les CADETTES DE LA CYBER

CYBERSÉCURITÉ :
Un défi citoyen et stratégique

Novembre 2025

PÔLE D'EXCELLENCE CYBER

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

SOMMAIRE

PRÉAMBULE

Par Iris HOURCADE

Cet ouvrage est l'avènement de plusieurs mois de travail de la part d'une communauté de jeunes femmes engagées dans le numérique et la cyber.

Porté par une dizaine de Cadettes c'est à travers ces pages qu'elles portent un message simple et nécessaire : les femmes ont leur place dans ce milieu, elles en maîtrisent les enjeux, et elles y réussissent. Ingénieures, juristes, géo-politologues, techniciennes… Elles travaillent, analysent, protègent et aujourd'hui, elles écrivent.

Cet ouvrage, c'est leur travail. Pas un manifeste, pas un plaidoyer : un livre pratique, né d'un constat simple : le numérique, tout le monde en parle, les cybermenaces, tout le monde en a peur. Mais qui explique vraiment comment ça marche, sans jargon ni fatalisme ? Qui montre que la sécurité informatique, ce n'est pas qu'une affaire de «hackers en capuche», mais bien un enjeu de société qui concerne les hôpitaux, les PME, les citoyens, et oui, aussi les femmes ?

L'idée est venue de Naïké Fremin du Sartel (Directrice de la communication au Pôle d'excellence cyber) et Dylan Massieux (Chargé de communication au Pôle d'excellence cyber), qui ont imaginé un projet ambitieux : et si les Cadettes écrivaient un livre grand public ? Pas un manifeste, pas un plaidoyer, mais un ouvrage concret, fait par celles qui vivent la cyber au quotidien. Contrairement à leurs actions habituelles souvent tournées vers les jeunes, cette fois, l'enjeu était plus large : s'imposer dans le paysage professionnel et prouver que leur place y est naturelle.

Un projet comme celui-ci ne voit le jour que grâce à l'implication de nombreuses personnes. Charlotte Wojcik, la fondatrice du programme des Cadettes de la Cyber mais aussi d'un comité de relecture qui nous a apporté leur expertise et un retour précieux. Enfin, merci aux cadettes, qui ont trouvé le temps d'écrire, relire et peaufiner chaque article souvent tard le soir, entre deux réunions ou deux partiels.

Ce livre ne vous dira pas que la cyber, c'est facile.

Mais il vous montrera que c'est moins compliqué qu'on ne le croit et que les femmes en parlent très bien.

Alors, on commence ?

PRÉFACE

Par Véronique TORNER, Présidente de Numeum
Marraine de la 4e promotion des Cadettes de la Cyber

Dans un monde où le numérique s'insère toujours plus profondément dans notre quotidien, la cybersécurité n'est plus seulement une préoccupation technique : elle est devenue un enjeu citoyen, éthique et sociétal.

La protection de nos données, de notre vie privée et de nos interactions en ligne, touche chacune et chacun d'entre nous, et il est essentiel que chacun comprenne les mécanismes et les bonnes pratiques qui permettent de naviguer en toute sécurité dans cet univers complexe.

C'est dans cet esprit que je salue l'initiative des Cadettes de la Cyber, qui, à travers ce projet, démontrent que l'engagement, la curiosité et l'expertise peuvent transformer la manière dont nous abordons la cybersécurité.

L'Équipe de France du Numérique incarne cette volonté de fédérer et de donner une voix forte et unie à l'ensemble de la filière. Face aux défis de notre siècle, il est essentiel de dépasser la fragmentation de notre écosystème pour mieux agir collectivement. Ce collectif inédit, qui réunit déjà plus de 70 organisations issues de tous horizons illustre la richesse et la diversité de nos talents. En mettant en synergie leurs initiatives et leurs expertises, ces acteurs construisent une dynamique commune au service d'un numérique plus puissant, durable et compétitif. Notre ambition est claire : unir les forces de la filière numérique pour mieux peser, mieux agir.

Parmi les grands projets portés par l'Équipe de France du Numérique, la féminisation du secteur occupe une place centrale, car elle constitue à la fois un impératif d'équité et un levier stratégique d'innovation et de compétitivité. Dans la cybersécurité en particulier, domaine ou la résilience et la vigilance conditionnent la confiance numérique, la diversité des parcours et des regards est une richesse indispensable. Nous ne pouvons pas bâtir un espace numérique innovant, sûr et responsable en nous privant de la moitié de l'humanité : ce serait renoncer à un réservoir considérable de talents, de créativité et de compétences.

Miser sur la féminisation, c'est donc refuser une vision appauvrie et incomplète du numérique, et choisir au contraire d'élargir le champ des possibles pour mieux relever les défis technologiques, économiques et sociétaux de notre temps. La compétitivité de notre filière en dépend : dans un contexte mondial où la puissance numérique est un facteur de souveraineté, il serait impensable de se priver de ces contributions décisives. Promouvoir la place des femmes dans le numérique et dans la cybersécurité, c'est non seulement un devoir d'équité, mais aussi une condition incontournable pour bâtir un futur numérique plus diversifié, plus durable et véritablement à la hauteur de nos ambitions collectives.

L'ouvrage que vous vous apprêtez à découvrir est bien plus qu'un guide technique : il est un outil pédagogique et citoyen, destiné à sensibiliser chacun aux enjeux de la cybersécurité dans la vie quotidienne. Il illustre comment la vigilance, la réflexion et la responsabilité individuelle peuvent, ensemble, créer un environnement numérique plus sûr et plus éthique.

En tant que présidente de Numeum et marraine de le 4è promotion des Cadettes, je suis profondément honorée de soutenir ce projet. Il reflète les valeurs qui me tiennent à cœur : l'excellence, l'innovation responsable et la promotion de talents féminins dans la tech.

Aujourd'hui, chacun de nous, qu'il soit citoyen, professionnel ou étudiant, a un rôle à jouer.

La cybersécurité n'est pas seulement l'affaire des experts : elle est l'affaire de tous. En adoptant des pratiques responsables, en partageant nos connaissances et en restant vigilants, nous contribuons à bâtir un numérique plus sûr, plus inclusif et plus respectueux de chacun. Que ce message guide chacun de vos pas dans l'univers numérique et inspire votre engagement citoyen.

La cybersécurité n’est pas une affaire de genre. Pourtant, elle reste trop souvent perçue comme un domaine réservé aux hommes, aux experts, aux techniciens en blouse blanche.

Rien n’est plus faux et cet ouvrage en est la preuve.

INTRODUCTION

Par Hélène Chinal, Vice-présidente en charge des Enjeux Sociétaux | Pôle d’excellence cyber

Réalisé par les Cadettes de la Cyber, un collectif de jeunes femmes passionnées et engagées, il démontre que la sécurité numérique se construit aussi par la diversité des regards, des expériences et des approches.

Les cyberattaques contre les hôpitaux, les fraudes en ligne qui touchent des milliers de citoyens, les campagnes de désinformation qui fracturent nos sociétés : ces menaces ne discriminent pas. Pourquoi, alors, ceux qui les combattent seraient-ils tous identiques ? À travers des études de cas concrets, les autrices de cet ouvrage décryptent les mécanismes des attaques, analysent les vulnérabilités et proposent des solutions mais surtout, elles montrent qu’une autre cybersécurité est possible : plus collaborative, plus accessible, et porteuse de sens pour toutes et tous.

Aujourd’hui, les femmes ne représentent que 11 % des effectifs mondiaux en cybersécurité. Ce déséquilibre n’est pas seulement une injustice, c’est un risque pour notre résilience collective. Comment protéger un monde numérique complexe si nous nous privons de la moitié des talents ? Les Cadettes de la Cyber répondent à ce défi avec brio. Leur travail prouve que la cybersécurité n’est pas une discipline élitiste, mais un savoir-faire qui s’apprend, se partage et se réinvente, surtout quand on ose sortir des sentiers battus.

Cet ouvrage est bien plus qu’un guide pratique. C’est un manifeste pour une cybersécurité inclusive, où chaque lecteur, étudiant, professionnel, décideur ou citoyen, trouvera des clés pour agir. Mais c’est aussi un appel: celui de rejoindre ce mouvement, de briser les stéréotypes, et de faire de la sécurité numérique un levier d’égalité et de progrès. Car si les cybermenaces concernent tout le monde, les solutions doivent être imaginées par tous et surtout par toutes.

En découvrant ces analyses, j’espère que vous serez, comme moi, impressionné par la rigueur et l’audace de ces jeunes femmes, qui transforment un secteur encore trop masculin en un espace d’opportunités. Et surtout, que vous retiendrez cette conviction : la cybersécurité de demain se construira avec la diversité ou elle ne sera pas.

Hélène
CHINAL

CYBERSÉCURITÉ ET SOUVERAINETÉ

01

- Symboles détournés et souveraineté numérique : le cas de TikTok
- Cryptomonnaies : Outils de liberté ou armes géopolitiques ?
- Les câbles sous-marins en Polynésie française : une infrastructure à risques.

SYMBOLES DÉTOURNÉS ET SOUVERAINETÉ NUMÉRIQUE :

Le cas de TikTok :

Depuis plusieurs mois, des signalements d'associations, des enquêtes de journalistes mais également des rapports de police, révèlent l'utilisation détournée d'émojis sur TikTok pour dissimuler des références à la pédocriminalité[1]. Derrière ces pratiques se cache un réseau qui exploite la viralité de la plateforme pour en contourner les règles de modération. Cette dérive soulève des enjeux géopolitiques où se mêlent la souveraineté numérique, la sécurité ainsi que la gouvernance des plateformes et des tensions entre les puissances numériques.

1 *Pédocriminalité : le sens caché des emojis*, 2025, https://www.youtube.com/watch?v=sUp70DTKKIQ , consulté le 9 juillet 2025

Des symboles qui peuvent être perçus comme anodins deviennent alors des codes implicites dans les communautés de pédocriminels qui échappent à la modération algorithmique. En effet, ces utilisateurs emploient des codes visuels ou linguistiques issus du lexique crypté dans le monde de la pédopornographie. L'un des exemples les plus courants est celui de la pizza. En anglais le terme « cheese pizza » est utilisé comme acronyme pour « child pornography »[2]. Ainsi, l'emoji, et les mots-dièse associés peuvent être utilisés pour signaler discrètement un intérêt sexuel envers les enfants, tout en échappant à la détection automatique. L'algorithme de TikTok, conçu pour maximiser l'engagement, analyse les comportements des utilisateurs (likes, commentaires, partages) et recommande des contenus similaires. Cela créer un effet de spirale algorithmique, où des utilisateurs malveillants se voient proposer toujours plus de contenus mettant en scène des enfants, ce qui invisibilise la toxicité du réseau et favorise la diffusion de ces contenus[3]. Ce phénomène montre comment un espace numérique à vocation récréative peut être infiltré par des logiques criminelles, à quel point l'intelligence artificielle peut être détournée.

La prolifération de ces contenus illégaux sur TikTok révèle les limites de l'action étatique face aux plateformes transnationales[4]. En effet, TikTok, propriété du groupe chinois ByteDance, fonctionne selon des logiques commerciales et techniques qui échappent aux juridictions locales. Même en Europe, où le Digital Service Act impose désormais aux grandes plateformes des obligations de modération plus strictes, les résultats sont limités par le manque de moyens humains, l'opacité des algorithmes et les obstacles à la coopération transnationale4. Dans ce contexte, la notion de souveraineté numérique prend une dimension centrale. Les États peinent à faire appliquer leurs lois aux plateformes numériques comme TikTok, qui touchent leur population mais échappent en grande partie à leur juridiction car elles ne sont pas établies légalement sur leur territoire. Les moyens de modération sont aujourd'hui largement automatisés et souvent inefficaces face à l'évolution constante des codes utilisés. En parallèle, des communautés malveillantes continuent d'adapter leurs stratégies afin de contourner la censure, en s'appropriant de nouveaux symboles, comme expliqué précédemment.

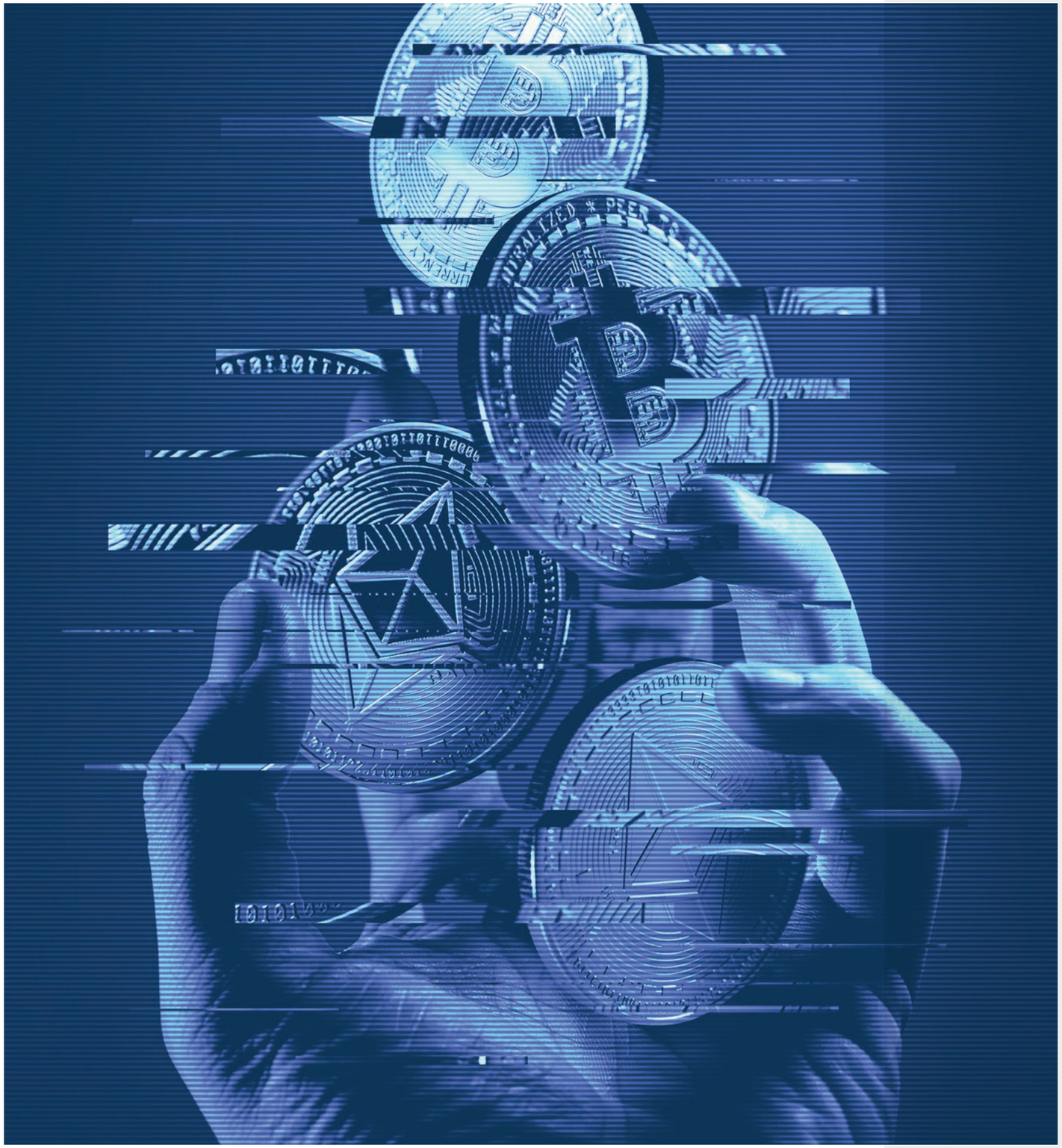
Face à l'impuissance croissante des Etats à réguler efficacement les plateformes comme TikTok, ces enjeux de modération et de sécurité ne relèvent plus uniquement de la protection des citoyens mais deviennent aussi le terrain d'une confrontation plus large entre puissances numériques. Derrière l'apparente neutralité technologique des algorithmes, se joue une compétition stratégique pour le contrôle des données.

Les Etats Unis ont désormais franchi un cap en adoptant une loi imposant à ByteDance de se séparer de l'application sous peine d'interdiction de l'application sur l'ensemble du territoire. Les raisons invoquées sont celles de la sécurité nationale, comme la question autour de la collecte de données sensibles, ou encore celle de l'incapacité de la plateforme à protéger les mineurs[5]. Cette menace, mise à exécution dans un premier temps, est actuellement suspendue[6]. L'Union Européenne a également intensifié la pression sur TikTok. En mai 2025, l'Autorité irlandaise de protection des données a infligé une amende de 530 millions d'euro à la plateforme. ByteDance est ici accusée d'avoir transféré illégalement les données des utilisateurs européens vers la Chine, violant ainsi le Règlement Général de Protection des Données (RGPD)[7]. Ces mesures témoignent de la volonté croissante des Etats et des institutions européennes d'imposer une régulation plus stricte aux grandes plateformes, notamment en matière de souveraineté numérique et de protection des données personnelles.

Au-dela des questions de régulation et de modération, la multiplication des sanctions contre TikTok, qu'elles viennent des Etats-Unis ou de l'Union Européenne, illustre une inquiétude plus large : celle d'un affrontement entre modèles de gouvernance numérique. Pour la Chine, TikTok ne constitue pas seulement une entreprise privée, mais un instrument stratégique d'influence globale. En exportant une plateforme difficilement contrôlable par les juridictions occidentales, Pékin propose un contre-modèle à la régulation numérique libérale défendue par l'Europe et les Etats-Unis. Dans ce contexte, TikTok est perçu comme un levier d'expansion technologique et culturelle, renfonçant une gouvernance numérique profondément liée aux intérêts chinois. Cette situation illustre une nouvelle forme de rivalité stratégique, où le contrôle des données et des normes numériques devient un enjeu de puissance.

Par Diarra MBAYE

2 Op cité.
3 *Global: TikTok's 'For You' feed risks pushing children and young people towards harmful mental health content - Amnesty International*, https://www.amnesty.org/en/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/, consulté le 11 juillet 2025.
4 *Aristotelis, Violation de la DSA ? La Commission européenne prend de nouveau des mesures contre TikTok*, https://2b advice.com/fr/2025/05/15/infraction-a-la-dsa-la-commission-europeenne-prend-des-mesures-contre-tiktok/ , 15 mai 2025, consulté le 18 juillet 2025.
5 *TikTok aux Etats-Unis : tout comprendre de la situation en 4 dates clés*, https://www.brut.media/fr/articles/culture lifestyle/reseaux-sociaux/tiktok-aux-etats-unis-tout-comprendre-de-la-situation-en-4-dates-cles, consulté le 18 juillet 2025.
6 *Vente de TikTok aux Etats-Unis : Donald Trump va de nouveau reporter la date butoir*, https://www.lemonde.fr/pixels/article/2025/06/18/vente-de-tiktok-aux-etats-unis-donald-trump-va-de-nouveau-reporter-la-date butoir_6613989_4408996.html, consulté le 18 juillet 2025.
7 *TikTok condamné à 530 millions d'euros d'amende pour avoir enfreint le RGPD*, https://www.leclubdesjuristes.com/en bref/tiktok-condamne-a-530-millions-deuros-damende-pour-avoir-enfreint-le-rgpd-10535/ , 2 mai 2025, consulté le 18 juillet 2025.



CRYPTOMONNAIES :

Outils de liberté ou armes géopolitiques ?

San Salvador, 2021. Sous les applaudissements de ses partisans, le président Nayib Bukele annonce une mesure historique [8]: le Salvador devient le premier pays au monde à adopter le Bitcoin comme monnaie légale.

8 *Le BITCOIN reconnu comme MONNAIE légale | El Salvador*, s.l., s.n., 2021.

«C'est une révolution pour l'inclusion financière», promet-il.

L'objectif est clair : réduire les frais de transferts, attirer les investisseurs étrangers et donner accès aux services financiers aux 70 % de Salvadoriens non bancarisés[9]. Mais quatre ans plus tard, l'expérience s'est transformée en leçon d'humilité : le Bitcoin n'a pas changé le Salvador, c'est le Salvador qui a mis en lumière les limites du Bitcoin.

Quand la promesse d'émancipation rencontre la réalité du terrain :

À l'origine, les cryptomonnaies ont été pensées comme une alternative au système bancaire, un moyen d'échanger sans intermédiaire, de transférer de l'argent sans contrôle, et d'échapper à la dépendance au dollar. Dans les faits, elles se sont rapidement transformées en un écosystème à plusieurs visages : à la fois outil d'émancipation, instrument géopolitique et vecteur de dérives.
Dans les rues de San Salvador, Maria, vendeuse de pupusas, a essayé le Bitcoin grâce aux 30 dollars offerts via l'application gouvernementale Chivo Wallet. *«Au début, c'était nouveau, j'étais curieuse»*, raconte-t-elle. *«Mais les clients préfèrent le cash, et je ne comprends pas quand le prix change tous les jours.»*[10] Comme elle, des milliers de Salvadoriens ont abandonné l'usage du Bitcoin après la phase de découverte. Moins de la moitié ont téléchargé l'application et seulement 40 % l'utilisent encore. En 2025, face à la pression du FMI[11] (Fonds Monétaire International) et au rejet populaire, le gouvernement a retiré au Bitcoin son statut de monnaie légale.

Le bilan est clair :

- 20 % des entreprises acceptent le Bitcoin, mais 88 % le convertissent immédiatement en dollars.
- Les rémittences (transferts d'argent depuis l'étranger) en Bitcoin représentent moins de 2 % du total.
- Les promesses de «Bitcoin City» et d'afflux d'investisseurs étrangers ne se sont jamais concrétisées.

L'expérience salvadorienne révèle une vérité essentielle : la technologie seule ne suffit pas. Sans éducation financière, sans confiance et sans stabilité, même les innovations les plus ambitieuses échouent à s'ancrer dans le quotidien.

Les cryptomonnaies : entre contournement des sanctions et levier géopolitique :

Pendant que le Salvador tâtonne, d'autres pays utilisent les cryptomonnaies d'une tout autre manière. l'Iran[12] utilise ses ressources en électricité pour «miner»[13] du Bitcoin, c'est-à-dire participer au fonctionnement du réseau en validant des transactions, ce qui rapporte de la cryptomonnaie. Grâce à cette méthode, l'Iran peut obtenir des devises qu'il ne peut plus obtenir via les banques, à cause des restrictions internationales. La Corée du Nord [14], quant à elle, est accusée d'utiliser un autre procédé, celui des cyberattaques menées par le groupe Lazarus, soutenu par l'État. Ces cyberattaques visent des plateformes d'échange de cryptomonnaies, avec des vols estimés à plusieurs centaines de millions de dollars[15]. Ce type d'utilisation est possible car les transactions en cryptomonnaie sont souvent plus difficiles à retracer que les virements bancaires classiques.

Face à ces pratiques, les pays occidentaux s'organisent. Des entreprises spécialisées comme Chainalysis sont chargées d'analyser les flux d'argent pour identifier les transactions suspectes. Parallèlement, des institutions comme l'Union européenne ou le GAFI (Groupe d'action financière)[16] renforce ses régulations (règlement MiCA). Mais la lutte est complexe ; les privacy coins comme Monero ou Zcash, conçues pour masquer les transactions, et les services de mixage de fonds (comme Tornado Cash) brouillent les pistes, rendant le blanchiment quasi indétectable.

La réponse des États : les monnaies numériques souveraines :

Pour ne pas laisser le champ libre aux cryptomonnaies privées, plusieurs grandes puissances développent leurs monnaies digitales de banque centrale (CBDC).
- La Chine a déjà lancé son e-yuan, testé dans plusieurs grandes villes.
- La Russie prépare un rouble numérique.
- Les États-Unis explorent un projet de dollar digital.

L'objectif est de reprendre le contrôle des flux financiers et préserver la souveraineté monétaire dans

9 *L'économie circulaire du Bitcoin s'attaque aux mentalités bien ancrées au Salvador*, https://www.coindesk.com/fr/opinion/2023/08/28/the-bitcoin-circular-economy-battles-entrenched-mindsets-in-el-salvador, consulté le 10 octobre 2025.
10 « *L'envolée du bitcoin a été formidable » : au Salvador, certains habitants se frottent les mains*, https://www.bfmtv.com/crypto/bitcoin/l-envolee-du-bitcoin-a-ete-formidable-au-salvador-certains-habitants-se-frottent-les-mains_AD-202403200301.html , 20 mars 2024, consulté le 10 octobre 2025.
11 GUIMOND Antoine, *Le Salvador fait un pas en arrière : Fin de l'utilisation du bitcoin comme monnaie officielle*, https://news.chastin.com/le-salvador-fait-un-pas-en-arriere-fin-de-lutilisation-du-bitcoin-comme-monnaie-officielle/ , 19 février 2025, consulté le 10 octobre 2025.
12 Le Monde, « *L'Iran mise sur le minage de cryptomonnaies pour contourner les sanctions* », avril 2024.
13 Boulanger Philippe, *Planète médias.* Géopolitique des réseaux et de l'influence, 2021.
14 The Guardian, « *North Korea's Lazarus Group and the $600M Crypto Heist* », mars 2024
15 Chainalysis, *Crypto Crime Report 2024*, https://www.chainalysis.com
16 GAFI – Groupe d'Action Financière, www.fatf-gafi.org

un monde où le numérique redéfinit les rapports de force. Mais ces monnaies d'État posent elles aussi des questions allant de la protection des données, au risque de surveillance accrue, ou encore de vulnérabilité face aux cyberattaques, le numérique ne supprime pas les problèmes économiques mais il les transforme.

Trois usages des cryptomonnaies dans notre quotidien :

1. L'outil de liberté
Dans les zones de conflit ou sous régime autoritaire, les cryptomonnaies peuvent être un refuge[17]. En Ukraine, elles ont permis de financer la résistance dès les premiers jours de la guerre. À Hong Kong[18], les militants pro-démocratie y voyaient un moyen d'échapper à la surveillance bancaire.

2. Le placement spéculatif
Dans les pays développés, elles sont souvent perçues comme une nouvelle classe d'actifs. Mais leur volatilité extrême (le Bitcoin a perdu plus de 60 % de sa valeur en 2022) limite leur usage quotidien.
Pour beaucoup, la crypto reste un pari sur l'avenir plus qu'un moyen de paiement[19].

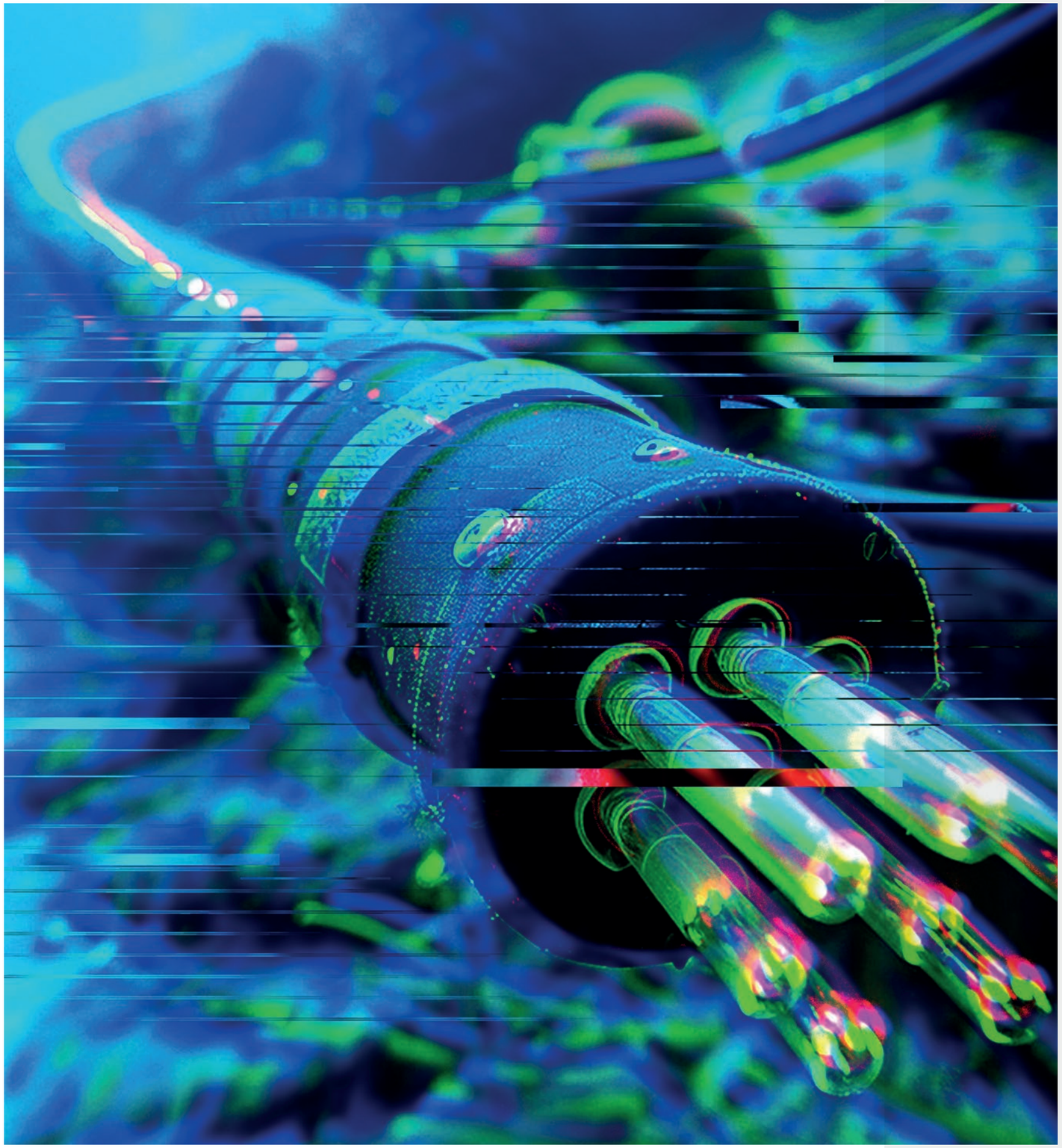
3. Le casse-tête des régulateurs
Fraudes, piratages, effondrement de plateformes comme FTX[20], les scandales ont fragilisé la confiance du public. Les régulateurs multiplient les garde-fous pour encadrer un marché aussi innovant qu'instable.

Les cryptomonnaies illustrent les deux visages du numérique. C'est à la fois un outil d'émancipation, capable de redonner du pouvoir aux citoyens et aux États marginalisés. Mais c'est aussi un moyen de déstabilisation, utilisée par les régimes autoritaires, les criminels, ou les spéculateurs.

Le cas du Salvador montre que la technologie seule ne suffit pas : sans acceptation populaire, sans cadre réglementaire solide, et sans pédagogie, même les projets les plus ambitieux peuvent échouer. À l'heure où les CBDC[21] se multiplient et où les cybermenaces se sophistiquent, une chose est sûre, le futur de la monnaie sera numérique… mais son succès dépendra de notre capacité à en maîtriser les risques.

Par Amal MERNIT

17 CHEVALLIER Valentin, *Les cryptomonnaies dans la guerre d'Ukraine ?*, https://institut-rousseau.fr/les-cryptomonnaies-dans-la-guerre-dukraine/ , 31 mars 2022
18 ADMIN, *Bitcoin Eyes Demand As Hong Kong Protestors Announce Bank Run* (#GotBitcoin?), https://dpl-surveillance-equipment.com/bitcoin-and-crypto-currency/bitcoin-eyes-demand-as-hong-kong-protestors-announce-bank-run-gotbitcoin/ , 7 octobre 2019
19 TAYLOR Chloe, « *Bitcoin is not an asset class »: UK's biggest investment platform has a stark warning for investors,* https://www.cnbc.com/2025/10/10/uk-investment-platform-warns-traders-to-avoid-bitcoin-crypto.html , 10 octobre 2025
20 *7 meilleures alternatives à FTX après leur effondrement* (octobre 2025), https://coinkickoff.com/fr/ftx-alternatives/
21 LAZARO Vincent, *Montée des monnaies numériques de banques centrales* (CBDC) : explications, https://www.numedia.fr/montee-monnaies-numeriques-de-banques-centrales-cbdc-explications-559142024.html , 24 juillet 2024



LES CÂBLES SOUS-MARINS EN POLYNÉSIE FRANÇAISE :

Une infrastructure à risques.

Aujourd'hui, 99% du trafic Internet passe parmi plus de 500 câbles sous-marins à fibre optique installés au fond des océans[22]. Ces infrastructures permettent d'assurer l'accès aux ressources Internet. Trop souvent, nous pouvons considérer l'accès à ce vaste réseau comme un bien acquis or ces câbles sont au cœur d'enjeux géostratégiques où chaque acteur souhaite tisser sa propre toile. Ces câbles représentent une cible privilégiée afin, par exemple, de couper et isoler une zone géographique du reste du monde. Cela nous rappelle que sans cet équipement de la couche physique du modèle Open System Interconnection, Internet ne peut pas fonctionner.

22 Article révisé en janvier 2025, https://geoconfluences.ens-lyon.fr/glossaire/cables-sous-marins

Cet article se consacre au cas unique de la Polynésie française. Elle se situe dans le Pacifique sud et est divisée en cinq archipels qui regroupent 118 îles pour 280 000 habitants seulement. Les 3 500 km² de terres émergées de la Polynésie française sont dispersées sur un territoire presque aussi vaste que l'Europe, ce qui lui offre une Zone Économique Exclusive (ZEE) prisée de 4,5 millions de km². Par conséquent, ces caractéristiques géographiques rendent le territoire difficile à couvrir et à relier à Internet de par sa fragmentation, sa large surface mais aussi ses reliefs. La Polynésie possède un statut singulier car elle est sous autonomie interne dans le cadre de la République Française. Elle est dirigée par le président Moetai Brotherson depuis mai 2023 qui a constitué son propre gouvernement ayant la fonction exécutive. L'île principale, Tahiti, concentre la majorité des implantations des forces armées françaises et permet aujourd'hui d'avoir une présence militaire locale. Cela représente un appui stratégique et une protection des zones maritimes françaises face aux excursions des Etats-Unis et de la Chine.

Un élément notable met en exergue une dépendance matérielle de ce territoire pour obtenir accès à Internet. Historiquement en Polynésie, l'accès à Internet se faisait via des connexions satellitaires à la fiabilité et au débit limités. Aujourd'hui, les points d'alimentation des câbles sous-marins de la Polynésie sont américains. Ils sont pour le moment principalement alimentés par deux nœuds : les Mariannes du Nord et Hawaï. Ces territoires sont tous deux sous l'autorité de l'administration américaine. Ces îles du Pacifique Nord alimentent et connectent le Pacifique sud à Internet. Cette toile ainsi tissée est donc stratégique pour les Etats-Unis en termes de souveraineté et constitue un atout majeur notamment en cas de conflit.

Cependant, le marché des câbles à fibre optique est complexe et dépend de différents acteurs à savoir le fournisseur de matières premières, le constructeur, le poseur, le mainteneur et enfin le/les propriétaires. La France n'a pas à rougir car elle s'impose en maître de la construction et de la pose des câbles avec notamment l'Alcatel Submarine Networks ou encore Orange Marine. Cependant, le premier propriétaire de câble est aujourd'hui un GAFAM, plus précisément Google qui possède trente-deux câbles à son actif dont dix-sept en tant que propriétaire exclusif. Et lorsque l'on parcourt la carte interactive mondiale des câbles sous-marins[23], on se rend compte que de nombreux câbles sud Pacifique sont détenus par Google mais aussi qu'un certain nombre vont être ajoutés grâce à de larges investissements dans la zone. En effet, fin février 2025, le président de la Polynésie a confirmé un ajout de huit câbles Google, dont le déploiement final est attendu pour la fin 2027. Cela pose des questions sur la confidentialité des informations qui transitent mais aussi sur la souveraineté. Dans son livre *Mémoires vives* publié en 2019, Edward Snowden[24] révèle qu'il a travaillé à Hawaï pour le compte de la NSA dans un ancien établissement militaire souterrain. Il y espionnait les informations qui passaient sur ces câbles transpacifiques. Rassurant, quand on sait que les informations sont nécessairement déchiffrées sur certains tronçons. Par cette politique de quadrillage du Pacifique Sud, le géant américain souhaite contrer l'émergence chinoise. En effet, la Chine a une empreinte visible en Polynésie Française, notamment dans les lycées où la langue vivante proposée est majoritairement le chinois. Il est ici essentiel de préciser que les documents chinois sur les « routes de la soie » (BRI) confirment que les câbles sous-marins font partie des axes d'influence portés par le pays.

Le constat en Polynésie française est que depuis 2016, le réseau Internet tend à se densifier, assurant ainsi le déploiement de la 2G, 3G et 4G dans les îles et aux larges des côtes. La 5G n'est pas présente, bien que clamée par les opérateurs principaux que sont : Vini, Vodafone et Ora. La progression n'est pas uniforme car elle se fait par zone. Elle a commencé par les îles les plus peuplées, plaçant des archipels en seconde zone de priorité. Les habitants payaient alors des forfaits chers pour une qualité de connexion maigre. Néanmoins, les niveaux de prix se sont rapprochés avec l'ouverture à la concurrence ces dernières années. En 2016, les communications[25] (téléphonie, mobile et Internet) étaient 95 % plus chères en Polynésie française qu'en métropole alors qu'en 2022, l'écart mesuré s'élève à 33 %. Au quotidien, il est commun de constater des pannes réseaux fréquentes et des fortes latences. Le secteur médical doit alors s'adapter avec des circuits secondaires afin d'assurer un maintien des services et des aides à la population. En moyenne, le débit y est quatre fois plus faible qu'en métropole. Il est alors nécessaire de préciser qu'en termes de clientèle, la comparaison est simple : 60 millions de consommateurs contre à peine 250 000 en Polynésie ce qui explique en partie cette transition lente de la connectivité.

Les différents projets de câbles financés entre autres par Google sont donc bienvenus par la population locale. Mais une autre technologie, dont l'utilisation est toujours interdite en Polynésie, émerge de plus en plus sur le territoire. Il s'agit de délaisser les opérateurs agréés, qui reposent sur les câbles à fibre optique, pour le service satellitaire Starlink grâce à une mini-antenne dédiée[26]. Les raisons de cette interdiction évoquent une mise en concurrence sur le marché de la fourniture d'accès à Internet mais pointent également un non-respect des normes françaises. A noter que l'importation des antennes Starlink n'est pas illégale. Cette situation singulière de part son étrangeté est fortement dénoncée par les polynésiens.

Aux termes de cet article, il devient évident que la Polynésie française est au cœur d'enjeux stratégiques pour la souveraineté de la technologie des câbles à fibre optique. Cette zone est un théâtre d'opérations pour affirmer autorité et influence de la part de différentes nations sur des territoires isolés tels que la Polynésie. Le sujet de l'accès à Internet n'est pas récent mais est très important pour assurer à la population locale une connexion et donc un lien avec le reste du monde.

Par Léa GRIFFON

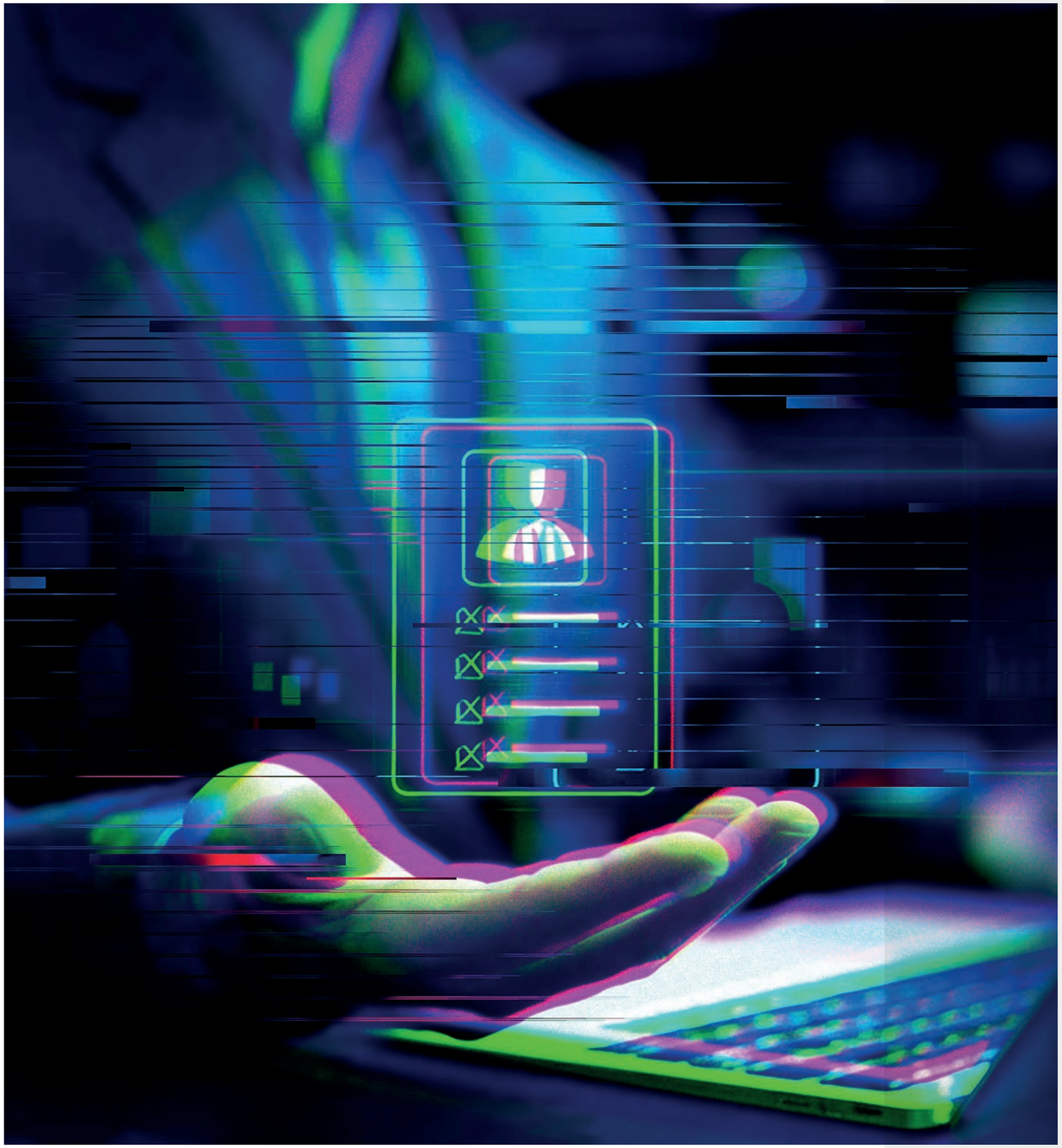
23 Carte interactive mondiale des câbles sous-marins https://www.submarinecablemap.com/
24 Lanceur d'alerte qui a travaillé des années pour la CIA (Central Intelligence Agency) puis pour la NSA (National Security Agency).
25 Selon une étude ISPF (Institut de la statistique de la Polynésie française) publiée en octobre 2023

26 Starlink est le fournisseur d'accès à Internet développé par l'entreprise américaine SpaceX qui s'appuie sur sa constellation de satellites en orbite basse. Cela permet de réduire significativement la latence et de fournir du haut débit.

02

DONNÉES, INFLUENCE ET DÉMOCRATIE

- Exploitation des données : Comment nos informations personnelles peuvent être vendues, analysées ou détournées pour influencer les décisions politiques et économiques
- Cyberattaques et Genre : un nécessaire changement de paradigme ?



EXPLOITATION DES DONNÉES :

Comment nos informations personnelles peuvent être vendues, analysées ou détournées pour influencer les décisions politiques et économiques

À l'ère du numérique, chacune de nos activités quotidiennes laisse une empreinte digitale. Smartphones, objets connectés, applications et réseaux sociaux produisent, partagent et analysent en continu nos données personnelles.

Longtemps exploitées à des fins marketing ou pour améliorer l'expérience utilisateur, ces données servent désormais à prédire et parfois influencer nos comportements, soulevant de nouveaux défis démocratiques. Leur collecte, souvent déguisée derrière la gratuité des services, alimente une économie numérique de plusieurs centaines de milliards d'euros[27]. Cet article s'intéresse à ce glissement de l'usage des données vers l'influence politique et sociale, en s'appuyant sur le cas emblématique de Cambridge Analytica, avant d'interroger la capacité des sociétés européennes, notamment la France, à relever ce défi.

L'affaire Cambridge Analytica : une démonstration de l'influence politique par les données

En 2018, le scandale éclate : Cambridge Analytica, société britannique de conseil politique, a illégalement exploité les données de 87 millions d'utilisateurs[28]. Une application Facebook, présentée comme un test de personnalité à visée académique, permettait en réalité de collecter non seulement les données des utilisateurs ayant accepté l'installation, mais également celles de leurs amis[29] — sans leur consentement explicite[30]. Ainsi, à partir de seulement 270 000 utilisateurs initiaux, Cambridge Analytica a accédé aux données personnelles de près de 87 millions de profils dans le monde. Ces données incluaient sexe, âge, localisation, centres d'intérêt et interactions sociales.

Cambridge Analytica utilisait un modèle de profilage psychométrique fondé sur les Big Five[31]. L'objectif était de relier des comportements numériques (likes, contenus consultés, publications) à des traits de personnalité, afin de segmenter l'électorat et de diffuser des messages politiques personnalisés, adaptés aux émotions, valeurs ou vulnérabilités de chacun : cette méthode s'appelle le microciblage comportemental. Par exemple, les électeurs anxieux recevaient des messages alarmistes sur l'immigration, et les indécis des contenus émotionnels voire trompeurs. Cette stratégie fut utilisée dans plusieurs campagnes majeures, dont le référendum sur le Brexit et l'élection présidentielle de Donald Trump en 2016[32].

Focus sur la France : exploitation des données, un danger sous-estimé ?

Si ces pratiques ont d'abord concerné les campagnes anglo-saxonnes, la France n'est pas épargnée. L'écosystème français mêle acteurs publics, start-ups et dépendance à des plateformes souvent étrangères notamment auprès des GAFAM[33]. Une hybridation qui complexifie la gouvernance et la régulation des données.

Des outils de profilage électoral sont apparus dès la présidentielle de 2017, notamment pour la campagne d'Emmanuel Macron. Des entreprises françaises telles que Liegey Muller Pons ou Qomo[34] proposent désormais des services de géolocalisation électorale, de cartographie sociale et de ciblage par zone ou catégorie. En 2022, des soupçons de microciblage via Facebook Ads ont été soulevés[35]. Parallèlement, des plateformes comme YouTube, TikTok ou X jouent un rôle non négligeable dans la circulation des idées politiques, en accentuant certaines opinions ou controverses par le biais d'algorithmes de recommandation[36].

Comment mobiliser conjointement ces trois dimensions pour garantir à la fois la protection des données et la préservation de notre liberté de décision ?

Face à cela, le cadre juridique européen notamment le RGPD impose des principes fondamentaux : consentement libre et éclairé, droit à l'oubli, portabilité des données. En France, la CNIL est l'autorité chargée de veiller à leur application. Le consentement doit être libre, spécifique, éclairé et univoque. En théorie, chaque individu devrait pouvoir choisir ce qu'il partage et avec qui. En pratique, ce consentement est souvent biaisé, expéditif les utilisateurs cliquent sur « accepter » sans lire voire illusoire : refuser l'accès revient parfois à se priver du service.

Pour une culture numérique partagée : au-delà du cadre légal

27 OECD (2020), *Data-Driven Innovation for Growth and Well-Being*
28 The Guardian, «*Cambridge Analytica scandal*», 2018
29 L'origine remonte à 2014, le chercheur Aleksandr Kogan, via sa société Global Science Research (GSR), développe une application Facebook nommée *This Is Your Digital Life.*
30 Wired, «*Facebook Owes You More Than This*», 2018
31 Big Five ou OCEAN : Ouverture, Conscience, Extraversion, Agréabilité, Névrosisme. Voir *Private traits and attributes are predictable from digital records of human behavior.*
32 Channel 4 News, «*Data, Democracy and Dirty Tricks*», 2018
33 Le recours à Microsoft Azure pour le Health Data Hub a suscité de vives critiques de la CNIL et du Conseil d'État en 2022, Avis sur Health Data Hub, 2020
34 LMP, Qomon - Sites officiels.
35 Mediapart, «*Ciblage electoral en 2022*», avril 2022
36 Une étude menée par l'INA et Sciences Po en 2022 a montré que les vidéos politiques les plus recommandées sur YouTube penchaient souvent vers des discours anti-gouvernementaux ou populistes. INA & Sciences Po (2022), «*Recommandations politiques*» sur YouTube

Au-delà du droit, la régulation se heurte à plusieurs limites : lenteur des procédures, domiciliation étrangère des plateformes, traitement opaque des données. Certains rapports du Conseil national du numérique ou du Défenseur des droits appellent à une transparence accrue des algorithmes, notamment ceux utilisés par les grandes plateformes. C'est l'un des objectifs du Digital Services Act (DSA), entré en vigueur en 2024, qui prévoit davantage de transparence algorithmique mais sa mise en œuvre soulève encore des interrogations juridiques.

La sensibilisation s'impose alors comme un levier démocratique fondamental[37] car un consentement n'a de valeur que s'il est véritablement éclairé. Bien que des initiatives portées par des acteurs publics et associatifs émergent, elles restent limitées face à la puissance du marketing numérique, qui incite à la surexposition volontaire des données (jeux concours, applications gratuites, cookies intrusifs[38]). La véritable question est donc celle de l'articulation entre droit, technique et éducation citoyenne : comment mobiliser conjointement ces trois dimensions pour garantir à la fois la protection des données et la préservation de notre liberté de décision ?

Par Massilia BOULARAOUI

37 CNIL, associations d'éducation populaire (Framasoft ou la Quadrature du Net), médias, écoles mènent des actions pédagogiques sur la vie privée, le paramétrage des réseaux sociaux ou l'usage raisonné des écrans. Voir par exemple : *CNIL, Tous ensemble, prudence sur Internet !*
38 CNNum, Education au numerique, 2023

CYBERATTAQUES ET GENRE :

Un nécessaire changement de paradigme ?

Avec l'augmentation des cyberattaques à travers le monde, les parties prenantes du secteur se sont principalement concentrées sur la gestion rapide des incidents, l'assistance aux organisations affectées ainsi que sur la réponse judiciaire apportée à ces attaques. Cependant, les rapports grand public (ANSSI, Cybermalveillance) abordent encore de manière limitée l'analyse des typologies de victimes individuelles, notamment en ce qui concerne leur genre ; pourtant, l'intégration de tels paramètres permettrait d'offrir une réponse et une assistance mieux adaptées aux victimes.

Cet article vise ainsi à éclairer cette zone d'ombre en analysant les victimes des cyberattaques sous le prisme du genre ; il suggérera également des solutions proposées par des chercheurs et chercheuses en études de sécurité.

I - Des attaques genrées avec des conséquences différenciées

Cyberattaques "classiques" - Des attaques qui touchent en majorité les hommes

D'après une enquête Ipsos publiée en septembre 2024, les trois principales attaques signalées sur Cybermalveillance en 2024 - hameçonnage, le piratage de compte, les faux ordres de virement[39] - concernent majoritairement les hommes âgés de 18 à 34 ans : 47% d'entre eux ont subi un virus informatique, 42% ont vu leur compte en ligne être piraté et 34% ont été victime d'utilisation frauduleuse de leur carte bancaire, contre respectivement 34%, 30% et 23% des femmes de la même tranche d'âge. Au total, les hommes sont 66% à être sujets de cybermalveillances contre 57% de femmes.

Cela peut s'expliquer par les différences de comportement en ligne des utilisateurs, influencée par leur socialisation genrée. En effet, les jeunes hommes tendent à avoir des comportements plus risqués : ils représentent près de 85% des utilisateurs du dark web[40]. Ils ont également tendance à utiliser un plus grand nombre d'applications et d'appareils connectés, ce qui augmente le risque de cyberattaque.
Pour les victimes de ce type de cyberattaque, si 22% des victimes estiment avoir subi une perte financière et matérielle, l'impact psychologique (perte de confiance, anxiété, dépression) reste limité, puisqu'il concerne environ 9% des victimes.[41]

Sextorsion, Revenge porn, Cyberviolence : une répartition genrée qui peut surprendre

De même, les attaques à caractère sexuel touchent de manière disproportionnée les femmes et les hommes, avec des résultats qui semblent à première vue contre-intuitifs :

- La sextorsion, une cyberattaque qui consiste à obtenir de la victime des vidéos ou photos à caractère sexuel, souvent par les réseaux sociaux, pour ensuite faire du chantage, a augmenté de 924% entre 2023 et 2024 et touche majoritairement des hommes : au Royaume-Uni, 91% des signalement étaient des garçons, en général âgés de 14 à 18 ans.[42]
- En revanche, le revenge porn, aussi appelé pornodivulgation, qui désigne la diffusion non consentie d'images ou de vidéos à caractère sexuel, souvent par un ex-partenaire, dans un but de vengeance, d'humiliation ou d'extorsion, touche en majorité les femmes : selon l'étude de l'organisation Cyber Civil Rights Initiative, 90% des victimes étaient des femmes. Pour 57% des victimes, le contenu avait été posté par leur ex-compagnon, et dans 23% des cas, par un ami.[43]

Il faut ainsi rappeler que les femmes sont également victimes de cyberviolence (terme désignant tout acte de violence commis à travers le numérique, touchant à l'humiliation, l'insulte, la menace, la diffusion d'informations privées ou de contenus humiliants, le harcèlement ou la manipulation en ligne)[44] en raison de leur genre : selon l'enquête Ipsos menée par l'association Féministes contre le cyberharcèlement, 84% des victimes de cyberviolences sont des femmes, et 43% sont des personnes LGBTQIA+. [45]

L'impact psychologique de la cyberviolence - qui inclut également les situations de harcèlement - est bien plus élevé que pour les cyberattaques citées en première partie : 49% des victimes de diffusion d'informations intimes ont déclaré avoir pensé au suicide. 34% des victimes de publication de photos dégradantes ou intimes ont déclaré avoir fait une tentative de suicide. Les femmes victimes sont également plus nombreuses à se sentir déprimées et désespérées à la suite de cyberviolences.[46]

II - Au-delà des recommandations classiques, une nouvelle approche prônée par les sciences sociales : des politiques de cybersécurité fondées sur les droits humains

La France applique principalement une approche centrée sur la protection des infrastructures, des

39 Panorama de la menace 2024, ANSSI
40 Tajammul Pangarkar, « *Dark Web Statistics By Country, Demographics And Facts (2025)* », Sci-Tech Today (blog), 21 mai 2025, https://www.sci-tech-today.com/stats/dark-web-statistics-updated/.
41 « *Cybermoi/s 2024 : les Français face aux cybermenaces Une étude IPSOS pour Cybermalveillance.gouv.fr* », Assistance aux victimes de cybermalveillance, consulté le 30 juin 2025, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermois-2024-etude-ipsos.
42 Par Le Parisien avec AFP Le 30 avril 2024 à 00h21, « *Chantage aux photos intimes visant des adolescents : face au nombre de cas, la police britannique alerte les enseignants* », leparisien.fr, 29 avril 2024, https://www.leparisien.fr/international/chantage-aux-photos-intimes-visant-des-adolescents-face-au-nombre-de-cas-la-police-britannique-alerte-les-enseignants-30-04-2024-CPL5HPZLJRB7JILFGTICASUMVU.php.
43 Cyber Civil Rights Initiative, « *Revenge Porn Statistics* », consulté le 30 juin 2025, https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf.
44 Tralalère. « *Les cyberviolences : qu'est-ce que c'est ?* » Internet Sans Crainte. https://www.internetsanscrainte.fr/dossiers/cyberharcelement-2/conseils/les-cyberviolences-quest-ce-que-cest Consulté le 11/09/2025.
45 « *Cyberviolences et cyberharcèlement : le vécu des victimes | Ipsos* », 15 décembre 2022, https://www.ipsos.com/fr-fr/cyberviolences-et-cyberharcelement-le-vecu-des-victimes.
46 Etienne Mercier et al., « *CYBERVIOLENCE ET CYBERHARCÈLEMENT : ETAT DES LIEUX D'UN PHÉNOMÈNE RÉPANDU* », Enquête Ipsos 2022.

entreprises, de l'État et de l'ordre public, tout en intégrant des garanties pour les droits humains, mais sans placer ces droits au cœur de la conception de ses politiques de cybersécurité. La cybersécurité reste ainsi largement pensée comme une question de sécurité nationale, de défense et de lutte contre la criminalité.

Cette approche n'est pas suffisante pour bâtir des politiques de cybersécurité qui prennent suffisamment en compte les victimes, selon les partisans de l'approche dite "humano-centrée" de la cybersécurité[47] ; en effet, elle tend à occulter les dimensions de genre et notamment le fait que, bien souvent, pour les femmes et pour les victimes d'attaques à caractère sexuel, la violence en ligne est souvent en continuité avec la violence hors ligne. En mettant les droits humains au coeur des politiques de cybersécurité, cette approche permettrait ainsi d'adopter une réponse différenciée selon le genre des victimes - par exemple, une prise en charge psychologique spécialisée pour les femmes victimes de pornodivulgation, compte tenu des conséquences souvent plus dévastatrices qu'elles subissent mais aussi en tenant compte du profil des cybercriminels, qui sont majoritairement des hommes.

Par Joséphine BOURRINET

47 Julia-Silvana Hofstetter, Panthea Pourmalek, Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity, 2023. http://gnwp.org/gender-cybersecurity-through-women-peace-security, p.12

USAGES NUMÉRIQUES ET PROTECTION DES PUBLICS

03

- Télétravail et cybersécurité : Comment protéger son quotidien numérique ?
- L’Intelligence Artificielle à l’École : Opportunités et Défis
- L’enfance en ligne : une cible facile dans un monde numérique à risque

TÉLÉTRAVAIL ET CYBERSÉCURITÉ :

Comment protéger son quotidien numérique ?

Une transformation accélérée… mais à risque

Depuis 2020, le télétravail s'est imposé comme un mode d'organisation incontournable, largement amplifié par la pandémie de COVID-19. Si cette pratique offre flexibilité et continuité des activités, elle expose également les entreprises et les salariés à des cybermenaces accrues. D'après une étude du site Infogene, près de 20 % des organisations ont subi une cyberattaque due au télétravail pendant la pandémie, souvent via des rançongiciels, avec des conséquences pouvant aller jusqu'à l'arrêt de l'activité. [48]

Travailler depuis chez soi signifie en effet quitter l'environnement sécurisé du réseau de l'entreprise pour se connecter via un réseau domestique, souvent moins protégé. Cela multiplie les opportunités pour les cybercriminels. Selon Cybermalveillance.gouv.fr, la généralisation du télétravail nécessite « l'ouverture vers l'extérieur du système d'information », ce qui constitue un risque majeur en cas de rançongiciel ou de vol de données.[49]

Des exemples concrets l'illustrent. Aux États-Unis, le géant Target a été victime d'un vol massif de données bancaires de clients après qu'un prestataire a compromis l'accès à son réseau, entraînant des millions de dollars de pertes et le départ de son PDG[50]. En France, plusieurs hôpitaux ont dû reporter des opérations à cause de rançongiciels bloquant totalement leurs systèmes médicaux[51], tandis que le logiciel Zoom, massivement adopté pour la visioconférence, a vu ses lacunes en chiffrement exposées au grand jour au début de la pandémie.[52]

Des cybermenaces opportunistes et ciblées

Les campagnes d'hameçonnage et particulièrement celles ciblées ont explosé depuis 2020, exploitant la peur du coronavirus pour inciter les télétravailleurs à cliquer sur des liens malveillants. Le cabinet d'avocat Pinsent Masons relève que 39 % des cyberattaques entraînent des perturbations prolongées de l'activité, et 19 % des pertes directes de données ou d'argent.[53]

Les cybercriminels adaptent aussi leurs techniques aux nouveaux outils de collaboration à distance. Zoom, par exemple, a été pointé du doigt pour des failles de sécurité, permettant parfois une prise de contrôle du micro ou de la webcam. Les attaques via le protocole RDP[54] (Remote Desktop Protocol) ou l'exploitation de VPN[55] mal configurés sont également fréquentes.[56]

Protéger l'entreprise : les bonnes pratiques incontournables

Face à cette évolution des risques, les recommandations des experts convergent. Cybermalveillance.gouv.fr insiste sur la nécessité pour les entreprises de fournir des équipements professionnels sécurisés plutôt que de laisser les salariés utiliser leur matériel personnel, difficile à contrôler. Il s'agit aussi de limiter et filtrer les accès distants, en cloisonnant les systèmes sensibles et en utilisant des pares-feux adaptés, tout en imposant un VPN avec authentification forte pour restreindre les accès aux seuls équipements autorisés. La gestion des mots de passe demeure cruciale : ils doivent rester longs, complexes et uniques, accompagnés d'une double authentification quand c'est possible. À cela s'ajoute l'importance de déployer sans attendre les mises à jour pour corriger les failles, de sauvegarder régulièrement les données sur des solutions indépendantes pour contrer les rançongiciels, ou encore d'installer des antivirus professionnels différenciés selon qu'il s'agit de l'infrastructure ou des terminaux. Enfin, la supervision des activités réseau permet de détecter rapidement toute anomalie, tandis que la sensibilisation des collaborateurs et un soutien technique réactif restent le socle de la sécurité numérique.[57]

48 Infogene, « *Cybersécurité et télétravail : quelles sont les bonnes pratiques ?* » : https://www.infogene.fr/publications/cybersecurite-teletravail
49 Cybermalveillance.gouv.fr, « *La sécurisation du télétravail* » : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securisation-du-teletravail
50 New York Times, « *Target C.E.O. Resigns After Data Breach* », 2014
51 Le Monde, « *Rançongiciels : les hôpitaux français en première ligne* », 2021
52 *The Verge, « Zoom says it will offer end-to-end encryption to all users* », juin 2020
53 Pinsent Masons, « *Cybersécurité et télétravail : difficile cohabitation* » : https://www.pinsentmasons.com/fr-fr/out-law/analyses/cybersecurite-et-teletravail
54 RDP (Remote Desktop Protocol) : protocole développé par Microsoft permettant de prendre le contrôle d'un ordinateur à distance via une interface graphique. Il facilite le télétravail mais, mal configuré, il peut devenir une porte d'entrée privilégiée pour les cyberattaques.
55 VPN (Virtual Private Network) : un réseau privé virtuel est un tunnel sécurisé entre l'ordinateur de l'utilisateur et le réseau de l'entreprise. Il chiffre les données qui transitent, empêche les interceptions sur des réseaux publics et permet d'accéder aux ressources internes comme si l'on était physiquement dans les locaux.
56 CNIL, « Quels outils pour les visioconférences ? », avril 2020
57 Cybermalveillance.gouv.fr, « *La sécurisation du télétravail* » : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securisation-du-teletravail

Infogene une ESN experte en transformation digitale, va plus loin en conseillant de « *profiler les télétravailleurs* », c'est-à-dire d'adapter précisément les droits d'accès aux besoins effectifs de chaque poste, afin de limiter l'exposition inutile des données sensibles et réduire d'autant la surface d'attaque.[58]

Au-delà des mesures techniques, l'entreprise a également un rôle déterminant dans la mise en place d'une véritable culture de cybersécurité. Elle doit définir une politique claire encadrant le télétravail (chartes d'utilisation, règles d'accès aux données, plan de réponse aux incidents) et veiller à ce que chaque collaborateur en ait connaissance. La responsabilité ne peut pas reposer uniquement sur les salariés : c'est à l'organisation de fournir un cadre, des outils adaptés et un accompagnement constant.

Télétravailleurs : des réflexes simples mais essentiels

La cybersécurité au quotidien n'est pas qu'une affaire de direction informatique. Les salariés en télétravail doivent eux aussi adopter des pratiques rigoureuses pour éviter que leur domicile ne devienne la porte d'entrée des cybercriminels. Cela passe par la sécurisation de leur box internet et du WiFi, en changeant les mots de passe par défaut et en utilisant le mode de protection le plus récent proposé dans les réglages de la box (chiffrement WPA2 ou WPA3), ainsi que par une stricte séparation entre usages professionnels et personnels pour éviter toute contamination croisée. Utiliser systématiquement le VPN fourni par l'entreprise et éviter de se connecter sur des WiFi publics non sécurisés réduit considérablement les risques. Il est tout aussi essentiel de mettre à jour antivirus et systèmes pour corriger les failles exploitées par les attaquants, et de sauvegarder régulièrement son travail sur des supports validés par l'entreprise.

Rester vigilant face aux e-mails suspects demeure une règle de base, surtout lorsque le message cherche à créer un sentiment d'urgence pour pousser à cliquer trop vite. Enfin, protéger son écran et verrouiller la session à chaque absence évite que des informations confidentielles ne soient exposées, même dans le cadre familial. Comme le rappelle Agiris, la cybersécurité reste fragile quand « *62 % des salariés utilisent leur ordinateur professionnel à des fins personnelles et 42 % ne mettent pas à jour régulièrement leurs systèmes de sécurité* », laissant la porte ouverte à des incidents pourtant évitables.

Une vigilance qui s'inscrit dans la durée

Les données du rapport scientifique publié sur arXiv, une archive ouverte de pré-publications et de post-publications, montrent que le passage massif au télétravail pendant la pandémie a doublé le nombre de violations de données observées dans l'étude (de 242 000 à plus de 400 000 personnes affectées). Si la durée des attaques a diminué, traduisant une meilleure détection, le délai de notification s'est allongé, preuve que l'adaptation complète à ce nouveau contexte prend encore du temps.

Le télétravail continuera d'être une modalité forte du monde professionnel. C'est pourquoi il est crucial que chaque acteur - entreprise, manager, collaborateur - fasse de la cybersécurité une routine du quotidien. Les organisations doivent donner les moyens, les salariés doivent appliquer les bonnes pratiques, et les managers doivent créer un climat de confiance et de vigilance partagée.

Par Leina SI LAKHAL

58 Infogene, « *Cybersécurité et télétravail : quelles sont les bonnes pratiques ?* » : https://www.infogene.fr/publications/cybersecurite-teletravail

L'INTELLIGENCE ARTIFICIELLE À L'ÉCOLE :

Opportunités et Défis

L'Intelligence Artificielle (IA) a connu une démocratisation fulgurante ces cinq dernières années. Selon l'étude Born AI menée par l'agence Heaven en 2025, 93 % des jeunes âgés de 14 à 24 ans déclarent avoir utilisé l'IA au cours des six derniers mois.[59]

Cette adoption massive s'explique par sa facilité d'accès et l'émergence de modèles toujours plus performants. Les entreprises comme les particuliers l'utilisent désormais pour des tâches variées : recherche d'informations, prise de notes, planification, et bien d'autres. L'IA s'impose ainsi comme un outil polyvalent, optimisant la productivité au quotidien.

59 L'utilisation des IA génératives déjà intégrée aux habitudes quotidiennes des jeunes - Stratégies, https://www.strategies.fr/actualites/culture-tech/LQ4753088C/lutilisation-des-ia-generatives-deja-integree-aux-habitudes-quotidiennes-des-jeunes.html , 13 juin 2025

Quid de l'utilisation de l'Intelligence Artificielle chez les plus jeunes en milieu scolaire ?

L'intelligence artificielle s'impose progressivement dans le milieu scolaire, où son usage par les jeunes s'effectue souvent en dehors des recommandations pédagogiques, posant ainsi des défis majeurs. D'une part, cette utilisation non encadrée peut conduire à des productions biaisées ou erronées en raison des limites algorithmiques.[60] D'autre part, la méconnaissance des enjeux liés à ces technologies, tant chez les apprenants que chez certains enseignants, accentue les risques d'un emploi inapproprié.

Pour autant, l'État français qui a accueilli en février dernier le sommet de l'IA, semble désormais encourager l'intégration progressive de ces technologies dans la société française, aussi bien dans les services publics[61], que dans le système éducatif[62]. Pour cela, Elisabeth Borne alors ministre de l'Éducation, a entre autres annoncé la mise en place d'une charte permettant d'encadrer l'usage de l'IA à l'école[63], la mise en place d'un assistant pédagogique pour les professeurs ou encore d'outils de soutien scolaire pour les élèves comme l'application de soutien scolaire MIA déployée depuis septembre 2024 pour les élèves de seconde.

Bien que ces décisions soient ambitieuses, il semblerait qu'il n'y ait pas de consensus sur la mise en place d'un tel dispositif à l'heure où la France tend à se projeter comme leader européen dans les technologies d'intelligence artificielle.

L'IA à l'école : bienfaits ou inconvénients ?

En France, seulement 35 % des enseignants estiment que les outils d'IA sont bénéfiques pour les élèves[64]. D'un côté, l'IA offre des opportunités notables, notamment en matière de personnalisation de l'apprentissage. Elle offre des outils adaptatifs qui ajustent les contenus pédagogiques au niveau et au rythme de chaque élève, favorisant ainsi une meilleure assimilation des connaissances avec des outils tels que **Smart enseigno** pour les mathématiques ou encore **Lalilo**[65] pour le français. Parallèlement, l'État, via le Réseau Canopé[66], a mis en place des dispositifs innovants pour accompagner les enseignants dans l'élaboration de contenus pédagogiques adaptés à des objectifs spécifiques libérant ainsi du temps aux enseignants pour se concentrer sur d'autres tâches.

Certains soutiennent également que l'IA contribue à une accessibilité renforcée de l'éducation, en proposant des ressources numériques aux élèves situés dans des zones isolées et en offrant un soutien adapté aux apprenants en difficulté un petit peu à la manière du CNED qui permet l'éducation à distance.

Le cas de l'Unbound Academy - Pheonix - Arizona :

Pour autant, certains observateurs expriment leur réticence, en partie par la crainte d'une automatisation progressive de l'enseignement, comparable à la disparition des caissiers au profit des caisses automatiques. Cette évolution, qui réduit les interactions humaines, est déjà en marche aux États-Unis avec des projets comme L'Unbound Academy, où l'IA commence à remplacer partiellement le système éducatif traditionnel.[67]

Alors que les élèves sont en pleine constructions cognitive le chercheur Umberto Domínguez de l'université de Monterrey révélait dans une étude publiée en 2024[68] qu'une dépendance excessive aux technologies d'IA peut entraîner une diminution des capacités cognitives, en réduisant nos aptitudes à la réflexion critique et à la résolution autonome de problèmes. De plus, des projets comme l'Unbound Academy pourraient limiter les interactions humaines essentielles au développement des compétences sociales, en réduisant les échanges entre élèves et enseignants. Cette situation rappelle les défis rencontrés lors de la pandémie de Covid-19, où la diminution des interactions sociales a conduit à des cas de décrochage scolaire.[69]

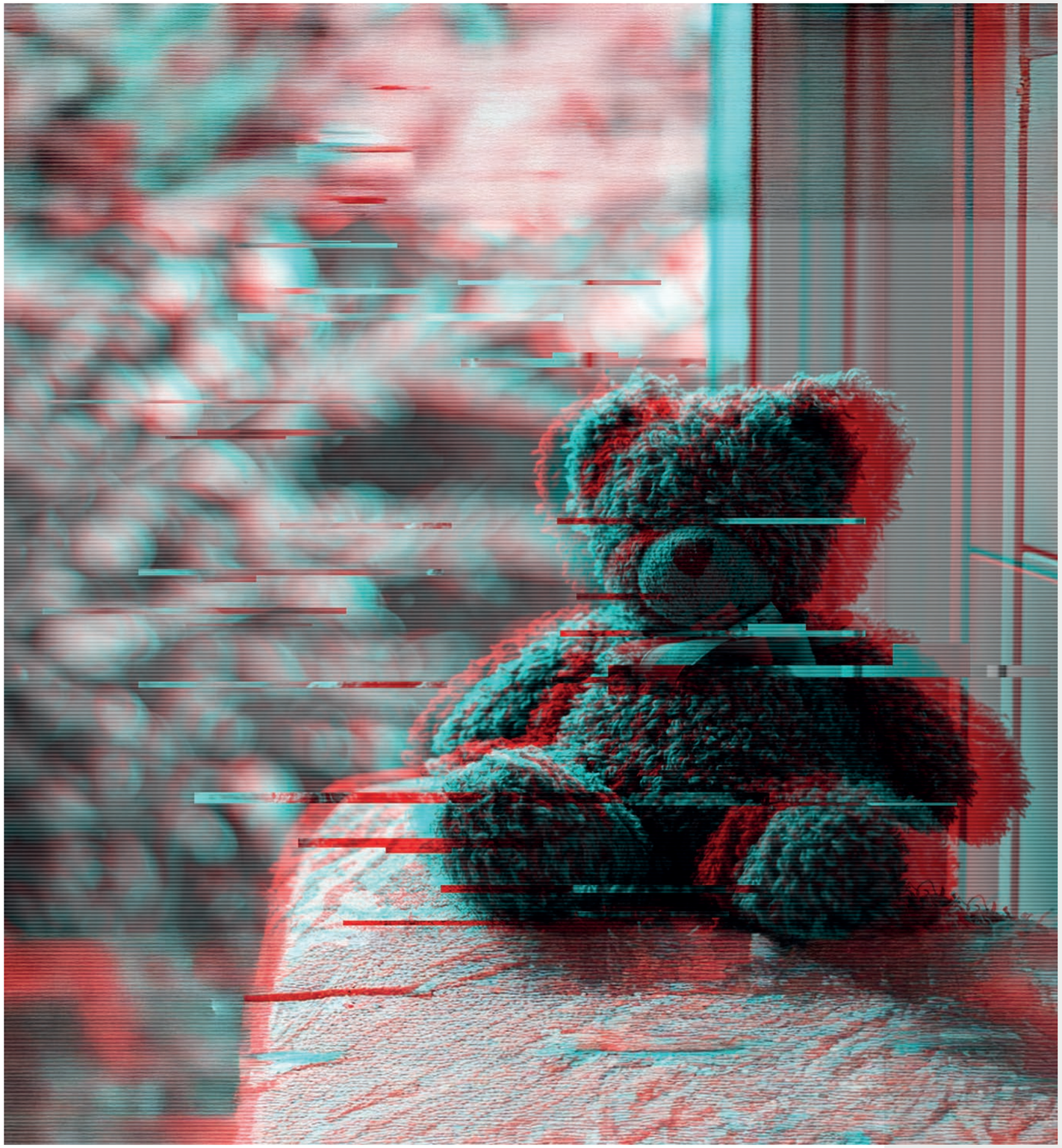
Finalement, les arguments en faveur ou en opposition à l'intégration de l'IA dans le milieu scolaire sont tous légitimes. D'une part, l'IA peut offrir des solutions aux élèves des zones isolées en facilitant l'accès à des ressources éducatives, d'autre part, l'accès inégal aux technologies avancées risque d'accentuer les disparités existantes entre les élèves issus de milieux favorisés et défavorisés.

Par ailleurs, L'État est conscient des défis liés à l'intégration de l'IA dans le système éducatif et appelle à une vigilance accrue, en l'absence de solutions définitives. Parmi ces défis, l'on retrouve les biais algorithmiques qui peuvent perpétuer des stéréotypes ou privilégier certains types d'apprentissage, compromettant ainsi la neutralité éducative. Actuellement, aucune certification n'est établie pour garantir des IA fiables et éthiques dans le domaine de l'éducation.

En outre, la collecte massive de données sur les élèves soulève des questions éthiques significatives concernant la confidentialité et l'utilisation de ces informations. L'absence de transparence quant à la manière dont ces données sont collectées, stockées et utilisées peut entraîner des violations de la vie privée et une exploitation inappropriée des informations personnelles. Malgré une protection approximative via le Règlement Général de Protection des Données (RGPD), aucune solution pérenne n'est à ce jour trouvée.

Par Iris HOURCADE

60 *Intelligence artificielle, de quoi parle-t-on ?*, https://www.cnil.fr/fr/intelligence-artificielle/intelligence-artificielle-de-quoi-parle-t-on
61 *L'IA au service de l'amélioration continue des services publics | Direction interministérielle de la transformation publique*, https://www.modernisation.gouv.fr/actualites/lia-au-service-de-lamelioration-continue-des-services-publics
62 *La France est-elle prête pour l'IA ?* (Interview Emmanuel Macron), s.l., s.n., 2025.
63 *Dès 2025, les cours d'IA deviennent obligatoires au collège et au lycée | 1 jeune1 solution*, https://www.1jeune1solution.gouv.fr/articles/formation-intelligence-artificielle-ecoles-france-2025
64 « *L'intelligence artificielle à l'école, une révolution déjà en marche* », in , 8 févr. 2025 p.
65 *L'intelligence artificielle pour accompagner les apprentissages des fondamentaux au cycle 2*, https://eduscol.education.fr/1911/l-intelligence-artificielle-pour-accompagner-les-apprentissages-des-fondamentaux-au-cycle-2
66 *L'intelligence artificielle en classe*, https://www.reseau-canope.fr/ia-en-classe , 10 juin 2025, consulté le 21 juillet 2025.
67 *Une école IA Sans Profs Aux Etats-Unis. Voici La Unbound Academy*, https://stewdy.com/actualites/unbound-academy/ , 12 janvier 2025, consulté le 8 juillet 2025
68 *Conséquences néfastes de l'IA : cette technologie pourrait-elle entraîner un déclin de notre intelligence ?* Le chercheur Umberto Domínguez de l'université de Monterrey exprime ses craintes, https://intelligence-artificielle.developpez.com/actu/354219/Consequences-nefastes-de-l-IA-cette-technologie-pourrait-elle-entrainer-un-declin-de-notre-intelligence-Le-chercheur-Umberto-Dominguez-de-l-universite-de-Monterrey-exprime-ses-craintes/ , 14 février 2024
69 *Dispositif d'évaluation des conséquences de la crise sanitaire : comment les élèves ont-ils vécu le confinement de mars-avril 2020 ?*, https://www.education.gouv.fr/dispositif-d-evaluation-des-consequences-de-la-crise-sanitaire-comment-les-eleves-ont-ils-vecu-le-322830



L'ENFANCE EN LIGNE :

Une cible facile dans un monde numérique à risque

Plus d'un enfant sur trois commence à utiliser des écrans numériques entre deux ans et cinq ans.[70] À douze ans, 80 % d'entre eux sont déjà connectés quotidiennement à Internet, et près de 60 % des douze/dix-sept ans utilisent chaque jour les réseaux sociaux[71]. Ces chiffres traduisent une immersion de plus en plus précoce des enfants dans un environnement numérique complexe, sans toujours en comprendre les règles ni les dangers.

70 *"Les enfants de moins de 6 ans et les écrans numériques : à chacun son rythme, d'après l'enquête Elfe"*. INSEE Références, éditions 2022. "France, portrait social". https://www.insee.fr/fr/statistiques/6535295?sommaire=6535307
71 Pôle Société. *"Baromètre du numérique - Rapport"*. Mars 2025. https://labo.societenumerique.gouv.fr/documents/40/Rapport_barom%C3%A8tre_num%C3%A9rique_2025_final_compressed.pdf

Dès leur plus jeune âge, les enfants deviennent des utilisateurs réguliers de tablettes, smartphones, plateformes éducatives ou assistants vocaux, parfois avant même de savoir lire ou écrire. Mais cette familiarité apparente avec les technologies masque une réelle vulnérabilité des enfants face aux risques cognitifs, émotionnels et sociaux. Leur rapport au numérique est majoritairement ludique ou éducatif, mais souvent passif : ils « consomment » des contenus sans recul critique, ce qui les rend sensibles aux tentatives de manipulation, à la désinformation, ou à la collecte abusive de données personnelles. En l'absence d'accompagnement structuré, ils peuvent développer des habitudes à risque sans même en avoir conscience : cliquer sur des liens inconnus, utiliser des mots de passe faibles ou partager des informations personnelles.

Trois points de vulnérabilité numérique chez les enfants

Les dangers numériques pour les enfants se répartissent en trois catégories principales : les risques psychosociaux liés aux interactions, les risques techniques issus des dispositifs, et ceux liés aux modèles économiques fondés sur l'attention et les données.

- D'un point de vue psychosocial, le cyberharcèlement est une menace majeure. Il peut se manifester par des messages blessants ou humiliants sur des groupes de discussion comme Snapchat. Cela provoque détresse psychologique et isolement, d'autant que les enfants n'ont pas toujours les outils émotionnels pour se défendre ou alerter un adulte. Autre danger : le grooming, manipulation en ligne d'un adulte se faisant passer pour un enfant afin de gagner la confiance d'un jeune, souvent à des fins d'abus.[72] Ces approches, discrètes et personnalisées, sont difficiles à détecter, même par les systèmes automatisés.

- Sur le plan technique, de nombreux jouets connectés ou applications destinées aux enfants présentent des failles de sécurité. Certains jouets mal sécurisés, comme les peluches CloudPets, ont permis à des pirates d'accéder à des enregistrements vocaux d'enfants.[73] Beaucoup d'applications éducatives collectent aussi des données sensibles[74] (localisation, comportement, identifiants publicitaires) sans consentement ni chiffrement, parfois en violation des normes comme le RGPD.

- Les enfants sont aussi des cibles faciles pour des arnaques numériques : faux concours, offres gratuites, liens piégés dans des jeux populaires… Une simple incitation à « cliquer pour gagner » peut provoquer l'installation d'un logiciel malveillant ou une fuite de données. Enfin, les interfaces destinées aux enfants exploitent souvent des stratégies de manipulation cognitive, appelées dark patterns. Boutons colorés incitant à l'achat, récompenses intégrées pour prolonger l'usage ou publicités déguisées exploitent la malléabilité cognitive des plus jeunes et les exposent à une forme de manipulation commerciale difficile à repérer, même pour un adulte averti.

Combler les lacunes de la protection numérique

Face à cette diversité de menaces, les outils classiques de cybersécurité (antivirus, contrôles parentaux, filtres web) atteignent vite leurs limites. Ils reposent sur une logique de configuration technique peu accessible aux enfants et aux parents peu familiers du numérique. De plus, les systèmes de signalement intégrés aux réseaux sociaux sont rarement utilisés par les enfants, qui ne les comprennent pas ou n'osent pas s'en servir. Quant aux algorithmes de détection de contenus inappropriés, ils peinent à identifier les formes subtiles de harcèlement ou de manipulation.

Il existe également un écart significatif entre les outils techniques disponibles et leur intégration effective dans les environnements éducatifs : peu d'écoles primaires proposent des ateliers dédiés à la cybersécurité, et les parents ont souvent du mal à mesurer les risques auxquels leurs enfants sont vraiment exposés.

Pour répondre à ces défis, plusieurs solutions émergent. D'abord, sur le plan technique, certains outils sont spécifiquement conçus pour un jeune public : navigateurs filtrés (comme Qwant Junior), applications qui proposent une authentification via QR code pour relier comptes enfants et parents, ou encore logiciels utilisant l'intelligence artificielle pour détecter des comportements suspects ou des contenus inappropriés.

Mais la technique ne peut pas tout. L'un des leviers les plus puissants reste l'éducation. De plus en plus d'initiatives misent sur des jeux sérieux ou des applications ludo-éducatives pour initier les enfants à la sécurité numérique. Google propose par exemple « Interland », un jeu pour enseigner les bonnes pratiques. De même, des ateliers ludiques comme « La fresque des cybercitoyens », animés par des intervenants, constituent un bon moyen d'enseigner les bonnes pratiques en matière de cybersécurité.

Enfin, établir des règles claires en famille autour du numérique est essentiel. Il s'agit de décider ensemble ce qui peut être partagé ou non, de comprendre les paramètres de confidentialité et d'apprendre à repérer les pièges en ligne. En adoptant ces habitudes dès le plus jeune âge, on aide les enfants à être plus attentifs en ligne et à développer un vrai sens critique face aux risques liés au numérique.

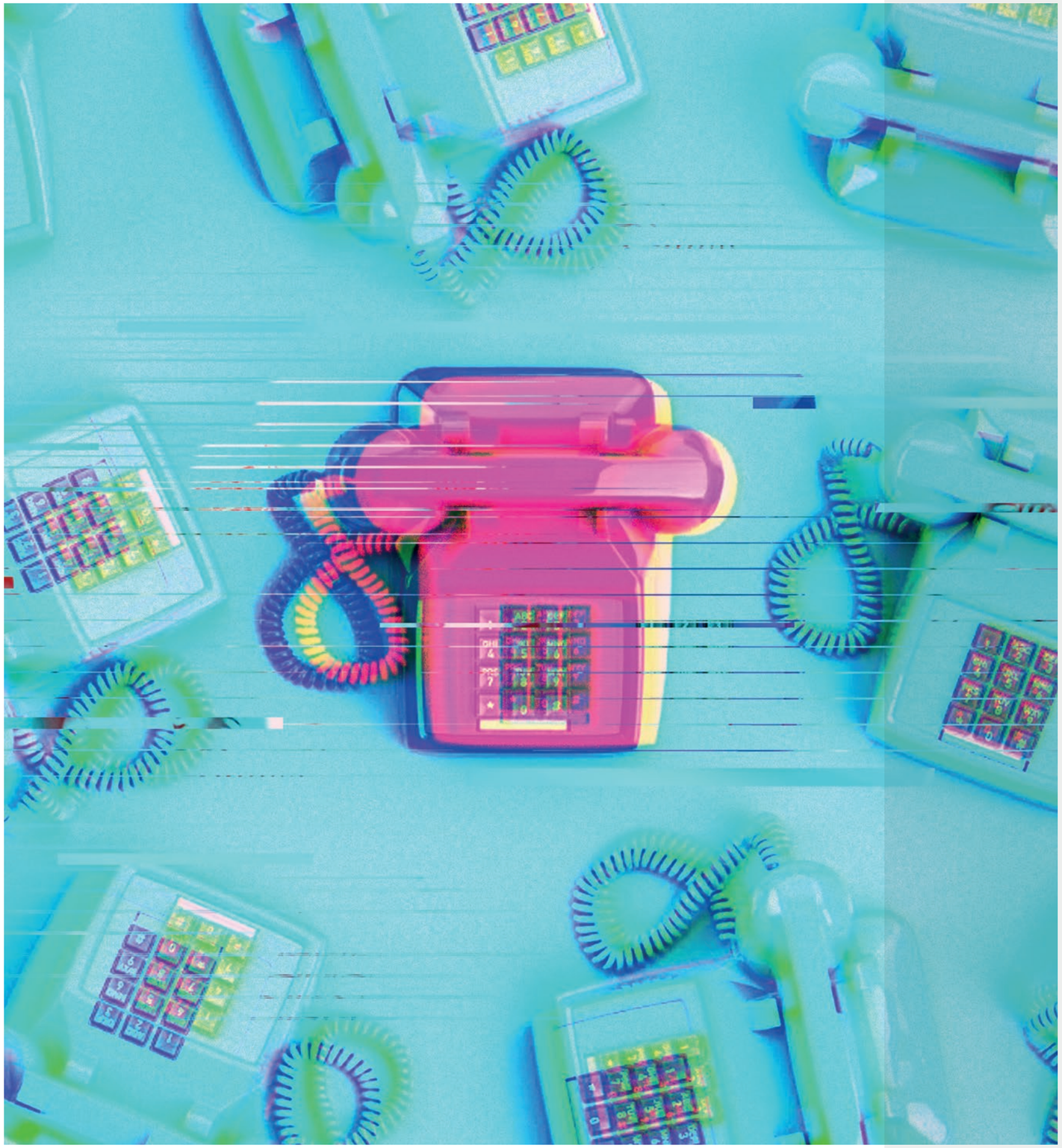
Par Solène LEMMONIER

72 Nellie Bowles, Michael H. Keller. "*Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*". 7 décembre 2019. The New York Times. https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html
73 Futura Sciences. "*Jouets connectés : les peluches Cloudpets sont piratables*". mars 2017. https://www.futura-sciences.com/tech/actualites/securite-jouets-connectes-peluches-cloudpets-sont-piratables-66497/
74 Human Rights Watch. "*Governments Harm Children's Rights in Online Learning*". 2022. https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning

04

INFRASTRUCTURES, VECTEURS ET TECHNIQUES D’ATTAQUE

- Smartphones : quand observer suffit à hacker – Les dessous des attaques physiques passives par canaux auxiliaires (SCA)
- Les réseaux sociaux: failles inattendues des services de sécurité
- Les QR codes piégés : un risque sous-estiméfacile dans un monde numérique à risque



SMARTPHONES :

Quand observer suffit à hacker – Les dessous des attaques physiques passives par canaux auxiliaires (SCA)

Les smartphones modernes sont de véritables coffres-forts numériques. Ils contiennent nos photos, nos mails, nos applications bancaires, et nos identifiants gouvernementaux. Pour protéger ces données sensibles, les constructeurs s'appuient sur de puissants mécanismes cryptographiques (aussi dit algorithmes) permettant que les données ne transitent pas en clair mais soient chiffrées[75]. La sécurité du chiffrement repose sur une clé de chiffrement devant impérativement rester secrète.[76]

75 (2020) *"Guide des mécanismes cryptographique."* (p. 7) ANSSI.
76 (2021) *"Guide de sélection d'algorithmes cryptographiques"* (p. 8) ANSSI.

Mais que se passe-t-il si un attaquant ne cherche pas à casser la cryptographie mais simplement à observer comment elle fonctionne afin d'en déduire la clé secrète ?

C'est là qu'entrent en jeu les attaques physiques passives, et plus précisément les attaques par canaux auxiliaires, aussi appelées Side-Channel Attacks (SCA). Ces attaques ne remettent pas en cause la sécurité mathématique mais elles utilisent des données physiques (temps de calcul, température, courant consommé) pour retrouver la clé secrète. On distingue les attaques actives des attaques passives. Les premières consistent à modifier le système attaqué. Ces attaques sont en général irréversibles et utilisent des découpages chimiques ou des lasers. Les attaques passives utilisent des mesures de paramètres physiques (temps, température, consommation de puissance, rayonnement) appelés canaux auxiliaires, pour en déduire des informations sur les données secrètes.[77]

Le graphe de mesures de consommation de courant ou de rayonnement d'un appareil exécutant un algorithme en fonction du temps est appelé "la trace"[78]. Voici quelques exemples de traces, le but n'est pas d'expliquer comment obtenir la clé à partir de ces graphiques mais de montrer des aperçus de traces desquelles il est possible d'extraire les clés d'algorithmes de chiffrement La Figure 1[79] correspond à une clé de chiffrement RSA. L'algorithme de chiffrement RSA est encore utilisé pour l'authentification en ligne mais la taille de la clé a augmenté au fil des années pour garantir la sécurité[80]. La Figure 2[81] correspond à une figure DES. Cet algorithme n'a plus de cas pratiques d'utilisation à notre époque.

Figure 1

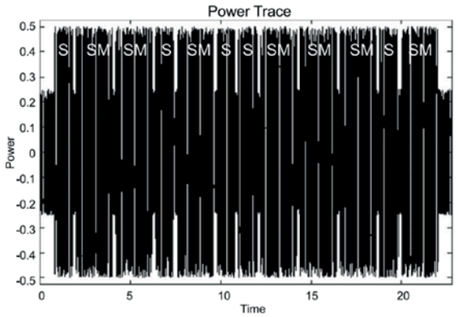
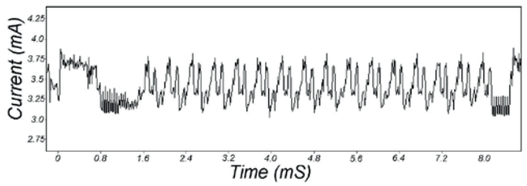


Figure 2



77 Mélissa Rossi Dabi (2016) "Cryptanalyse par canaux auxiliaires : attaques et contre-mesures." (p. 3) Thales / Telecom Paris Tech, Projet de fin d'études.
78 Mélissa Rossi Dabi (2016) "*Cryptanalyse par canaux auxiliaires : attaques et contre-mesures.*" (p. 3) Thales / Telecom Paris Tech, Projet de fin d'études.
79 Julien FRANCQ (2023). "*Basics in Side-Channel Analysis.*" (p. 46) Naval Group / Naval Cyber Laboratory.
80 (2024) "*Note clarification utilisation RSA 2048 bits PSCo qualifies.*" ANSSI.
81 Julien FRANCQ (2023). "*Basics in Side-Channel Analysis.*" (p. 81) Naval Group / Naval Cyber Laboratory.

Quels cas concrets ?

En 2018, l'équipe Project Zero de Google a découvert deux vulnérabilités liées à l'accès indirect à des données sensibles affectant la plupart des PC et des smartphones de l'époque. Ces vulnérabilités, Spectre et Meltdown, dans les circuits intégrés des processeurs Intel, AMD, Apple et ARM, exploitent l'exécution spéculative, une technique où les processeurs devinent et exécutent du code à l'avance afin d'améliorer les performances... Ces failles permettent aux attaquants d'accéder à des données sensibles (mots de passe, clés de chiffrement) stockées dans la mémoire du noyau[82]. Les attaques Spectre consistent à inciter une victime à effectuer de manière spéculative des opérations qui ne se produisent pas lors de l'exécution correcte d'un programme. Le but est de divulguer à l'attaquant ses informations confidentielles via un canal auxiliaire[83]. Les attaquants mesurent alors via un canal auxiliaire les propriétés micro architecturales du système (la synchronisation du cache[84], l'historique de prédiction de branchement[85], les tampons cibles de branchement[86], ou les lignes DRAM ouvertes[87] [56]) pour récupérer les données (mots de passe, clés de chiffrement) tout juste divulguées par le programme piraté.[88]

Comment les attaques passives par canaux auxiliaires s'invitent dans notre quotidien ?

En 2021, l'équipe de sécurité de Google sur l'exploitabilité de Spectre contre les utilisateurs web a partagé ses résultats d'un Proof Of Concept[89] rapide et polyvalent écrit en JavaScript capable de divulguer des informations depuis la mémoire des navigateurs web. Chrome a été utilisé pour démontrer l'attaque mais les failles ne sont pas spécifiques à Chrome, d'autres navigateurs web sont donc vulnérables.[90]

Plus récemment, en janvier 2025, trois chercheurs de Georgia Tech et un chercheur de l'Université Ruhr-Bochum ont dévoilé en janvier deux nouvelles vulnérabilités sur les processeurs Apple (A15/A17, M-series). Nommées SLAP (Speculative Load Address Prediction) et FLOP (False Load Output Prediction), elles concernent respectivement le prédicteur d'adresse de chargement[91] et le prédicteur de valeur de chargement[92]. Il s'agit de deux types de systèmes d'exécution spéculative qui prédisent l'adresse RAM à laquelle un programme en cours d'exécution aura probablement accès.

Pour SLAP, les chercheurs ont démontré comment le prédicteur d'adresse de chargement pouvait être utilisé pour lire des données restreintes. Pour FLOP, aucune donnée n'a été lue, cependant la prédiction précise du système quant à ce qui serait lu pourrait exposer des informations sensibles. Les chercheurs ont démontré comment SLAP et FLOP peuvent être utilisés pour contourner plusieurs couches de sécurité à la fois dans le CPU et dans le navigateur Safari pour accéder à des données sensibles. Les constructeurs de processeurs ont bien pris connaissance des vulnérabilités identifiées afin de les corriger. Par ailleurs, les failles de sécurité permettant de contourner le système de sécurité d'un iPhone et d'accéder aux données privées de son propriétaire atteignent des prix exorbitants sur le marché noir. Il est donc raisonnable de supposer qu'une vulnérabilité matérielle, qui restera probablement partiellement non corrigée (de par les corrections qui diminuent les performances des processeurs), serait exploitée lors d'attaques ciblées visant des données particulièrement précieuses.[93]

82 Noyau : programme qui se trouve au cœur du système d'exploitation d'un ordinateur. "*Qu'est-ce que Meltdown/Spectre ?*" Cloudflare. "*Qu'est-ce que Meltdown/Spectre ?*" Cloudflare
83 P. Kocker, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom (2019) "*Spectre Attacks: Exploiting Speculative Execution.*" (p. 1) IEEE.
84 D. J. Bernstein (2005) "*Cache-Timing Attacks on AES.*" University of Illinois à Chicago
85 O. Aciiçmez, J.-P. Seifert, and C. K. Koç (2006) "*Predicting Secret Keys via Branch Prediction.*
86 S. Lee, M.-W. Shih, P. Gera, T. Kim, H. Kim, M. Peinado (2017) "*Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing.*" USENIX / Georgia Tech / Microsoft Research.
87 P. Pessl, D. Gruss, C. Maurice, M. Schwarz, S. Mangard (2016) "*DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks.*" USENIX / Graz University of Technology.
88 (2018) "*Speculative Execution Side Channel Mitigations.*" (p. 5) Intel.
89 Le POC est l'un des moyens les plus efficace et rapide de valider votre concept avant de lancer votre projet d'application
90 S. Röttger, A. Janc (2021) "*A Spectre proof-of-concept for a Spectre-proof web.*" Google.
91 Prédicteur d'adresse de chargement : Load Address Predictor (LAP). J. Kim, D. Genkin, Y. Yarom (2025) "*SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon.*" (p. 1) Georgia Tech / Ruhr University Bochum.
92 Prédicteur de valeur de chargement : Load Output Predictor (LOP) . J. Kim, J. Chuang, D. Genkin, Y. Yarom (2025) "*FLOP: Breaking the Apple M3 CPU via False Load Output Predictions.*" (p. 1) Georgia Tech / Ruhr University Bochum.
93 E. Root (2025) "SLAP and FLOP: Complex vulnerabilities in Apple CPUs." Kaspersky.

Que faire contre ses attaques ?

Il est indispensable d'appliquer aussitôt que disponible l'ensemble des mises à jour proposées par les éditeurs et les constructeurs, en tout premier lieux les navigateurs et les systèmes d'exploitation (Windows, Macos, iOS, Android).[94]

Les attaques passives par canaux auxiliaires montrent que la sécurité des smartphones ne repose pas uniquement sur la robustesse des algorithmes cryptographiques, mais aussi sur la sécurité physique et matérielle des composants. En exploitant des fuites d'informations comme la consommation d'énergie ou l'exécution spéculative, les attaquants peuvent accéder à des données sensibles sans même casser le chiffrement. Les failles comme Spectre, Meltdown, SLAP et FLOP illustrent la persistance de ces menaces, même sur les technologies les plus récentes.

Pour s'en prémunir, il est crucial de maintenir ses appareils à jour. Cependant ce n'est pas une condition suffisante étant donné que certaines vulnérabilités peuvent rester partiellement corrigées, auquel cas l'utilisateur ne peut agir.

Par Hanaé LOPEZ

94 (2018) "Alerte : multiples vulnérabilités dans des processeurs - Comprendre Meltdown et Spectre et leur impact." ANSSI.

LES RÉSEAUX SOCIAUX :

Failles inattendues des services de sécurité

À l'ère de la twiplomacy[95], ou encore du global village[96], les réseaux sociaux sont le champ de bataille de relations de forces. Désormais dans un contexte inévitable de culture de la transparence, ces réseaux sociaux rendent la frontière entre vie privée et vie publique extrêmement poreuse. Ces applications de partage et l'usage que tout un chacun en fait doit être interrogé. Toute donnée échangée sur ces applications du quotidien, aussi banale et insignifiante puisse-t-elle sembler, peut se transformer en information sensible et se muter en véritables enjeux de défense une fois agglomérées et agrégées. Et ce, d'autant plus lorsque les utilisateurs sont de près ou de loin reliés aux institutions diplomatiques et militaires.

95 Expression popularisée par l'agence de communication Burson-Marsteller visant l'usage devenu quasi systématique des réseaux sociaux, notamment Twitter par tous les représentants d'Etats afin d'influencer la sphère diplomatique.
96 Expression popularisée par Marshall McLuhan tiré de son ouvrage The Medium is the Massage (1967), visant l'interconnection de la société exacerbée par l'avènement des nouvelles technologies.

S'étant rapidement emparé des enjeux relatifs à l'usage des réseaux sociaux, le ministère des Armées s'est appuyé sur des études afin de qualifier et quantifier les motifs d'utilisation des réseaux sociaux par ses agents[97]. Ceci a permis de dresser une liste des différents besoins en communication des utilisateurs, organisée sous forme de pyramide inspirée par les travaux de Maslow. Cette hiérarchisation des motifs d'usage des réseaux sociaux se présente en quatre niveaux.

Au socle de cette pyramide se trouvent les recherches d'informations les plus communément partagées et largement diffusées. Cette recherche d'information se fait notamment au travers des forums et consultations de moteurs de recherche. La seconde strate vise quant à elle la "fabrication du lien social" via le partage d'information. L'étude traite ici des récits du quotidien des agents faits pour ou par les proches au travers des publications sur les réseaux sociaux par exemples de soutien à l'égard des militaires partis en Opération exterieure. Le troisième niveau correspond quant à lui aux "actions de revendication" ou "mobilisation". Il s'agit à titre d'exemple de participation au relais de publication de soutien aux militaires. Enfin, la dernière catégorie vise "l'aspiration créatrice". Cette dernière se multiplie aujourd'hui au travers des comptes sur les réseaux sociaux de "miltok", des militaires, anciens engagés ou compagnes de soldats créant du contenu relatif à leur quotidien. Si certains de ces influenceurs participent à la politique de communication des forces armées, d'autres électrons libres peuvent parfois laisser circuler des informations méritant à être plus discrètes. Aussi, pour chacune de ces strates, les informations circulant sur les réseaux sociaux, même de façon privée peuvent revêtir des implications de sécurité et défense et doivent faire l'objet d'une attention très particulière.

Les risques pour la protection des enjeux de défense de l'usage d'applications du quotidien tels que les réseaux sociaux se sont d'ores et déjà illustrés de multiples manières.

Il peut s'agir dans un premier temps de l'utilisation de réseaux qui par manque de précaution attribuée au partage d'information a pu dans le passé fuité des informations délicates pour les institutions publiques. Les cas les plus connus sont très certainement les affaires américaines en raison de leur ampleur et des données extrêmement sensibles ayant fuitées. À titre d'exemple, STRAVA, une application sportive utilisée par du personnel militaire a permis de localiser leurs activités professionnelles en s'appuyant sur le parcours de leurs courses Ainsi, des positions de bases militaires américaines jusqu'alors secrètes ont été découvertes au travers de cette application en Syrie, Irak et Afghanistan. De plus ces informations, même lorsqu'elles sont d'apparence indifférentes car visant des bases militaires connues, peuvent révéler des informations intéressantes telles que le mode de vie et ainsi deviner les habitudes et l'emploi du temps des militaires.

Dans un second temps, il est envisageable que d'autres informations, bien plus sensibles et qui ne devraient en aucun cas circuler sur les réseaux sociaux, pourraient néanmoins s'y retrouver. Les États-Unis en ont récemment fait les frais, comme l'illustre l'affaire liée à l'application Signal. Un journaliste américain a en effet révélé avoir été ajouté par erreur à une boucle de discussion chiffrée sur Signal, où le vice-président JD Vance échangeait avec de hauts responsables militaires au sujet de frappes imminentes contre les Houthis au Yémen.

Afin de limiter ces risques, le Ministère des Armées a élaboré un "Guide du bon usage des réseaux sociaux" à destination des militaires et civils du Ministère ainsi que de leur entourage. Y sont présentées les erreurs à ne pas commettre, les bonnes pratiques ainsi que les risques et dangers. Il y est notamment rappelé que le personnel tant civil que militaire du Ministère doit faire preuve de discrétion pour tous les faits et informations dont il aurait connaissance dans l'exercice de ses fonctions, en vertu respectivement des articles 26 de la loi portant droits et obligations des fonctionnaires[98] et L. 4121-2 du code de la défense. Plus précisément pour les militaires, si le principe reste la liberté d'expression et d'utilisation des réseaux sociaux, le droit prévoit que l'usage des moyens de communication et d'information, quels qu'ils soient, puissent être restreints ou interdits pour assurer la protection des militaires en opération et la sécurité des activités militaires.

Il s'agit là de la troisième édition du guide des bonnes pratiques. Celle-ci datant d'octobre 2021 mériterait certainement à être complétée afin de prendre en considération les nouvelles pratiques sur les réseaux sociaux, en premier lieu desquels l'évolution de l'intelligence artificielle. En effet, le guide met en garde contre les fakes news, celles-ci pouvant potentiellement altérer le devoir de réserve et de discrétion des agents ; enjeu bien réel comme en témoigne la campagne de désinformation sur les réseaux sociaux mettant en scène de faux témoignages de soldats français en Ukraine. Cependant, le document ne mentionne pas

97 M. Hecker, N. Vanbremeersch, M. de Durand et T. Souchet, "Nature et conséquence des réseaux sociaux pour les forces armées", Etude finale réalisée au profit du Centre Interarmées De Concepts, de Doctrines et d'Expérimentations (CICDE), de la Délégation à l'Information et à la communication de la Défense (DICOD) et de la DAS, septembre 2012.
98 Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

les deepfakes ou autres imageries génératives. C'est pourtant un nouveau danger pris en considération par les cybercombattants, ces derniers s'exerçant à détecter les fausses informations circulant par ce prisme. À ce titre, lors du Salon international Eurosatory 2024, le COMCYBER a présenté un outil de détection de ces hyper trucages. Aussi, le Ministère des Armées, gagnerait en fiabilité de l'usage de l'ensemble de ces agents en ajoutant la mention de ce nouveau défi auquel tout un chacun fait face et qui revêt un enjeu primordial dans le cadre de la défense nationale.

Par Lika LHOSTE

LES QR CODES PIÉGÉS :

Un risque sous-estimé

Initialement conçus pour tracer des pièces dans l'industrie automobile, les QR codes ou Quick Response codes (code de réponse rapide) - nom choisi pour signifier que l'on peut faire une lecture ou un accès rapide aux informations de l'objet sur lequel il est apposé- se sont imposés dans notre quotidien. Ils facilitent l'accès aux services de la vie quotidienne qui ont été digitalisés comme des menus de restaurant, billets d'embarquement, paiements sans contact, ou encore authentifications à plusieurs facteurs- MFA et pas que. Les mots à retenir sont : facilité, accès et digital. Leur simplicité d'utilisation et leur polyvalence ont conquis les usagers. Cependant, cette popularité grandissante attire aussi l'attention des cybercriminels. Discrets et visuellement identiques, les QR codes malveillants deviennent des vecteurs efficaces d'attaques, souvent qualifiées de Quishing, contraction de QR et phishing.

QR Code : fonctionnement et détournement

Si dans l'industrie ils suivent un standard approuvé par l'Agence Nationale de la Sécurité des Systèmes d'Information (MH10.8.2) et le standard SQRL compatible avec la norme ISO 15434 afin d'homogénéiser les informations fournies et s'assurer qu'elles soient lisibles par les applications agréées pour les utilisateurs de ces produits et les partenaires logistiques[99], les QR codes réguliers du quotidien sont quant à eux produits selon un standard ouvert.
Un QR code est une sorte de code barre qui est une matrice de points pouvant encoder jusqu'à 7089 caractères numériques et 4296 caractères alphanumériques. Il utilise la correction d'erreur Reed-Solomon pour rester lisible même s'il est partiellement endommagé. Un code QR est un moyen facile d'envoyer les clients vers une destination numérique. Ils encodent en quelque sorte un itinéraire numérique[100]. L'encodage suit les étapes suivantes :

1. **Conversion des données** : l'URL (ex. **https://faux-site.fr/login** qui n'existe pas) est convertie en binaire selon un mode d'encodage (numérique, alphanumérique, byte, etc.);
2. **Ajout de données de format** : niveau de correction d'erreur, masque, etc;
3. **Distribution dans la matrice** : les bits sont répartis dans un schéma prédéfini ;
4. **Génération visuelle** : une image carrée avec motifs détectables par les scanners.

Les cybercriminels exploitent divers canaux pour diffuser des QR codes malveillants, souvent en jouant sur la confiance et/ou la distraction des utilisateurs. L'une des méthodes les plus répandues consiste à faire un détournement physique en collant des QR falsifiés sur des supports existants. Cette superposition discrète transforme un objet familier en piège numérique. D'autres vecteurs passent par le phishing par email ou SMS, avec des messages alarmants ou attrayants du type "Votre colis est en attente, scannez ce code pour le suivre". Les bots sur les applications de messagerie sont également mobilisés pour diffuser massivement des QR codes piégés, souvent sous forme de fausses promotions ou de jeux-concours. Enfin, les réseaux sociaux deviennent un terrain fertile pour ce type d'attaque, via des publications sponsorisées, des vidéos virales ou des visuels contenant des QR codes frauduleux menant à des sites d'hameçonnage ou à des téléchargements malveillants.
Le Quishing redirige l'utilisateur vers un site frauduleux imitant une banque, une plateforme de messagerie ou pire, un service administratif. L'objectif est d'amener la victime à saisir ses identifiants, coordonnées bancaires ou autres données sensibles. L'aspect anonyme du QR code rend ce type d'attaque particulièrement difficile à détecter.

D'autres QR codes peuvent servir à distribuer des malwares en redirigeant alors vers des fichiers exécutables malveillants, souvent présentés comme des applications utiles (par exemple, un scanner ou un outil de sécurité). Une fois installés, ces logiciels peuvent intercepter les SMS, accéder aux contacts ou détourner des sessions bancaires. Certains QR codes contiennent les informations nécessaires pour se connecter automatiquement à un réseau Wi-Fi. Un utilisateur peu méfiant peut ainsi se retrouver connecté à un point d'accès malveillant, utilisé pour intercepter le trafic.
Enfin, des QR codes peuvent déclencher l'envoi automatique de SMS ou d'appels vers des numéros surtaxés. Cette méthode repose sur des failles de configuration des appareils Android, et peut entraîner une surfacturation importante sans que l'utilisateur ne s'en rende compte immédiatement.

Le Quishing tire son efficacité d'un enchaînement de facteurs techniques, contextuels et psychologiques qui exploitent la crédulité des victimes en contournant les protections classiques. L'opacité du QR code, dont le contenu reste invisible avant le scan, constitue la faille majeure. Contrairement à un lien cliquable, l'URL encodée n'est pas directement lisible, ce qui empêche toute évaluation préalable.S'ajoute à cela une confiance largement répandue dans la fiabilité du QR code, perçu comme un outil moderne et pratique, rarement remis en question. Cette perception, renforcée chez certaines populations comme les personnes âgées, renvoie souvent au code-barres traditionnel, synonyme d'authenticité. La faiblesse des protections sur mobile, notamment sous Android, accentue cette vulnérabilité car peu d'utilisateurs disposent d'un antivirus actif et les mécanismes natifs ne bloquent pas toujours les

99 https://rla.org/resource/12n-documentation
100 https://www.fortinet.com/fr/resources/cyberglossary/what-is-a-qr-code

actions malveillantes déclenchées via un QR. Enfin, l'effet de surprise joue un rôle central car un QR code discrètement apposé sur une affiche, un distributeur ou un menu attire l'attention et inspire confiance, créant ainsi un contexte idéal pour la fraude.

Des cas concrets

Il y a une diversité des contextes d'utilisation frauduleuse des QR codes, allant de la rue aux grands événements internationaux, en passant par le courrier postal. En Allemagne, dès 2021, des QR codes affichés dans les transports publics (notamment les métros et bus) redirigeaient vers de faux sites de traçage COVID-19. Ces pages collectaient des données personnelles et des identifiants sous couvert de participation à la gestion sanitaire, alors qu'il s'agissait de tentatives sophistiquées de vol d'informations. En France lors des Jeux Olympiques de Paris 2024, le dispositif officiel "Pass Jeux", reposant sur un QR code permettant d'accéder aux zones sécurisées, a été la cible de tentatives de falsification et de contrefaçon, dans le but d'usurper des accès ou de tromper les forces de sécurité.[101]

Par ailleurs, certaines arnaques prennent des formes plus insidieuses, comme en témoignent les fausses contraventions déposées dans les boîtes aux lettres de particuliers en France. Des escrocs impriment de faux avis d'amende, accompagnés d'un QR code redirigeant vers un site frauduleux de paiement, visuellement proche du site officiel de l'administration.[102]

Que dit la législation française à ce sujet ?

En France, aucun texte ne régit spécifiquement l'usage ou le détournement des QR codes. Néanmoins, plusieurs articles du Code pénal[103] permettent de sanctionner leurs usages malveillants.

- L'article 313-1 punit l'escroquerie, applicable notamment aux QR codes usurpant un site officiel ou menant à un faux paiement.
- Les articles 323-1 à 323-3 sanctionnent l'accès ou la modification frauduleuse d'un système informatique, ce qui couvre l'installation de malwares via QR.
- Les articles 226-16 à 226-24 protègent les données personnelles ; un QR redirigeant vers un faux formulaire entre dans ce cadre.
- L'article 226-4-1 s'applique en cas d'usurpation d'identité, possible lorsqu'un QR simule un site bancaire ou administratif.

En revanche, le Code de la consommation[104] ne traite pas spécifiquement des QR codes, et ses articles sur la portabilité des données ont été abrogés depuis l'entrée en vigueur du RGPD en 2018. Enfin, l'usage de QR codes pour générer des appels ou SMS surtaxés constitue une escroquerie électronique (art. 313-1), aggravée si la victime est vulnérable.

Quelques contre-mesures

Côté utilisateur	Côté entreprise
Vérifier l'URL affichée avant d'ouvrir le lien.	Vérifier régulièrement les supports contenant des QR.
Éviter de scanner des QR dans l'espace public sans contexte clair.	Intégrer un marquage visuel (logo, style) pour distinguer les QR légitimes.
Ne pas installer d'application via un QR.	Préférer des QR temporaires (lien à usage unique).
Utiliser des scanners qui montrent l'URL en clair (ex: Kaspersky QR Scanner).	Sensibiliser les collaborateurs au Quishing.
Éviter les connexions WI-FI par QR code dans les lieux sécrurisés.	Surveiller les QR codes diffusés via Google Images, réseaux sociaux, etc.

Les bonnes pratiques de sécurité liées aux QR codes[105]

Le QR code, symbole d'innovation et surtout de simplicité, s'est imposé dans notre quotidien comme un outil pratique… mais aussi, dans l'ombre, comme une arme redoutablement discrète entre les mains des cybercriminels. Son opacité intrinsèque et sa facilité de fabrication en font un vecteur idéal pour des attaques de phishing, de diffusion de malwares ou encore d'interception de données, souvent sans éveiller le moindre soupçon. La sensibilisation des usagers, la formation continue des professionnels du numérique, et la mise en place d'un cadre réglementaire plus précis sont des piliers indispensables pour renforcer notre résilience. Car derrière ce simple carré noir se cache parfois bien plus qu'un raccourci, une faille. Il est donc urgent d'adopter une culture de vigilance, où chaque scan devient un acte conscient, réfléchi et non un automatisme naïf.

Par Joseline YOUEGO

101 Le Monde. (2024). *Paris 2024 : au bord de la Seine, les forces de l'ordre face au casse-tête du « Pass Jeux »*, 25 juillet 2024.
102 TF1 Info. (2024). *Faux QR codes : comment déjouer les pièges ?* Bonjour ! La matinale, TF1.
103 Legifrance. (2024b). Code pénal – Partie législative.
104 Legifrance. (2024a). Code de la consommation – Section abrogée sur la portabilité des données.
105 France Num. (2024). *QR Code : quelle sécurité et quelles précautions ?* Guide cybersécurité PME.

CONCLUSION

Par Charlotte WOJCIK, Fondatrice des Cadettes de la cyber

Nous espérons que ces pages ont nourri votre réflexion, éveillé votre curiosité et stimulé votre engagement. Car la cybersécurité n'est pas une fin en soi : elle est un chemin collectif vers un futur où le numérique sera non seulement maîtrisé et respectueux des citoyens, mais aussi porteur de progrès pour tous.

Ce livre dépasse le simple recueil d'articles : il reflète un mouvement. Chaque contribution des Cadettes de la Cyber témoigne de la curiosité, de la rigueur et de l'engagement d'une nouvelle génération qui choisit de regarder le numérique autrement. Les incidents deviennent des opportunités d'apprentissage, les analyses se transforment en boussoles, et les regards multiples dessinent une vision élargie de la cybersécurité, aujourd'hui et demain.

En croisant leurs parcours, leurs connaissances et leurs sensibilités, elles montrent que la cybersécurité n'est pas seulement une question d'outils ou de protocoles : c'est un défi humain, sociétal et stratégique qui touche toutes nos activités. Il s'agit avant tout de permettre à chacun de se sentir et d'être en sécurité dans l'espace numérique.

À travers leur travail et leur réflexion, les Cadettes rappellent que protéger le cyberespace, c'est aussi défendre la confiance, l'éthique et la responsabilité qui fondent nos sociétés démocratiques. Ce livre invite donc chaque lecteur - étudiant, professionnel ou citoyen - à s'emparer de ces enjeux, à s'engager et à contribuer à un numérique plus sûr, inclusif et respectueux des citoyens et de leurs données.

Charlotte
WOJCIK

Avec cet ouvrage, Les Cadettes affirment haut et fort que la cyber est aussi une affaire au féminin : oser sa passion, et aller droit devant !

BIBLIOGRAPHIE

Sources : Cyber attaques et genre

00h21, Par Le Parisien avec AFP Le 30 avril 2024 à. « *Chantage aux photos intimes visant des adolescents : face au nombre de cas, la police britannique alerte les enseignants* ». leparisien.fr, 29 avril 2024. https://www.leparisien.fr/international/chantage-aux-photos-intimes-visant-des-adolescents-face-au-nombre-de-cas-la-police-britannique-alerte-les-enseignants-30-04-2024-CPL5HPZLJRB7JILFGTICASUMVU.php.

Assistance aux victimes de cybermalveillance. « *Cybermoi/s 2024 : les Français face aux cybermenaces Une étude IPSOS pour Cybermalveillance.gouv.fr* ». Consulté le 30 juin 2025. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermois-2024-etude-ipsos.

« Cyberviolences et cyberharcèlement : le vécu des victimes | Ipsos », 15 décembre 2022. *https://www.ipsos.com/fr-fr/cyberviolences-et-cyberharcelement-le-vecu-des-victimes.*

Cyber Civil Rights Initiative. « *Revenge Porn Statistics* ». Consulté le 30 juin 2025. *https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf.*

Hofstetter, Julia-Silvana et Panthea Pourmalek, Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity, 2023. *http://gnwp.org/gender-cybersecurity-through-women-peace-security [consulté le 08/12/2023]*

LFPT. « *Fraudes aux moyens de paiement et escroqueries en hausse de 64 % entre 2016 et 2023* ». La finance pour tous (blog), 18 juillet 2024. *https://www.lafinancepourtous.com/2024/07/18/fraudes-aux-moyens-de-paiement-et-escroqueries-en-hausse-de-64-entre-2016-et-2023/.*

Mercier, Etienne, Adeline Merceron, Sophie Morin, et Amélie Marmuse. « *CYBERVIOLENCE ET CYBERHARCÈLEMENT : ETAT DES LIEUX D'UN PHÉNOMÈNE RÉPANDU* », s. d.
Pangarkar, Tajammul. « *Dark Web Statistics By Country, Demographics And Facts (2025)* ». Sci-Tech Today (blog), 21 mai 2025. *https://www.sci-tech-today.com/stats/dark-web-statistics-updated/.*

« *Quelle est la place des femmes dans la cybercriminalité ?* » INCYBER NEWS , 14 mars 2023. *https://incyber.org/article/quelle-est-la-place-des-femmes-dans-la-cybercriminalite/.*

Sources : Pour aller plus loin

Sources académiques

Ashraf, Cameran "*Defining cyberwar: towards a definitional framework*". Defense & Security Analysis, vol. 37, no 3, 2021, pp. 274-294
Bengtsson Meuller, Elsa, A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism. London, Global Network on Extremism and Technology, 2023. doi: *https://doi.org/10.18742/pub01-132*

Brown, Deborah et Allison Pytlak. «*Why gender matters in international cyber security.*» Women's International League for Peace and Freedom and the Association for Progressive Communications, 2020
Bjola, Corneliu et Markus Kornprobst. Digital International Relations. Abingdon, Oxon, 2023

Buzan, Barry. People, states and fear: An Agenda for security Analysis in the PostCold War Era. Brighton, Weatsheaf, 1991 Dwyer, Andrew et al. «*What can a critical cybersecurity do?.*» International Political Sociology vol.16 n°3, 2022, pp.1-26

Gurumurthy, Anita et Niveditha Menon. «*In order to open up.*» Economic & Political Weekly, vol.44 n°40, 2009, pp.19-21

Haciyakupoglu, Gulizar et Yasmine Wong. "*GENDER, SECURITY AND DIGITAL SPACE: ISSUES, POLICIES, AND THE WAY FORWARD*". S. Rajaratnam School of International Studies, 2021

Hall, Matthew et Jeff Hearn, "*Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts*", Journal of Gender Studies, vol.28 n°2, 2019, pp.158-170
King-Close, Alexandria A Gender Analysis of Cyber War. Harvard, Harvard University, 2016
Lewis, Ruth et al, «*Online/Offline Continuities: Exploring Misogyny and Hate in Online Abuse of Feminists.*» In Online Othering: Exploring Digital Violence and Discrimination on the Web, Liverpool, Palgrave Macmillan, 2019
Li, Yuchong et Qinghui Liu. «*A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.*» Energy Reports, vol.7, 2021, pp. 8176-8186

Linden, Emmie, «*Gender in Cyber policy, is it really necessary?: A critical analysis of gender in EU's cybersecurity policy.*» Uppsala University, 2022

MacKenzie, Megan «*Women, Gender, and Contemporary Armed Conflict.*» Oxford Research Encyclopedia of International Studies, Oxford, Oxford University Press, 2010

Nieminen, Linda « *Why Is Human Trafficking Excluded from the EU's Cybersecurity? An Explorative Study about Cybersecurity and Human Trafficking in the European Union* », Swedish Defence University, 2020

Pernot, François et Philippe Wolf. "*Cyberguerre et géographie*". Revue de géographie historique, n°8., 2016, DOI : *https://doi.org/10.4000/geohist.5504*

Shepherd, Laura. "*Feminist Security Studies*", In The International Studies Encyclopedia. Oxford, Wiley-Blackwell, 2010, *<https://www.oxfordreference.com/view/10.1093/acref/9780191842665.001.0001/acref-9780191842665-e-0120>*,[consulté le 08/12/23]

Sjoberg, Laura, «*Feminist security and security studies.*» The Oxford Handbook of International Security, Oxford, Oxford University Press, 2018, p.45-59

Sjoberg, Laura, Gender and international security: feminist perspectives. Abindgon, Routledge, 2009

Sjoberg Laura et Jillian Martin. "*Feminist security studies: Conversations and introductions*". ISA Compendium Project, 2007, p. 50-59.

Slupska, Julia «*Safe at home: Towards a feminist critique of cybersecurity.*» St Antony's International Review vol.

15, n° 1, ,2019, pp.83-100.

Slupska, Julia. Safer (cyber) spaces: reconfiguring digital security towards solidarity. University of Oxford, 2022

Techan, Mahlet «*Gendering Cyber Warfare: A theoretical and exploratory paper addressing the research gap on the gendered aspects of cyber warfare.*» Uppsala University, 2020

Tickner, J. Ann "*Feminist responses to international security studies*", Peace Review, vol.16 n°1, 2004, pp.43-48

Tickner, J. Ann «*Re-visioning Security*», dans K. Booth et Smith, International Relations Theory Today, Pennsylvania, Pennsylvania State University Press, 1995, pp. 175-197

Windsor, Leah "*The language of radicalization: Female Internet recruitment to participation in ISIS activities*", Terrorism and political Violence, vol. 32, no 3, 2020, pp. 506-538

Sources gouvernementales et médiatiques

Arango, Diana Jimena et al,"*Forced Displacement and Violence Against Women : A Policy Brief*". World Bank Group, 2018.
<http://documents.worldbank.org/curated/en/593151638940044686/forced-displacement-and-violence-against-women-a-policy-brief> [consulté le 08/12/2023]

Hofstetter, Julia-Silvana et Panthea Pourmalek, Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity, 2023.
<http://gnwp.org/gender-cybersecurity-through-women-peace-security> [consulté le 08/12/2023]

Jankowicz, Nina "*How disinformation became a new threat to women*", Coda Media, 11 Décembre 2017, *<https://www.codastory.com/disinformation/how-disinformation-became-a-new-threat-to-women/>* [consulté le 08/12/2023]

Mhajne, Anwar, Luna K.C, Crystal Whetstone, "*A call for feminist analysis in cybersecurity: highlighting the relevance of the Women, Peace and Security agenda*", LSE, 17 Septembre 2021, *<https://blogs.lse.ac.uk/wps/2021/09/17/a-call-for-feminist-analysis-in-cybersecurity-highlighting-the-relevance-of-the-women-peace-and-security-agenda/ >* [consulté le 08/12/2023]

Sources : L'enfance en ligne

INSEE Références. "*Les enfants de moins de 6 ans et les écrans numériques : à chacun son rythme, d'après l'enquête Elfe*". Edition 2022. *"France, portrait social*".
https://www.insee.fr/fr/statistiques/6535295?sommaire=6535307

Pôle Société. "*Baromètre du numérique - Rapport*". Mars 2025.
https://labo.societenumerique.gouv.fr/documents/40/Rapport_barom%C3%A8tre_num%C3%A9rique_2025_final_compressed.pdf

Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri. "*Cybersecurity awareness for children : A systematic literature review*". 2021. International Journal of Child-Computer Interaction.
https://doi.org/10.1016/j.ijcci.2021.100343

Alžbeta Kovaľová. "*Grooming & prédateurs en ligne : une menace en plein essor*". 12 mars 2025. Safer kids online.
https://saferkidsonline.eset.com/fr/article/grooming-predateurs-en-ligne-menace-grandissante

Nellie Bowles, Michael H. Keller. "*Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*".

7 décembre 2019. The New York Times.
https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html

Nikoleta Lydaki Simantiri. "*Abus et exploitation sexuels des enfants en ligne - Formes actuelles et bonnes pratiques pour la prévention et la protection.*" Juin 2017. ECPAT France Luxembourg.
https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/09/Revue-SECO_FR-interactive.pdf

Futura Sciences. "*Jouets connectés : les peluches Cloudpets sont piratables*". mars 2017.
https://www.futura-sciences.com/tech/actualites/securite-jouets-connectes-peluches-cloudpets-sont-piratables-66497/

Kaspesky. "*Smart toy vulnerabilities could let cybercriminals video-chat with kids*". 2024.
https://www.kaspersky.com/about/press-releases/smart-toy-vulnerabilities-could-let-cybercriminals-video-chat-with-kids

Human Rights Watch. "*Governments Harm Children's Rights in Online Learning*". 2022.
https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning

CNIL. "*Design trompeur : les résultats de l'audit du Global Privacy Enforcement Network*" 2024.
https://www.cnil.fr/fr/design-trompeur-les-resultats-de-laudit-du-global-privacy-enforcement-network

Google. Jeu Interland.
https://beinternetawesome.withgoogle.com/fr_all/interland

Fresque des cybercitoyens.
https://fresquedescybercitoyens.fr/

les CADETTES DE LA CYBER

www.les-cadettes-de-la-cyber.org
02 23 06 10 30 | les-cadettes-de-la-cyber@pole-excellence-cyber.org