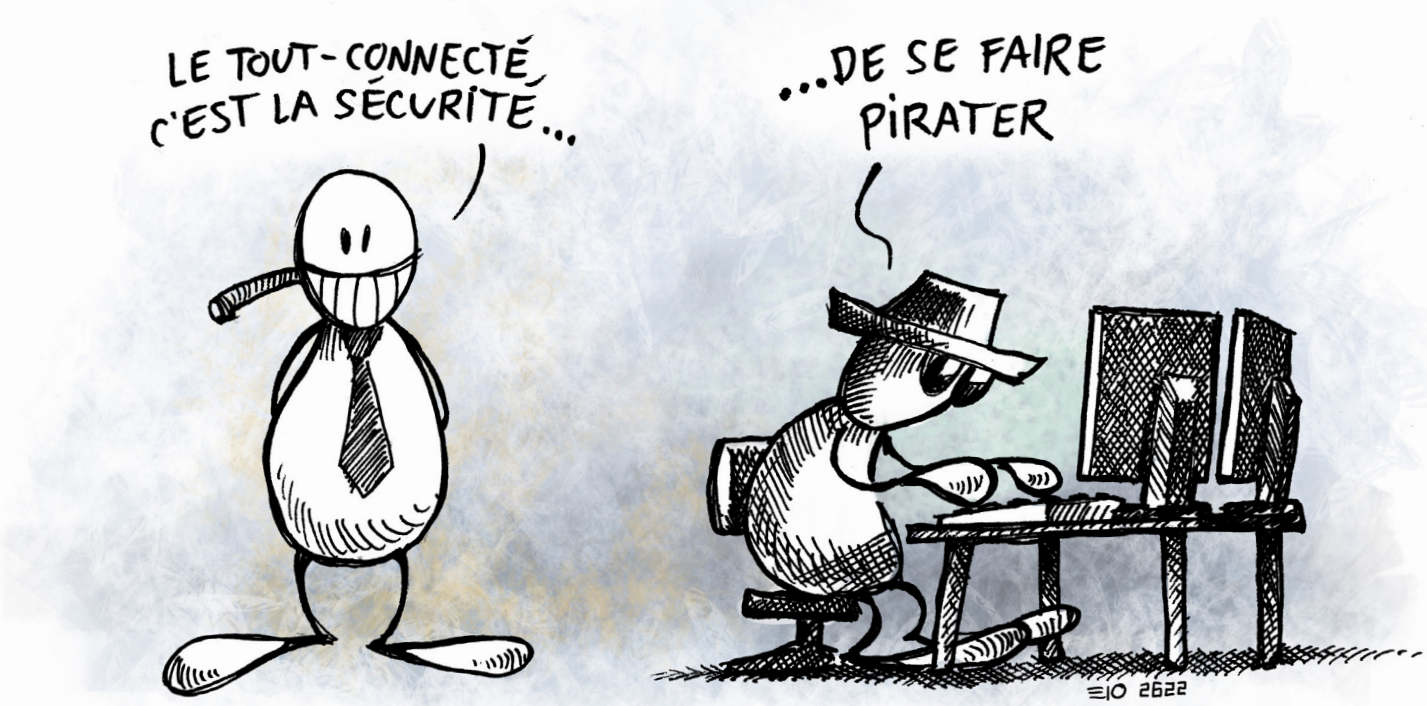
> *« Allons droit au but: l'État n'est, aujourd'hui, pas à la hauteur face à la vague massive de cyberattaques qui nous frappe. Que ce soit au niveau fédéral, cantonal ou communal, les autorités n'ont visiblement pas encore pris la mesure des enjeux liés à ces piratages. Or ce sont nos données personnelles qui sont en jeu, celles que nous confions à des administrations, des banques ou des assurances. »*
> (*Le Temps*, 2022)

Les promesses de la 5G et les enjeux sécuritaires



SÉCURITÉ DES DONNÉES

L'on ne peut faire l'économie d'une réflexion liant le déploiement de la technologie 5G et la question des cyber-attaques et du terrorisme informatique, menace bien silencieuse et souvent indétectable.

En effet, avec la 5G s'accompagne la déferlante d'objets connectés en tout genre. Eux aussi sont sujets aux vols de données et toute forme de prise de contrôle depuis l'extérieur. Notre dépendance accrue aux applications à la mode, la virtualisation de nos données et les quantités de données formées – data produites par les objets connectés (IoT, ou IdO en français) présents et à venir, mettent clairement en danger notre indépendance et notre sécurité. Avec la 5G, cette dernière sera décuplée.

Mais la cyber-sécurité, c'est quoi?

La cyber-sécurité est un terme général qui englobe la protection des ordinateurs, des serveurs, des téléphones portables, de systèmes électroniques, des réseaux et des données contre des attaques malfaisantes (Kaspersky).[1]

La menace sur la cyber-sécurité s'accélère chaque année à l'échelle globale avec l'augmentation en complexité et en connectivité de l'infrastructure de réseau, ce qui compromet sérieusement la sécurité du public, de la santé, de l'économie et de la Suisse (National Institute Of Standards And Technology).[2]

Aux USA, une entreprise spécialisée en cyber-sécurité a reporté une augmentation annuelle de 112% du nombre de fichiers exposés à la suite de cyber attaques en 2019, représentant 7.9 milliards de documents en octobre 2019 seulement (Risked Based Security).[3]

Le rapport du WEF sur les risques globaux de 2018 place le risque d'attaques informatiques en 3e position, devancé seulement par les catastrophes naturelles et les changements climatiques extrêmes (World Economic Forum) [4].

Le risque augmente exponentiellement avec la croissance des objets connectés car chaque objet est aussi une faille potentielle à être exploitée (World Economic Forum).[5]

L'augmentation des objets connectés, ou IoT, augmente ainsi le risque de cyber-attaques.

Pour comprendre l'ampleur du danger en Suisse, une rétrospective est nécessaire.

1 https://www.letemps.ch/opinions/face-aux-cyberattaques-letat-nest-hauteur
2 https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
3 https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
4 https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/
5 http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/

PANORAMA DES CYBER-ATTAQUES

«C'était prévisible. Et c'est déjà devenu réalité. Il n'est désormais plus possible de tenir à jour la liste des entreprises et administrations suisses victimes de cyberattaques. Les agressions sont incessantes. Depuis l'annonce, mardi soir, du piratage de l'importateur automobile Emil Frey, de nouveaux incidents se seront certainement produits au moment où vous lisez ces lignes. Et de plus en plus, une question se pose: que font et que devraient faire les autorités pour lutter contre ce fléau?» (*Le Temps*, 2022)

La Suisse a connu en 2021 une recrudescence de cyber-attaques. Les tentatives d'intrusion enregistrées par les entreprises helvétiques ont ainsi bondi de 65% par rapport à 2020, à en croire le spécialiste californien en sécurité informatique Check Point Software, qui ne fournit pas de chiffre absolu (TDG, 2022).[1]

Principales cibles, les entreprises industrielles. Check Point Software a dénombré 738 attaques hebdomadaires en 2022, soit une hausse de 20%. A noter que les statistiques de Check Point Software reposent sur les données des clients et ne représentent ainsi qu'une partie des cyberattaques survenues en Suisse.

En bref:

- Le secteur de la santé: +107%

305 attaques hebdomadaires par entreprise en moyenne

- La place financière et bancaire: +98%

271 attaques hebdomadaires par entreprise en moyenne

- Les agences gouvernementales et militaires: +8,6%

388 attaques hebdomadaires par entreprise en moyenne

- Secteur de la communication: +65%

107 attaques hebdomadaires par entreprise en moyenne

- Compagnies d'assurances et cabinets d'avocats: +1%

191 attaques par entreprises en moyenne [2]

Les attaques ayant abouti pour la seule 2021 ont touché les entités suivantes:

Le constructeur de véhicules agricoles et de voirie Bucher
L'organisateur de foires MCH
Le comparateur en ligne Comparis
La compagnie de navigation sur le Léman CGN
La Banque cantonale de Neuchâtel
Le groupe de cliniques privées Pallas
Le fournisseur de l'industrie pharmaceutique Siegfried
La commune de Rolle

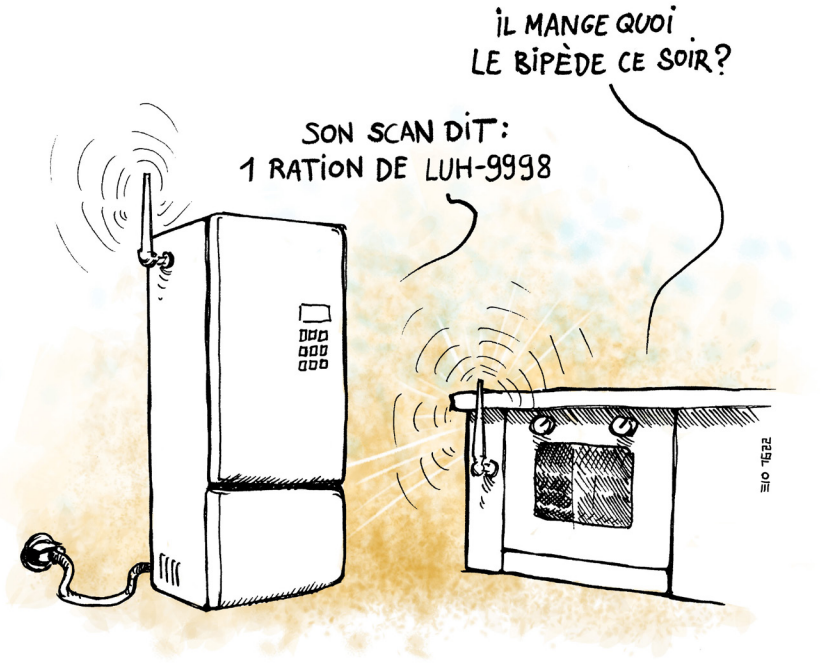
En 2022, les attaques effectives ont d'ores et déjà touché les acteurs suivants:

Le CICR [3] [4]
Le groupe automobile Emil Frey [5]
Le groupe pharmaceutique Zur Rose [6]
La commune d'Yverdon-les-Bains [7]
Le groupe industriel lucernois Chemie + Papier Holding (CPH) [8]

A titre de comparaison, l'Europe a connu la hausse la plus importante avec plus de 600 cyberattaques hebdomadaires (+68%), suivie des États-Unis (500 soit +61%), suivie de l'Amérique latine (+38%).

1 https://www.tdg.ch/le-nombre-de-cyberattaques-a-bondi-de-65-en-suisse-en-2021-283750587480Ibid
2 Ibid.
3 https://www.24heures.ch/les-donnees-de-plus-de-500000-personnes-piratees-au-cicr-566330900259
4 https://www.letemps.ch/economie/contre-cicr-cyberattaque-etait-puissante-ciblee
5 https://www.ictjournal.ch/news/2022-02-03/cyberattaque-contre-emil-frey-des-donnees-publiees-sur-le-darkweb-update
6 https://www.swissinfo.ch/fre/zur-rose-potentiellement-victime-de-cyberpirates/47275872
7 https://www.rts.ch/info/regions/vaud/12785714-la-ville-dyverdonlesbains-a-ete-victime-dune-minicyberattaque.html
8 https://agefi.com/actualites/entreprises/cph-victime-dune-cyberattaque

AVEC QUELLES CONSÉQUENCES?



Santé

Vols et publications de données privées liées à la santé dans le canton de Neuchâtel, et demande d'une rançon.[1] [2] Qui paiera la note? Quels dangers pour les citoyen.nes à voir leur dossier de santé publié sur le darknet à l'échelle nationale?

Dépression, cancer, IVG, etc., toutes ces données se sont momentanément retrouvées à la vue de tous sur le net. Et pourtant: les compagnies d'assurance poussent à utiliser leurs nouvelles applications via les smartphone et les smartwatch, notamment grâce à l'arrivée de la 5G, augmentant ainsi la vulnérabilité de nos données sensibles.

Finance

Selon la FINMA, on observe une hausse de la cybercriminalité, de l'espionnage et du cyber-espionnage, alors même que les technologies de l'information nous rendent toujours plus connectés et interdépendants. Ceci se traduit par une vulnérabilité aigüe de nos institutions financières, avec pour conséquences des répercussions sur le bon fonctionnement de la place financière nationale dans son ensemble. Les dommages en termes de réputation seraient considérables et la confiance dans la place financière s'en trouverait mise à mal (FINMA).[3]

Et pourtant, les banques suisses respectent insuffisamment l'obligation d'informer sur les cyber-incidents qui les ciblent, constate un audit du Contrôle fédéral des finances (CDF).[4] La situation est accentuée par le fait que les banques refusent à la FINMA un accès direct à MELANI (Centre national pour la cybersécurité NCSC).

«De la protection des données à la dépendance des technologies étrangères, la Suisse affiche des lacunes béantes, en plus de celles qui sont apparues dans le domaine de la santé. Le mal est profond (…)»

(*Le Temps*, 29 mars 2021)

Après la crise de 2008, et à la lumière du conflit actuel à l'est, nos données financières ainsi que notre indépendance sont mises à mal. Cependant, la multiplication d'applications liées notamment au e-Banking, au trading, à la crypto-monnaie, au paiement sans contact etc., fragilisent grandement notre capacité à sécuriser nos données. Ces dernières utiliseront entre autre le réseau utilisé par les smartphones, notamment des antennes de facture chinoise controversées (Huawei, par exemple).[5]

Gouvernement et armée

Le Seco (Secrétariat d'état à l'économie) avoue le piratage de 130' 000 noms d'entreprise qui ont demandé un crédit Covid sur la plateforme EasyGov en 2020. Des lacunes apparaissent clairement au sein de la Confédération.

Communication, dégât d'image, et données sensibles de l'État sont prises en otage par des pirates étrangers.[6] Quid de nos données liées à notre sécurité, au terrorisme ou à la sphère privée? La virtualisation et la dépendance numérique de divers secteurs du gouvernement, de l'administration publique et de l'armée mettent en danger nos institutions et nos données privées. La déferlante des IoT promise par un certain secteur de l'économie augmentera massivement la vulnérabilité de l'État et de ses membres.

Assurances et cabinets d'avocats

«Zurich Insurance semble avoir été victime d'une cyberattaque. Différents domaines informatiques de l'assureur suisse et de ses entreprises partenaires ont été touchés. Mais après avoir réparé la brèche dans sa sécurité, la compagnie n'en a informé ni sa clientèle, ni les médias. "Déçu" par le manque de transparence du géant, le hacker a donc décidé de publier sur le darknet les données volées, révèlent lundi nos confrères de *20 Minuten*.»[7] (*Le Matin*, 2021)

Chantage, rançon, les citoyen.nes sont pris au piège par le stockage de leurs données sur le Net. Que se passera-t-il quand, de surcroit, la multitude d'applications et d'objets connectés seront eux aussi détenteurs de telles données?

1 https://www.letemps.ch/economie/donnees-medicales-milliers-neuchatelois-ont-mises-ligne
2 https://www.rtn.ch/rtn/Actualite/Region/20220330-Les-donnees-medicales-de-milliers-de-Neuchatelois-sont-en-ligne.html
3 https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/cyberrisiken/
4 https://www.ictjournal.ch/news/2021-02-23/les-banques-suisses-dissimulent-trop-souvent-les-cyberattaques-qui-les-ciblent
5 https://www.euractiv.fr/section/economie/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/
6 https://www.lenouvelliste.ch/suisse/cyberattaque-le-secretariat-detat-a-leconomie-pris-a-son-tour-au-piege-1121460
7 https://www.lematin.ch/story/les-donnees-des-clients-de-la-zurich-insurance-finissent-sur-le-darknet-526688604451

INCIDENTS ET SCANDALES HISTORIQUES

En 2021, la Suisse décide de bâtir son cloud national avec Amazon, Alibaba, Oracle, IBM et Microsoft. Cela veut dire que toutes les données de la Confédération seront stockées sur les serveurs de ces multinationales américaines et chinoises. Mais pourquoi pas suisses? [1]

En 2011, WikiLeaks documente la vente de technologies d'espionnage à des États autoritaires. Ces armes servent à la surveillance des populations. Parmi les entreprises qui les conçoivent, certaines sont suisses comme Dreamlab. La société bernoise a vendu ses technologies à Oman. Grâce à elles, le Sultanat a pu mater son Printemps Arabe.[2]

En 2015, les ordinateurs de l'entreprise britannique Cambridge Analytica ont utilisé les données Facebook d'au moins 87 millions d'utilisateurs afin d'influencer le vote de citoyens. Grâce à nos données, Cambridge Analytica est capable de brosser un portrait très précis des électeurs. Et de cibler le message politique.[3] [4]

En 2013, la Suisse confie la fabrication du système d'écoutes de ses polices et tribunaux à l'entreprise israélienne Verint, fondée par un ancien agent du Mossad. A Berne, ce choix inquiète. La Suisse est-elle sous écoute d'Israël? [5]

En 1995, les services de renseignement américains (un organe d'espionnage crée par la CIA en partenariat avec les services secrets allemands) et l'entreprise suisse Crypto AG concluent un accord confidentiel qui permettra l'espionnage des communications de 130 pays. Durant des décennies, un pan de l'industrie helvétique sera impliqué dans ces activités, malgré la "neutralité" du pays et avec la bénédiction du Conseil fédéral.[6] [7] L'affaire a mis des décennies à être rendue public, de quoi sérieusement ternir l'image de la Suisse.

Avec les 200 millions de produits connectés que pourraient compter la Suisse d'ici quelques années, combien espionneront votre activité?

1 https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html
2 Ibid.
3 Ibid.
4 https://securityaffairs.co/wordpress/72058/social-networks/cambridge-analytica-closes.html
5 https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html
6 Ibid.
7 «Opération Rubicon» https://www.bilan.ch/economie/operation-rubicon-la-suisse-dans-le-mal

ACTUALITÉ: COÛT DU CRIME NUMÉRIQUE

Le coût du crime numérique augmente lui aussi. Une étude sur 254 entreprises dans 7 pays estime à 27,4% le coût annuel par entreprise 11.7 million GBP (14,5 millions CHF) le coût annuel par entreprise en 2017, ce qui représente une augmentation annuelle de 27.4% (World Economic Forum).[1]

Il est estimé à 8 trillions USD pour la période 2018-2022.

Les attaques de rançon comptabilisaient 64% des attaques en 2017 (Proofpoint Quarterly Threat Report).[2]

1 http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#view/fn-44
2 https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf

IOT: RISQUES?

Avec l'IoT (*Internet of Things* ou Internet des Objets) la nature des attaques va changer. Aujourd'hui déjà, **les risques connus et moins connus, sont réels:**

- Vol des données (numéros bancaire, identifiants, etc.)
- Manipulation des adolescents
- Espionnage
- Désactivation de voitures à distances
- Manipulation de machines de votes
- Meurtre à distance par piratage de pacemakers

(Proofpoint Quarterly Threat Report).[1]

Ce nouveau modèle de société nous est imposé par des acteurs plus fort, c'est-à-dire ceux qui savent capter et exploiter les données (GAFAM).

Avec la possibilité de bénéficier de certaines de ses applications, ce nouveau modèle sociétal apporte avec lui de sérieuses menaces et défis pour la liberté individuelle.

Ceux qui contrôlent l'IA possèdent de nouveaux pouvoirs:

- Le pouvoir prédictif qui suggère et propose (permettant d'influencer la perception des masses)
- Le pouvoir d'énoncer une vérité déterminée et de l'imposer (en excluant toute autre réalité qui n'est pas programmée)
- Le pouvoir injonctif (en orientant les actions et les comportements des individus)
- Le pouvoir coercitif contraint (en pénalisant les comportements déviant par rapport à une normalité imposée)

(Solange Ghernaouti, *Swiss Cybersecurity Advisory & Research Group*).[2]

1 https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf
2 https://blogs.letemps.ch/solange-ghernaouti/

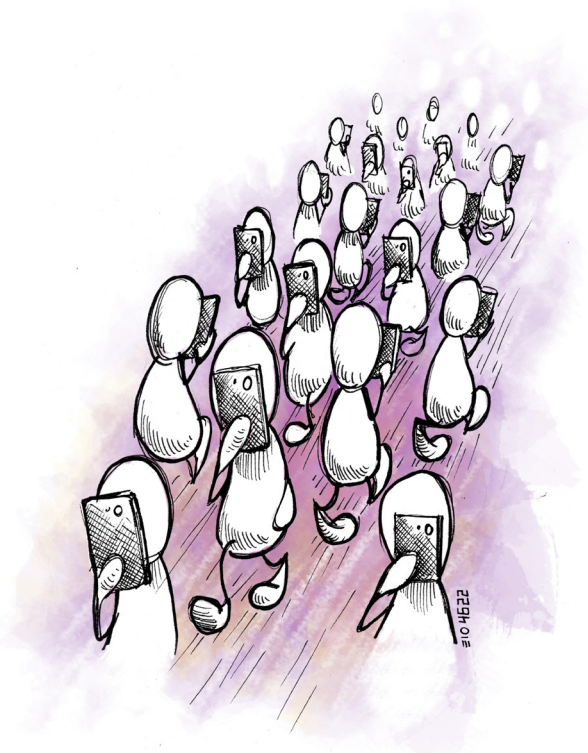
QUELLES DIFFÉRENCES POUR LA SÉCURITÉ NUMÉRIQUE ENTRE UN RÉSEAU 4G ET 5G?

Ceci n'est pas anodin. **Le saut vers la 5G aura pour résultat une commercialisation de nouveaux produits connectés.** Il s'accompagnera d'une augmentation des senseurs en tout genre en zones public (censeur de mouvement, bruit) et des caméras de surveillances. Tous les objets seront connectés, notamment au cloud, permettant ainsi la communication et l'échange de données ultra-rapide entre machines (M2M).

Risques généraux au déploiement des IoT et des outils permettant leur utilisation

Au sus des éléments mentionnés plus haut, voici une liste non-exhaustive des dangers potentiels liés au déploiement des IoT et des technologies permettant leur utilisation:

- **Le phishing:** un genre de "*social engineering*" exploité à des fins de vols de données telles qu'informations bancaires où identifiants dans un but d'usurpation d'identité, d'achats non-autorisés ou vols de fonds. Il existe différents types de phishing (spearphishing, whalephishing…) (Phoenixnap).[1]
- **Les virus:** des codes créés pour compromettre discrètement un système informatique à des fins d'espionnage, de rançons, de décisions, et de contrôles (Phoenixnap) [2]. Les virus peuvent affecter tout un réseau d'objets connectés, sans être détecté, jusqu'à finalement les rendre inutilisables
- **Injection de SQL:** un code malin particulièrement à risque pour les entreprises car il peut manipuler et détruire les bases de données en arrière-plan qu'il vise.



- **DoS:** une attaque visant la désactivation d'un réseau ou service le rendant inutilisable pour ces utilisateurs. Typiquement dirigée à un serveur web de grande utilité (gouvernements, multinationales, banques…), ces attaques sont souvent utilisées à des fins de distraction pour d'autres formes d'attaques (Phoenixnap).[3]
- **L'espionnage:** une redirection du flux d'information entre objets non-sécurisés, par exemple les smartphones, les ordinateurs et autres. Ces attaques sont imperceptibles car elles n'affectent pas l'utilisation de l'objet. Tout objet connecté en réseau en est vulnérable.
- **IA attaque:** ce sont de loin les plus dangereuses car elles peuvent transformer l'utilité d'objets à des buts destructeurs (attaques par drones, accidents de voitures, décharges de pacemakers, pannes électriques...)

Comment la technologie des IoT peut-elle être plus risquée? Il y a trois causes de l'augmentation du risque (Bruce Schneier, membre du conseil de l'*EFF, and the Chief of Security Architecture at Inrupt, Inc.*): [4]

1. Le contrôle de systèmes par logiciels informatiques
2. La connectivité entre systèmes
3. L'autonomie des systèmes

Soit:

1 **Contrôle par programmes informatiques:** l'IoT est l'intégration de micro-ordinateurs dans tous les objets du quotidien. Le contrôle à distance rendra les appareils ménagers et autres vulnérables aux attaques que connaissent aujourd'hui les ordinateurs.

2 **Inter-connectivité:** Lorsque les systèmes sont connectés entre eux, la vulnérabilité de l'un se traduit par la défaillance de l'autre. Déjà des comptes Gmail ont été compromis par des réfrigérateurs intelligents Samsung (Networkworld) [5], des réseaux informatiques hospitaliers compromis par des failles dans des appareils médicaux (Meddeviceonline) [6], et la multinationale Target piratée par une vulnérabilité de son système CVC qui a exposé l'information de 40 millions de cartes bancaires (Krebsonsecurity) [7]. Les failles d'un système se répercutent sur d'autres, et il en résulte une vulnérabilité imprévisible dont personne n'a la responsabilité de dédommager.

3 **L'autonomie:** Nos systèmes informatiques sont de plus en plus autonomes. Ils achètent et vendent des actions, allument et éteignent la chaudière, régulent le flux d'électricité dans le réseau et, dans le cas des voitures sans conducteur, pilotent automatiquement des véhicules de plusieurs tonnes vers leur destination. Du point de vue de la sécurité, cela signifie que les effets des attaques peuvent se faire sentir immédiatement. Plus nous retirons les humains de l'équation, plus les attaques rapides peuvent faire leurs dégâts et plus nous perdons en contrôle préventif.

1 https://phoenixnap.com/blog/cyber-security-attack-types
2 Ibid.
3 Ibid.
4 https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html
5 http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html
6 https://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001
7 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

GESTION DES DONNÉES PERSONNELLES

Qui gère nos données personnelles? En tant qu'utilisateur, on nous incite à faire confiance aux sociétés qui gèrent nos données et à se détacher de la responsabilité de leur stockage, notamment avec le cloud.

Mais le cloud, ce sont des infrastructures bien physiques, des centres de données, qui sont généralement américains ou chinois (Solange Ghernaouti, *Swiss Cybersecurity Advisory & Research Group*).[1]

Nous sommes donc poussés, sans notre consentement informé, à déléguer le droit de stockage, de gestion et de propriété de nos données les plus intimes à des entreprises étrangères, déjà éclaboussées par divers scandales liés à l'utilisation de nos données.

Nous acceptons donc docilement une perte de contrôle totale sur notre identité la plus précieuse, c'est-à-dire nos habitudes, notre comportement, nos pensées, notre évolution personnelle.

Avec le développement de la 5G, cette tendance s'accélérera significativement car plus on utilise de numérique, plus on produit de données, plus on a besoin de les stocker, plus on est contraint de faire confiance aux algorithmes qui automatisent le processus.

[1] *Allez Savoir* n°75, «Un monde virtuel, une pollution bien réelle», Rencontre avec Solange Ghernaouti, Professeure et spécialiste en cybersécurité à l'UNIL», sept. 2020 in https://com-www.unil.ch/allezsavoir/AS075.pdf

ALGORITHMES ET IA

En sachant que les développements d'algorithmes par IA sont mis en œuvre sous secret de fabrication de leurs propriétaires, comment peuvent-ils être vérifiés par des acteurs externes et indépendants afin de vérifier leur qualité et leur sécurité ? Sans pouvoir être en mesure de comprendre les logiques internes des systèmes IA, sans pouvoir vérifier et expliquer leur mode de fonctionnement, comment faire confiance aux décisions prises par de tels systèmes?

Avant de plonger vers un système dirigé par l'IA, comme nous sommes en train de le faire à l'échelle planétaire, il faudrait qu'il existe aux niveau national et international des mécanismes qui permettent de refuser l'usage de dispositifs d'IA portant atteinte à des valeurs convenues (UNESCO), de les dénoncer et de pouvoir poursuivre en justice les entités responsables.

En 2017, 90% de nos transactions financières étaient réalisées par des algorithmes (OCDE).[1] Or, selon Dominique Cardon, sociologue spécialisé dans les technologies du numérique, **l'intention de l'architecte lors du développement de l'algorithme est centrale afin de comprendre les impacts que pourraient avoir ces outils sur les utilisateurs.** Le concepteur doit faire le choix, selon sa perception de la réalité et selon ses objectifs, des composantes à intégrer dans son modèle, mais aussi de la manière dont l'algorithme va prioriser et hiérarchiser l'information ou prendre une décision (Cardon, 2018).[2]

Ces algorithmes résultent donc d'un choix stratégique qui cherche à répondre à certains objectifs, ils ne sont donc pas neutres.

[1] OCDE (2019), *Artificial Intelligence in Society*, OECD Publishing https://www.oecd-ilibrary.org/docserver/aa565467-fr.pdf

[2] Cardon, Dominique. 2018. «Le pouvoir des algorithmes», Pouvoirs: Revue française d'études constitutionnelles et politiques no. 164: 63-73

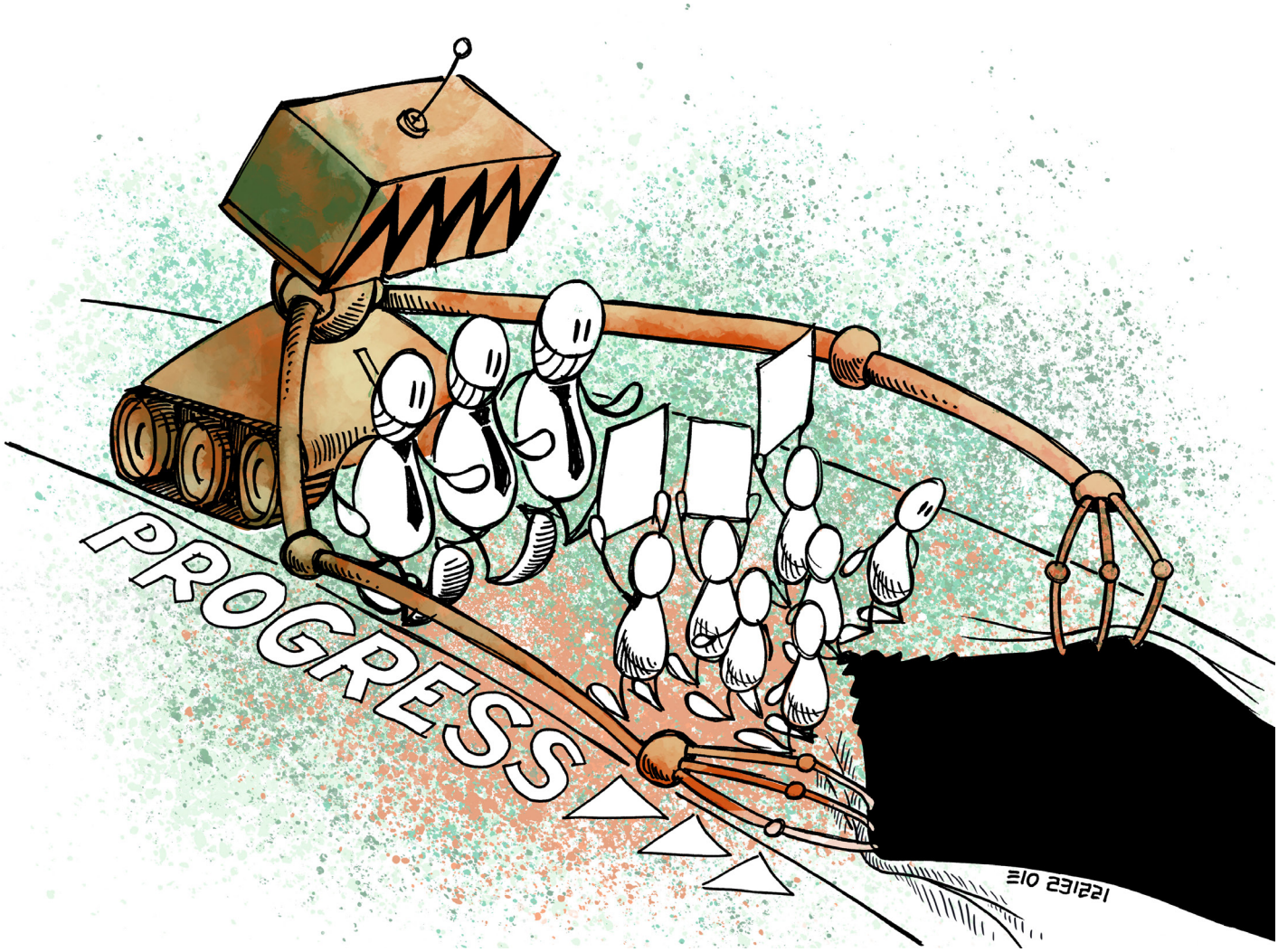
NUMÉRISATION, POUVOIR ET LÉGISLATION

Qui dit nouveaux pouvoirs, appelle à de nouveaux droits. Quels sont nos droits actuels? Ne devrions-nous pas prioriser la législation de nouveaux droits sur le numérique avant de plonger vers cette société imposée par des entreprises privées qui échappent au contrôle indépendant?

Voici une liste de nouveaux droits qui devraient être assurés avant d'imposer l'IoT à la société:

- Le droit des individus à avoir des opinions et des comportements différents de ceux énoncés par une IA
- La tolérance des dispositifs d'IA envers ceux et celles dont les particularités sont à la marge de ce qui est défini comme normal par les concepteurs d'IA
- Le droit de la liberté de l'humain de pouvoir se soustraire au pouvoir d'influence, d'orientation et de coercition de IA.
- Le droit à la déconnexion
- Le droit d'être oublié (effacement définitif des données)
- Le droit de ne pas vivre sous surveillance informatisée
- Le droit de la personne à savoir si elle interagit avec une intelligence artificielle
- Le droit à la transparence des prises de décisions effectuées par une intelligence artificielle
- Le droit de pouvoir recourir contre une décision prise par une intelligence artificielle
- Le droit à la sécurité de ses données
- Le droit à la privacité de ses données

En l'absence de ces droits, d'un cloud au moins européen à défaut d'être national, au vu des dangers pour la démocratie, le fonctionnement de l'État, nos données personnelles, notre vie privée, au vu des dangers réels liés à l'IA, à la définition des algorithmes, aux risques de cyber-attaques et aux rançons, nous estimons que le déploiement de la technologie 5G viendra renforcer les fêlures déjà observées aujourd'hui, et mettra sérieusement à mal notre indépendance et notre liberté en tant qu'État démocratique.



Bibliographie

https://www.letemps.ch/opinions/face-aux-cyberattaques-letat-nest-hauteur

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/

https://www.tdg.ch/le-nombre-de-cyberattaques-a-bondi-de-65-en-suisse-en-2021-283750587480

https://www.24heures.ch/les-donnees-de-plus-de-500000-personnes-piratees-au-cicr-566330900259

https://www.ictjournal.ch/news/2022-02-03/cyberattaque-contre-emil-frey-des-donnees-publiees-sur-le-darkweb-update

https://www.swissinfo.ch/fre/zur-rose-potentiellement-victime-de-cyberpirates/47275872

https://www.rts.ch/info/regions/vaud/12785714-la-ville-dyverdonlesbains-a-ete-victime-dune-minicyberattaque.html

https://agefi.com/actualites/entreprises/cph-victime-dune-cyberattaque

https://www.letemps.ch/economie/devraient-faire-autorites-suisses-face-fleau-cyberattaques

https://www.letemps.ch/economie/donnees-medicales-milliers-neuchatelois-ont-mises-ligne

https://www.rtn.ch/rtn/Actualite/Region/20220330-Les-donnees-medicales-de-milliers-de-Neuchatelois-sont-en-ligne.html

Bibliographie

https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/cyberrisiken/

https://www.ictjournal.ch/news/2021-02-23/les-banques-suisses-dissimulent-trop-souvent-les-cyberattaques-qui-les-ciblent

https://www.euractiv.fr/section/economie/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/

https://www.lenouvelliste.ch/suisse/cyberattaque-le-secretariat-detat-a-leconomie-pris-a-son-tour-au-piege-1121460

https://www.lematin.ch/story/les-donnees-des-clients-de-la-zurich-insurance-finissent-sur-le-darknet-526688604451

https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html

https://securityaffairs.co/wordpress/72058/social-networks/cambridge-analytica-closes.html

https://www.bilan.ch/economie/operation-rubicon-la-suisse-dans-le-mal

http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#view/fn-44

https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf

https://blogs.letemps.ch/solange-ghernaouti/

https://phoenixnap.com/blog/cyber-security-attack-types

https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html

http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html

https://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Allez Savoir n°75, «Un monde virtuel, une pollution bien réelle, Rencontre avec Solange Ghernaouti, Professeure et spécialiste en cybersécurité à l'UNIL», Sept 2020
https://com-www.unil.ch/allezsavoir/AS075.pdf

OCDE (2019), «Artificial Intelligence in Society», OECD Publishing
https://www.oecd-ilibrary.org/docserver/aa565467-fr.pdf

Cardon, Dominique. 2018. «Le pouvoir des algorithmes», Pouvoirs: Revue française d'études constitutionnelles et politiques no. 164: 63-73

Dessins et typographie: Eddy Juillerat – www.310.ch