s'agit probablement là de la prolongation de notre position envers la technoscience : symbole *de facto* du progrès, donc bonne par essence, nécessairement au service de l'humain, et dénuée de tout intéressement. Or, il s'agit là d'une erreur fondamentale de réflexion : science et technologie n'ont rien à voir le bon, le mauvais, le bien ou le mal. Le progrès ne résulte pas de la technoscience, mais *de la manière* dont nous utilisons ce complexe, ce qui est radicalement différent (le feu et l'arme à feu, le nucléaire et la bombe nucléaire, l'IA et la surveillance de masse). Une forme de naïveté au moins excessive, sinon infantile, accentuée avec le digital par la sensation d'être seul, car simplement devant une machine, sans autre humain matérialisé dans le champ de vision.

Cas d'école de cette naïveté, nos usages d'Internet. Nous avons ici parfaitement rompu avec nos principes élémentaires de précaution, pourtant appliqués avec rigueur dans le monde physique : le maintien de notre vie privée, de notre intimité, de notre souveraineté dans notre sphère personnelle. Au point qu'en matière de cybersécurité individuelle, nombre de nos concitoyens partent encore du principe « qu'ils n'ont rien à cacher, donc pourquoi se protéger ? ». Il s'agit là d'un parfait renversement conceptuel. Il serait tout à fait inacceptable, dans le monde physique, tangible, pour n'importe qui, d'être quotidiennement suivi par des individus, entreprises, états, chez soi comme à l'extérieur ; dans nos lectures, nos achats, l'expression de nos idées ; dans nos goûts, nos envies et nos fantasmes. Et ce, même si nous n'avons rien à cacher.

De manière certes un peu caricaturale, mais non excessive, la quasi-totalité des données digitales de la quasi-totalité des citoyens, professionnels, institutions, sont concentrées entre une poignée d'acteurs majeurs situés en deux endroits dans le monde : les USA, et la Chine. En pratique, une grande partie de nos entreprises et institutions stockent nombre de leurs données sur les mêmes serveurs, de la même manière, et avec les

mêmes outils, que les individus technologiquement ignorants ; les gouvernements eux-mêmes ne font pas exception. Ces mêmes endroits du globe, qui nous fournissent également les outils soft et hardware pour collecter et gérer ces données au *day-to-day*, en une boucle de maîtrise du cyberespace parfaitement bouclée.

Progressivement, par l'expérience (notamment celle des problèmes associés à cette oligarchie digitale chaque jour plus puissante), nos pratiques changent, à mesure que nous prenons le pouls correct de ce qui se passe derrière nos écrans ; nous rétablissons une compréhension plus réaliste de la machine humaine agissant derrière la machine physique ; et ainsi l'Europe et le RGPD, prise de conscience et action essentielle, ou encore, malheureusement bien trop récemment, le choix d'une solution de cloud européen pour certaines institutions nationales (Nextcloud). Il était plus que grand temps !

Il est maintenant indispensable de singulièrement renforcer la compréhension digitale du politique, de l'entreprise et du peuple pour regagner, à défaut de sa souveraineté digitale (objectif malheureusement compromis), au moins, suffisamment de bonnes pratiques pour un usage du digital non plus béat ou impuissant, mais conscientisé et raisonné[55].

La technocratie, mutant progressivement en techno-impérialisme imposé à marche forcée (et avalé avec grand appétit par la société humaine dans son ensemble) par les GAFA, les BAXT, et une poignée d'autres acteurs concentrés dans les Eldorado contemporains que sont la Silicon Valley ou Shenzhen, par exemple, sont les parfaits promoteurs d'une techno-utopie drivée par le business qui nous amène, plus vraiment doucement, mais bien sûrement, vers une société Transhumaniste.

La bonne vieille Europe, coincée entre ces deux puissances, peut pour certains apparaitre comme un outsider déjà mort ; mais il n'en est rien, bien au contraire. Certes parfois technologiquement (largement) dépassée, ses positions sur l'Intelligence Artificielle et le Transhumanisme sont néanmoins parfaitement intéressantes et pertinentes, et à coup sûr

[55] Plus généralement, la société doit augmenter sa compréhension technoscientifique dans son ensemble, et cesser d'être aveuglement séduite par les sirènes prônant le bien-fondé *intrinsèque* de ces outils. A nouveau, science et technologie sont par-delà bien et mal.

les nécessités du monde de demain : l'Éthique et l'Humanité, deux valeurs *largement bankables* du siècle en cours.

Et c'est exactement selon ces deux axes que doit s'étudier la pensée Transhumaniste, car elle entraîne la redéfinition même du concept d'Etre Humain, de son Identité, et par extension, de sa Sécurité. La cybersécurité occupera donc naturellement une position majeure dans le débat, en posant les questions suivantes :

- Quelles informations composeront mon identité comme Humain Augmenté ?
- Comment seront-elles gérées dans un monde en ligne, connecté ; dans un Big Data lui aussi augmenté par l'ADN, les profils cérébraux… mis à disposition par chacun, et largement exploité en dehors des pouvoirs publics ?
- Identité et Humanité seront-elles réduites à la seule somme de ces informations ? Serais-je encore réellement Humain dans ce Big Data ?
- Enfin, quelles informations devront être protégées ? Par qui, quoi et comment ? Jusqu'à quel degré, et à quel prix ?

In fine, il s'agira de définir les conditions de la Liberté X.0 dans un contexte Transhumain… tâche ardue s'il en est : la technoscience redéfinissant chaque jour les attributs accessibles de l'individu, et donc la notion même d'individu, comment définir Sécurité et Liberté quand on ne sait pas encore ce qui doit être protégé/préservé ?

Pour mener cette réflexion, plusieurs pistes existent :

- Organiser l'Humanité pour traiter ces sujets à un rythme *bien plus rapide*, permettant de mieux suivre l'évolution technologique : de la réactivité des pouvoirs publics à l'action de chacun sur le terrain ;
- Développer la nécessité d'une volonté partagée à l'échelle des grandes puissances, du globe : de l'importance des politiques, et donc des citoyens ;
- Établir une gouvernance planétaire de la cybersécurité : de la nécessité de l'émergence d'une conscience collective sur le sujet.

En augmentant massivement l'éducation digitale, en plaçant fondamentalement la *ressource Humaine au cœur de la Valeur de toute chose*, et en renforçant son large tissu de PME, ETI et organismes publics par le déploiement de solutions continentales (hébergement des données, culture massive de la cybersécurité, culture du paradigme open-source ; fiscalité digitale transcontinentale, appareil juridique proactif sur les enjeux de demain, c'est-à-dire aujourd'hui posés ; régulation), l'Europe peut tout à fait incarner, non plus l'âge avancé de la fanaison, mais celui de la sagesse qui vient de l'expérience du temps. Et cette sagesse nous sera à coup sûr indispensable dans les décennies à venir, comme ligne moyenne entre les extrêmes de l'utopie ultra-libérale, par essence incapable à développer une société planétaire équilibrée, et la dystopie totalitaire, elle aussi vouée à l'échec à l'échelle de notre espèce.

La bonne nouvelle, *l'excellente* nouvelle : la Marche du Monde, qui de tout temps peut sembler boiteuse, n'est pas une Loi extérieure qui nous tombe dessus, mais le résultat de chacun des étages qui le composent. L'ensemble du maillage socio-économique, du terrain à la gouvernance, et plus généralement le citoyen, le professionnel, le politique – le consommateur ! sont assurément tous acteurs. A chacun d'étudier et d'incarner son rôle avec conscience, éthique et responsabilité.

---------- Fin de document ----------