FOCUS TECHNIQUE >
Cyberharcèlement :
de la victime au prédateur

PROTECTION
DES PERSONNES > L'IA,
l'artifice sans intelligence

JUSTICE > Enquête judiciaire
et cybercriminalité

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / DECEMBRE 2019 / N° 266 / PRIX 6 EUROS

L'humain
au cœur de la cybersécurité

FIC 2020

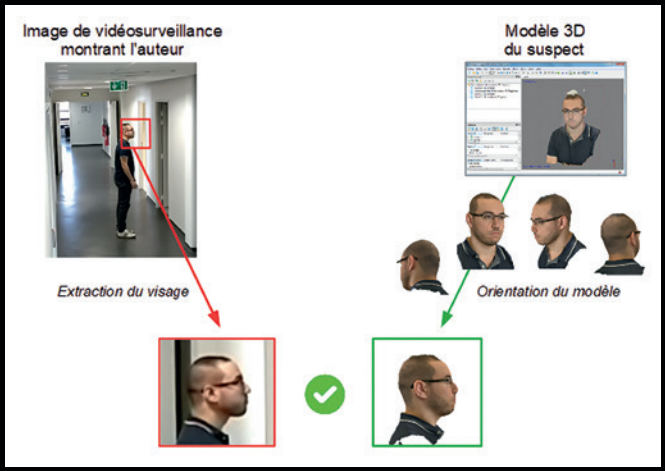
retour sur images NUMÉRO 265

© Karichs - AdobeStock - 61152912

LES VIOLENCES INTRAFAMILIALES

S'insérant dans les dispositifs plus larges de la lutte contre les violences faites aux femmes, celle contre les violences infra-familiales (VIF) est entrée dans le champ d'action des policiers et gendarmes de façon structurée au début des années 2000. Les progrès de la lutte contre les VIF sont sensibles, notamment au niveau des partenariats. On notera l'indispensable action du milieu associatif et des professions de santé. La recherche ouvre de nouvelles pistes. D'un ordre technologique, elles relèvent également d'une meilleure coordination des acteurs et de leur formation. Elles soulignent l'intérêt de considérer la prise en charge des enfants et des agresseurs ainsi que de faire évoluer les modes opératoires des primo-intervenants.

RETROUVEZ À PARTIR DE LA PAGE 141, UNE ÉTUDE SUR UN PROJET TECHNIQUE DE MODÉLISATION 3D DES VISAGES QUI S'INSÈRE DANS DES PROCESSUS D'IDENTIFICATION ET D'AUTHENTIFICATION.



Replacer l'humain au cœur de la cybersécurité

La cybersécurité s'est construite par strates successives. Au contrôle du « traitement » des données (1978) a succédé la protection des « systèmes » de traitement automatisé de données (1988), puis celle des « données », replacées au centre de l'écosystème numérique (2018). Les données à caractère personnel ont toujours fait l'objet d'une vigilance particulière, mais jamais leur sensibilité

n'a été autant mise en exergue, du fait de la croissance exponentielle des plateformes, des applications, des systèmes connectés qui « reformatent » notre société avec une vitesse souvent imperceptible par nos propres sens. Plus que jamais, ces données nous caractérisent, dévoilent notre intimité, pénètrent la sphère du secret de notre vie privée sans laquelle il n'y a pas de liberté. Plus que jamais profilé par des algorithmes, l'humain n'est plus tout à fait le maître et tend à devenir sujet, au risque de finir esclave. Pourtant, rien n'est perdu, car la maîtrise de la transformation numérique appelle avant tout une mobilisation des compétences, une acculturation partagée aux enjeux du nouveau monde. Trop souvent abandonnée aux spécialistes, aux experts, la cybersécurité doit être en vérité le fruit d'une posture individuelle et collective qui résulte d'une formation largement diffusée dès le plus jeune âge. Trop souvent identifiée comme une filière réservée aux hommes, la cybersécurité doit aussi être portée par des femmes qui ne représentent aujourd'hui que 10 % des emplois correspondants, alors qu'elles constituent plus de la moitié de la population. Sans doute faut-il envisager le recours aux technologies, comme l'intelligence artificielle, pour sécuriser nos réseaux, nos échanges, nos données. Mais il importe surtout de repositionner – de repositiver – l'humain comme acteur de la cybersécurité, alors qu'il est essentiellement regardé aujourd'hui comme victime ou comme auteur, volontaire ou involontaire, des cyberincidents ou des cybermalveillances.

Dans notre quête de la cybersécurité, nous sommes trop souvent en attente de la réponse à la question « comment ? », en laissant aux technologies le soin d'y répondre ; nous avons ainsi négligé la question « pourquoi ? » en exigeant des finalités conformes à notre conception de l'humain. « Science sans conscience n'est que ruine de l'âme » écrivait Rabelais dans Pantagruel. Cette invitation à conjuguer les sciences « dures » et les sciences humaines est plus que jamais d'actualité. La cybersécurité a besoin de juristes, de sociologues, de philosophes, d'historiens, *etc.* pour garantir une sécurité de tous au service de la liberté de chacun.

Il est temps de replacer l'humain au cœur du discours et de l'action. Nous savons que, sans une vision européenne partagée, nous aurons demain le choix entre une « liberté surveillée » et une « sécurité surveillée », selon que nous serons « colonisés » par l'ouest ou par l'est. À l'Europe d'avoir enfin un vrai projet politique qui ait pour objectif d'assurer une « liberté sécurisée », garante des valeurs partagées par les 27 États membres. C'est l'occasion de donner du souffle à une transformation numérique par trop matérialiste. C'est le socle minimal pour offrir au reste du monde une alternative à l'imperium croissant des deux géants du

numérique. Nous avons perdu la bataille du hardware, du software et des plateformes. Nous pouvons gagner celle de l'humain. Nombre d'internautes, en Europe, « de l'Atlantique à l'Oural » et en Afrique n'attendent que cela.

Général d'armée (2S) Watin-Augouard
Fondateur du FIC

SOMMAIRE

NUMÉRO 266

INTERNATIONAL

PROTECTION DE LA PERSONNE

DOSSIER

FOCUS TECHNIQUE

JUSTICE

DOSSIER

L'humain maillon de la cybersécurité

INTERNATIONAL

© Par everythingpossible - n° de fichier : 221016087
E-commerce concept with VR digital interface

LE COMMERCE ILLICITE DÉSTABILISE UN ORDRE ÉCONOMIQUE MONDIAL

Le commerce illicite est inhérent à l'activité commerciale. Comme elle, il bascule dans le numérique. Il trouble le jeu économique en perturbant le recouvrement des taxes et charges sociales nationales, en faussant les règles de la concurrence et en mettant en danger le consommateur. La numérisation du commerce illicite fait sa force mais également sa faiblesse. Un traitement international de ce phénomène peut viser la sécurisation des chaînes d'approvisionnement par l'utilisation des blockchains qui sont au cœur de la traçabilité des produits. Selon les méthodes employées dans la lutte contre les réseaux criminels sur le Net, il doit permettre la mise en œuvre d'outils permettant d'objectiver les transactions à titre probatoire puis de les bloquer techniquement. La répression, pour être dissuasive, doit toucher sur un plan pénal et économique tous les acteurs qui profitent du commerce illicite : producteurs, intermédiaires, vendeurs et consommateurs avertis du caractère illégal de la vente d'un produit.

Le e.commerce illicite : nouvelle réalité humaine dans l'espace numérique

Par Dominique Lapprand

Le commerce est par nature une activité humaine ; il est aussi vieux que l'humanité. À ce titre, il subit les évolutions que celle-ci rencontre. Il se réalise aussi depuis peu, mais de plus en plus dans l'espace numérique. Le e.commerce illicite apparaît comme la conjugaison de ces deux évolutions. Son développement rapide, les moyens qu'il utilise comme ceux qui sont nécessaires pour lutter contre lui en font un sujet majeur de la cyber sécurité, qui combine la technologie au service de l'économie et l'homme entreprenant, malfaisant ou protecteur.

DOMINIQUE LAPPRAND

Chercheur associé ISM-KA project (Erasmus) Enseignant HEIP (Paris) et SHU (UK)

Le commerce illicite, une réalité complexe et menaçante qui s'étend au numérique

Le commerce illicite est inhérent à l'activité commerciale. La définition qu'en donne Interpol reflète cette réalité qui définit le commerce illicite comme la vente au public de biens ou de services en violation de la loi applicable. Cette formulation est d'une apparente simplicité mais, il n'est pas besoin d'être grand juriste pour le comprendre, d'une grande complexité. De quelle loi parle-t-on ? De quelle applicabilité est-il question ? Force est de reconnaître que cette complexité s'est accrue au cours du temps et s'est emballée dans notre monde global et numérisé.

La complexité juridique du commerce illicite englobe désormais le numérique

Traditionnellement la violation de la loi utilisée pour appréhender une activité de commerce illicite emprunte à une quadruple distinction.

Une première catégorie est constituée par la violation du droit de propriété, la vente

d'objets volés ayant été longtemps le principal mode de commerce illicite. Oubliée, elle reste vivace avec, pour le vol de fret, un chiffre d'affaire de plusieurs milliards d'euros en France par an. Aujourd'hui, le droit de propriété s'étend à la propriété intellectuelle. Celle-ci est notamment victime de la contrefaçon, dont le chiffre d'affaire, supérieur à 500 milliards de dollars par an, en ferait un État du G 20.
Une seconde catégorie va être constituée par la violation de la loi fiscale. On trouve ici les faux sauniers d'autrefois comme les vendeurs de cigarettes de Barbès.
La violation de loi administrative visant la protection d'intérêts sociétaux ou internationaux majeurs (droits humains, environnement, hygiène et sécurité du consommateur, espèces protégées, droits du travail, embargo ONU...) représente désormais le principal facteur de commerce illicite. Elle est parfois abusivement assimilée à la contrefaçon pour ce qui est des produits non conformes aux règles techniques et de sécurité (jouets, outils, pièces détachées, électronique...). Enfin la violation du droit commercial, plus particulièrement des contrats, donne lieu à une autre forme de commerce illicite, dit parallèle, où la vente de produits, donc l'accès à la valeur, échappe aux entreprises.

Par ailleurs, il convient de souligner que la complexité et la diversité de la loi, fondant le commerce illicite, se double d'une même complexité et diversité au plan de l'applicabilité.

Avec ce large spectre, la tendance est désormais de placer le commerce illicite dans la loi émergente du numérique, soit à l'initiative du législateur qui va cibler l'activité de commerce illicite, soit par la violation de la loi sur le numérique. Ainsi, au premier titre, une recommandation de la Commission Européenne, du 1er mars 2018, place la vente en ligne de produits, contrefaits ou dangereux pour le consommateur, dans le contenu illicite de l'Internet.
Sous un autre regard, l'organisation juridique des places de marché électronique conduit à faire de la violation des règles ainsi instituées une activité de commerce illicite. C'est ce que fait, en France, la loi de lutte contre la fraude du 23 octobre 2018.

Le basculement du commerce illicite dans le numérique

Comme le commerce ordinaire, le commerce illicite bascule dans le numérique. S'il est impossible à son égard, comme pour toute activité délictueuse, de disposer de statistiques précises, il est cependant possible de s'appuyer sur les chiffres de l'évolution générale du commerce vers l'électronique et comme, pour tout fait criminel, sur les affaires constatées.

Selon la Fédérations des entreprises de vente à distance (FEVAD), le volume de ventes en ligne, en France, par des entreprises françaises (200 000 sites de vente) est de 92,6 milliards d'euros, en progression annuelle de 12,45 %.

Les ventes à partir de mobiles représentent 22 milliards d'euros, en progression annuelle de 22 %. Il est probable que le commerce illicite connaisse une évolution semblable.

Au point de vue des constatations objectives, deux données retiennent l'attention : l'une statistique, l'autre ponctuelle. Selon l'OCDE, 63 % des produits contrefaits saisis dans le monde sont livrés par voie de messagerie expresse ou postale. Il est généralement estimé que cette livraison se fait à l'issue d'une transaction en ligne. Une affaire traitée par la Gendarmerie nationale, en mars 2018, fait apparaître un réseau de vente illicite de cigarettes utilisant des réseaux sociaux comportant 350 000 « profils clients » et vendant plusieurs tonnes de cigarettes par mois.

L'affaire précitée reflète parfaitement la transformation numérique du commerce illicite. Là où une « fourgue » à partir d'une boutique s'appuyait au mieux sur une clientèle de quelques centaines de personnes, un vendeur de réseaux sociaux utilise de multiples profils pour toucher des centaines de milliers d'amis et un vendeur de place de marché sur internet va manœuvrer plusieurs dizaines des milliers de sites pour contacter des millions de clients potentiels.

Le e.commerce, au-delà de l'infraction, est une menace dans l'espace numérique

La réalité du e.commerce illicite comme infraction est indiscutable. Est-ce pour autant de nature à en faire une menace réelle et grave au plan de la sécurité ?
En retenant la méthodologie de l'analyse du risque, à savoir s'interroger sur la capacité de la menace à attaquer un intérêt légitime, il est possible de mesurer comment le commerce illicite a un effet dramatique sur la société, le fonctionnement de l'État, les activités des entreprises et la vie du citoyen.

Le e.commerce perturbe le fonctionnement de l'État et la vie sociale

En s'affranchissant du paiement des taxes et des charges sociales, le e.commerce illicite prive l'État des ressources nécessaires à son action. En offrant à la société un modèle économique alternatif, il met en cause l'organisation sociale et le fonctionnement de l'économie régulière.
À ce titre, le combat que l'État français mène pour recouvrer les taxes, auxquelles échappe le commerce électronique, couvre aussi les activités de commerce illicite mais peut-on parler de commerce licite pour une activité qui s'organise pour échapper à la loi ?

Le e.commerce illicite menace les entreprises et leur modèle

Le e.commerce illicite menace les entreprises selon deux modes différents.
Au niveau des achats et approvisionnements, l'entreprise peut acquérir des biens ou des matériaux qu'elle va intégrer dans son processus et ses produits.

Si ceux-là viennent du commerce illicite, de l'exploitation d'enfants, d'atteintes à l'environnement, de produits non conformes, la responsabilité de l'entreprise comme complice de commerce illicite est engagée.

Au niveau de la vente, le commerce illicite constitue une concurrence déloyale et mortelle pour l'entreprise. Le respect de la loi a un coût : le respect des normes, une qualité, des obligations contractuelles, l'acquittement des taxes… Sa violation en fait un avantage concurrentiel permettant un moindre prix et/ou un profit plus élevé. Le résultat est une situation insupportable pour l'entreprise qui perd son client et voit ses produits délaissés, son marché perturbé. Au-delà des activités courantes c'est le modèle même de l'entreprise qui est atteint.

L'e.commerce illicite, par ses pratiques déloyales, génère des profits substantiels au détriment des rentrées fiscales des États et de la loyauté des transactions entre entreprises et clients. C'est un facteur de déstabilisation d'un ordre économique mondial.

Le e.commerce illicite menace les citoyens consommateurs

En fournissant au citoyen, sans lui donner d'outils de discernement, des produits susceptibles de mettre en danger sa sécurité, sa santé ou son hygiène, le e-commerce illicite menace directement le citoyen. Régulièrement la DGCCRF et la Douane, saisissent, interdisent et retirent du marché des produits, des jouets, des cosmétiques et des bijoux dont l'analyse laboratoire prouve la dangerosité pour le consommateur.

Le recours de certains professionnels (bâtiment, réparation automobile...) à des achats dans le cadre du commerce illicite les conduit à réaliser des offres tout aussi dangereuses pour leurs clients.

L'éco système du e.commerce illicite en lien avec la criminalité organisée et la délinquance

À ce stade il paraît nécessaire de mentionner l'existence d'un véritable écosystème numérique. En effet, dans le e.commerce illicite la vente ne se résume pas à une transaction électronique. Pour que vendeurs et acheteurs se rencontrent, il leur faut des intermédiaires, des prestataires du Net, des organismes de paiement et des opérateurs logistiques. Tous fonctionnent dans l'espace numérique de façon sinon intégrée du moins continue.

Ces intermédiaires peuvent être vertueux et se rendre, à leur insu, complices de commerce illicite. Ils peuvent aussi être de véritables criminels. La criminalité organisée seule a la capacité de faire franchir les frontières à des containers de produits destinés au commerce illicite organisé sur des sites web. La livraison de chaussures contrefaites, commandées sur des réseaux sociaux, va être assurée par de petits délinquants passés du guet dans le deal de drogue à la livraison à domicile dans le commerce illicite. Un parallèle peut être fait entre le commerce illicite et le trafic de drogue : mêmes acteurs, mêmes techniques mais profits plus élevés et risques moindres pour le commerce illicite avec il est vrai une image moins virile...

La technologie numérique pour lutter contre le e.commerce

Parce qu'il se réalise dans l'espace numérique, le e.commerce illicite s'appuie sur la technologie numérique. Si celle-ci en fait sa force pour se développer, elle en fait aussi la vulnérabilité. Le e.commerce illicite peut être prévenu ou attaqué par une technologie supérieure.

Le premier axe de lutte contre le e.commerce illicite consiste à empêcher la circulation impunie de produits du commerce illicite dans les chaînes d'approvisionnement. Au-delà, il s'agit pour les entreprises de sécuriser leur chaîne de distribution et d'assurer au consommateur l'authenticité et la qualité des produits fournis. La blockchain, déjà largement employée en agro-alimentaire, apparaît

comme une solution prometteuse. Encore faut-il la sécuriser au plan des accès et de la gouvernance. Il y a là un terrain qui exige des développements importants et rapides.

C'est sur le plan offensif de la lutte contre le e-commerce illicite que la technologie est également indispensable. Dans l'espace numérique comme dans le monde réel, il s'agit de surveiller pour détecter et identifier les activités malfaisantes afin ensuite de les bloquer au plan technique, de les appréhender de façon à objectiver des constatations appelées à devenir éléments de preuve. Les outils et les techniques utilisées pour lutter contre les réseaux du commerce illicite sont à cet égard les mêmes que ceux utilisés contre tous les réseaux criminels du net et des réseaux sociaux, les terroristes diffusant un discours de haine ou de recrutement, les pédopornographes, les trafiquants de drogue….

Ces outils sont déjà utilisés par des entreprises, par leurs prestataires de service, par des organismes publics : OCLTICC, C3N, Cyberdouane, Centre de surveillance du commerce électronique. Ils sont ceux utilisés dans les enquêtes judiciaires de criminalité organisée. Ils demandent indéniablement à être développés pour suivre l'avancement de la menace

Ignorer le e.commerce illicite, c'est ignorer une cyber menace d'autant plus grave qu'elle est en développement rapide, qu'elle est présente partout et en permanence dans la vie des entreprises et dans celle des citoyens.

L'AUTEUR

L'auteur est un ancien officier de la Gendarmerie nationale au sein de laquelle il a servi en administration centrale et comme commandant de groupement de gendarmerie départementale. Il a également été détaché au ministère de la Justice (DACG), à l'international (projet PHARE police Bulgarie 1998-1999) et auprès de la Commission Européenne (Expert National détaché 2000-2005). Depuis 2005, il a multiplié pour le compte de l'UE, des Nations Unies, du gouvernement britannique, les missions de réforme du secteur de la sécurité dans dix-sept pays d'Afrique, du Moyen-Orient et d'Asie.
Il est expert sécurité et commerce illicite du projet ISM-KA (programme Erasmus) et conseille un groupe international en matière de commerce illicite, domaine dans lequel il anime, depuis 2017, une association (ALCCI) aux côtés d'Alain Juillet.

COMBATTRE LE COMMERCE ILLICITE DES PRODUITS RÉGLEMENTÉS EN LIGNE

LA CONTREFAÇON : UN ENJEU ÉCONOMIQUE ET DE SANTÉ PUBLIQUE

La contrefaçon procède selon des modalités massifiées et industrialisées. Internet est le second distributeur de produits de contrefaçon du fait du foisonnement de l'offre, de la diversité des circuits et de la maîtrise des protocoles commerciaux sur les réseaux par les contrefacteurs. Les produits de la contrefaçon inondent les secteurs de la santé, du vêtement, des cosmétiques, etc. Issus de pays où les conditions de productions des produits sont douteuses et où l'application du Code du travail est optionnelle, ils ne sont pas conformes aux normes et posent la problématique de la sécurité des acheteurs. L'Unifab, association française de promotion et de défense du droit de la propriété intellectuelle, regroupe plus de 200 entreprises issues de tous les secteurs d'activité. Elle travaille à instaurer de bonnes pratiques pour l'ensemble des acteurs du digital, notamment par des mesures de filtrage visant la suppression des annonces de contrefaçon. Elle concourt à la formation des agents opérationnels dédiés au contrôle de ces marchandises et à l'éducation des consommateurs.

Contrefaçon et Internet

Questions à Delphine Sarfati-Sobreira

Q

Quelle forme prend, aujourd'hui, la contrefaçon en France ?

En quelques décennies, la contrefaçon a complètement changé de nature. Nous sommes passés d'une modalité artisanale à une version massifiée et industrialisée où les conditions de production des produits sont douteuses et où l'application du Code du travail est optionnelle.

Le constat est sans appel : les réseaux qui fabriquent du faux sont les mêmes que ceux qui vendent des armes, de la drogue ou bien même agissent dans le spectre du terrorisme ! L'UNIFAB a d'ailleurs publié un rapport édifiant sur les liens qui unissent les réseaux terroristes à ceux de la contrefaçon du fait qu'il se livrent, tout simplement, à des activités criminelles peu punies et qui rapportent beaucoup. Les bénéfices colossaux dégagés par ces ventes illégales contribuent à organiser, acheter et former les « soldats » des plus grandes organisations internationales qui sèment la terreur.

DELPHINE SARFATI-SOBREIRA

Directrice générale de l'Unifab

Les faux s'écoulent-ils essentiellement via les plateformes de vente en ligne ?

Aujourd'hui, Internet est le second distributeur de produits de contrefaçon. Il n'a jamais été aussi facile de se procurer tout ce que l'on désire depuis son canapé ou son bureau. Un simple accès à cette mine incroyable d'informations et de propositions constitue une brèche dans laquelle les contrefacteurs peu scrupuleux se sont immiscés pour pénétrer dans le quotidien des consommateurs, portant ainsi atteinte à leur santé et leur sécurité. Il faut savoir que les produits de contrefaçon ne correspondent à aucune des normes mises en place pour la sécurité des acheteurs car seul le profit généré compte.

D'ailleurs, il faut le préciser, les vendeurs de faux n'hésitent plus à mettre la photo du vrai produit pour en expédier un faux !

Peut-on trouver de la contrefaçon dans des réseaux de vente plus traditionnels (marchés, foires, voire boutiques) ?

Bien sûr, les marchés sont également des lieux privilégiés que les contrefacteurs utilisent pour berner les consommateurs. L'indice principal et le conseil majeur à donner à tous, est de rester vigilants quant au lieu d'achat et aux prix pratiqués car un tarif trop attractif est suspect. Certains articles sont vendus par le biais d'un réseau de distribution sélectif et d'autres ne le sont que par des distributeurs agréés. Pour vous donner des exemples, des articles de luxe ou des médicaments, ne peuvent pas se retrouver sur des marchés ou des foires... Cela fait appel au bon sens de chacun…

A-t-on d'ailleurs une idée précise de la part des contrefaçons vendues *via* Internet ?

La France compte désormais 39 millions de cyberacheteurs, selon le dernier observatoire des usages Internet de Médiamétrie, ce chiffre a augmenté d'1,5 million, en un an.

Selon le rapport de la Douane française, il apparaît que sur les 5.4 millions de produits saisis aux frontières de la France en 2018, 30 % sont issus de petits colis, résultats d'achats sur internet.

Il faut savoir que les agents opérationnels, de la Douane dédiés au contrôle de ces marchandises réalisent un vrai travail de fourmi et de ciblage. Ils sont sensibilisés par l'Unifab à travers une cinquantaine de formations réalisées, soit annuellement plus de 700 agents de terrain formés à distinguer les faux des vrais.
En revanche, il est très difficile de savoir combien de contrefaçons sont vendues chaque année sur Internet, mais l'IFOP indique que 37 % des consommateurs qui ont été livrés d'un faux produit pensaient faire l'acquisition d'un produit authentique !

Quels produits et secteurs sont les plus concernés ?

L'Unifab, qui est l'association française de promotion et de défense du droit de la propriété intellectuelle, regroupe plus de 200 entreprises issues de tous les secteurs d'activité. Ce groupement de toutes les industries indique bien la présence de la contrefaçon dans tous les circuits que ce soit des biens de luxe, de consommation courante ou bien même des produits plus rares. De manière générale, plus un produit est à la mode, utile ou de saison, plus il est copié.

union des fabricants unifab

La contrefaçon s'est-elle particulièrement accentuée dans certains d'entre eux ?
Les contrefacteurs surfent sur les tendances et les périodes auxquelles ils projettent d'écouler et vendre leurs marchandises sur le marché. Ces produits sont de basse qualité et ne résisteront pas au temps et à l'usure. Ils ne correspondront en aucun cas aux attentes des consommateurs. Par exemple, l'été approchant, nous allons faire face à une recrudescence de lunettes de soleil, de crèmes solaires, de maillots de bain, *etc.* ... À Noël, seront proposés de nombreux faux jeux et jouets, de faux produits alimentaires nobles, *etc.* qui envahiront le marché. Ce sont autant de produits qui rythment le quotidien des consommateurs sur ces périodes.
Il est tout à fait possible de constater que le palmarès des produits saisis évolue et change en fonction des années.
En 2018, les jeux et les jouets ainsi que les produits de soins corporels ont occupé les premières places du podium des produits les plus stoppés.

Quels risques, d'un point de vue légal mais également en termes de santé et de sécurité, prennent les consommateurs qui achètent un produit contrefaisant ?
Nul n'est censé ignorer la loi. Un consommateur qui se fait contrôler en possession de produits contrefaisants est soumis à la législation en vigueur, c'est-à-dire qu'il se verra confisquer son achat et appliquer une amende pouvant atteindre deux fois la valeur de l'article authentique.
Autant vous dire qu'une fausse montre teintée couleur or achetée sur une plage 5 euros peut coûter plusieurs dizaines de milliers d'euros d'amende… un coût exorbitant pour une babiole ! En cas de poursuite pénale, les peines vont jusqu'à 7 ans d'emprisonnement et 750 000 euros d'amende. La contrefaçon n'est jamais un choix judicieux … Les produits authentiques respectent des normes dédiées à assurer la santé et la sécurité des consommateurs alors que le contrefacteur ne respecte pas ces obligations essentielles qui engendrent une étape de production et de ce fait un coût supplémentaire qui vient entacher sa marge bénéficiaire.

A-t-on des exemples de produits particulièrement dangereux ?
Potentiellement tous les produits peuvent être dangereux… Nous pouvons prendre l'exemple d'une contrefaçon de médicament car rien n'est plus grave qu'une pilule censée soigner et qui se révèle, dans le meilleur des cas, sans aucun principe actif ou, dans le pire des cas, composée de substances toxiques. Dans le domaine du textile, on peut évoquer une teinture trop chargée en plomb qui peut empoisonner la personne qui porte le produit.
Il en est de même pour les produits ménagers ayant des composantes néfastes ou des métaux lourds non vérifiés qui peuvent causer des allergies. Enfin, que dire de lunettes de soleil, sans filtre UV, qui peuvent provoquer des brûlures de rétine…

Quels conseils peut-on donner aux consommateurs AVANT l'achat, pour qu'ils sachent reconnaître une contrefaçon ou évitent les pièges, et APRES l'achat, en matière de recours (plateformes de signalement, *etc.*) ?

Avant l'achat, il faut que le consommateur se demande s'il achète le bon produit au bon endroit et à un prix cohérent. Cet indicateur est primordial et c'est souvent la clé pour consommer authentique. Il faut également s'attarder sur les conditions générales de ventes (principalement sur les sites Internet), les fautes d'orthographe pouvant révéler la présence d'un faux produit et éviter au consommateur de se faire duper. Le contrefacteur use de stratagèmes de plus en plus élaborés pour s'assurer que les acheteurs se leurreront… Il peut poster sur un site la photo d'un produit authentique avec un faible rabais pour appâter le consommateur et envoyer un faux par la suite.

Malheureusement, il n'existe pas de service après-vente dans ces cas-là. La plupart du temps, le consommateur est lésé, en plus d'avoir été abusé, et se retrouve avec le produit d'une contrefaçon, sans avoir de recours. Certaines plateformes de vente en ligne jouent très bien le jeu et acceptent en cas de duperie de rembourser l'acheteur victime de ces vendeurs peu scrupuleux, mais elles sont encore trop rares. L'Unifab travaille depuis de longs mois à instaurer et étendre ces bonnes pratiques à l'ensemble des acteurs du digital, notamment par la mise en place de mesures de filtrage destinées à pouvoir immédiatement supprimer les annonces de contrefaçon. Pour d'autres, cela est plus compliqué et une coopération public/privé encore plus intense pourrait être la réponse, si la coopération n'a pas raison de leur business model.

UNIFAB anime des campagnes de sensibilisation au profit des consommateurs.

© UNIFAB

Comment la contrefaçon impacte-t-elle les entreprises et les marques ? Le préjudice est-il à la fois moral et financier ?

La contrefaçon a un impact non négligeable sur l'économie… Il est clair que les contrefacteurs ne paient ni taxes, ni impôts. Lutter contre la contrefaçon représente un investissement colossal pour les entre-

prises car elles doivent mobiliser leurs efforts et leurs budgets pour pouvoir tenter de contrer ce fléau. Selon l'Organisation Mondiale du Commerce (OMC) la contrefaçon représente aujourd'hui 5 à 9 % du commerce mondial, ce qui correspond à près de 250 milliards de dollars. Le préjudice est également moral. Avant sa mise en circulation sur le marché, un produit est issu de la « Recherche et Développement », puis il est « markété » ce qui fait référence à des investissements importants.

L'atteinte à l'image peut être fatale pour certaines entreprises, notamment les plus petites, et perturber gravement la diffusion de certains produits.

Existe-t-il des moyens efficaces pour endiguer la cyber-contrefaçon ?

Devant cette recrudescence et la présence en ligne de produits contrefaisants, il devient urgent de prendre des mesures. C'est pour cela que certaines entreprises font appel à des prestataires externes,qui s'attèlent à dénoncer la présence de faux « online », par le biais d'une surveillance accrue de la toile, à la remontée de certaines informations et qui peuvent permettre de « couper » la tête de réseaux entiers.

Il faut vivre avec son temps et les industries l'ont bien compris ; les évolutions des modes de consommation passent par une adaptation technologique pour assurer une cyber-sécurité qui ne doit pas être optionnelle aujourd'hui.T

L'AUTEUR

Titulaire d'un Master of Communication & Business Administration, Delphine Sarfati-Sobreira a débuté sa carrière au journal Le Figaro, avant de rejoindre le groupe de communication Publicis où elle était en charge de budgets dans le secteur des produits de grande consommation. C'est à l'Unifab, association française de lutte contre la contrefaçon et de promotion des droits de propriété intellectuelle, qu'elle occupe par la suite le poste de Directrice de la communication et du développement, lui permettant de monter des projets européens de sensibilisation des consommateurs, des modules de formation pour les institutions publiques et de mener des actions concrètes en faveur des créateurs et des entreprises innovantes de tous les secteurs d'activités. Elle est nommée, en 2013, Directrice générale de l'Unifab et représente aujourd'hui le secteur privé français dans les organisations européennes et internationales.
Dans le cadre de ses fonctions, elle préside le groupe de communication du Comité National Anti-Contrefaçon (CNAC), publie de nombreux articles dans les médias et dispense régulièrement des conférences universitaires (Universités d'ASSAS, de MONTPELLIER, EDHEC, INSEEC, ESCE, EFAP, Sciences politiques, ESMOD, MODART, Sup de Luxe…)

NOTE DU RÉDACTEUR EN CHEF

La Gendarmerie nationale intervient dans le domaine de la lutte contre la contrefaçon et collabore étroitement avec l'UNIFAB : interventions récurrentes du SDPJ aux Forums Européens de la Propriété Intellectuelle, participation à la campagne de sensibilisation estivale de l'UNIFAB - affiches dans chaque brigade, actions de formations de l'UNIFAB dans le domaine de la contrefaçon au profit des gendarmes… On peut également évoquer la protection de la marque « Gendarmerie Nationale » qui a fait l'objet d'une démarche concertée.

FAKE-NEWS

LES FAUSSES NOUVELLES MINENT LES PROCESSUS DÉMOCRATIQUES EUROPÉENS

L'information revêt une dimension stratégique. Des puissances politiques ou des groupes d'intérêt l'incluent dans des protocoles d'insémination sémantique des populations pour les amener à adhérer à leurs objectifs. Ces menaces hybrides, car mêlant une palette d'activités coercitives ou d'induction, concourent à l'exposition des citoyens à une désinformation massive. Cette dernière menace la cohérence de la société en favorisant la cristallisation de points de vue orientés et en faussant la perception des mécanismes basiques de la démocratie. En effet, ce raidissement social est connexe d'un rejet des instances politiques et de régulation sociale. Consciente de cette menace, l'Union européenne a déployé deux types de stratégies relative à la gestion des menaces hybrides et contre la désinformation en ligne. Son action repose sur l'élaboration d'instruments de vérification des allégations, d'un dispositif d'alerte et l'instauration d'un code de bonnes pratiques en liaison avec les opérateurs des réseaux sociaux.

La lutte contre la désinformation en ligne, un thème essentiel de la gestion par l'UE des menaces hybrides

Par Pierre Berthelet

La prolifération des « fausses nouvelles » est devenue un nouveau défi pour l'Union européenne et ses États membres. Campagnes de diffusion d'informations erronées, développement des nouvelles technologies - telles que le Deep fake -, et influence étrangère sont devenus des dangers inédits pour la pérennité des sociétés actuelles. Le contrôle de la couche sémantique, particulièrement dans le cadre des processus électoraux, est un enjeu de survie pour la démocratie. En dressant un panorama des actions menées, l'objectif de cet article est d'analyser la manière dont l'UE se prémunit à l'égard des menaces hybrides.

PIERRE BERTHELET

Docteur en droit, Chercheur associé au CESICE (Université de Grenoble) Chercheur associé au CREOGN

« En cette époque de nouveaux défis partout dans le monde, nous renforçons notre action au sein de l'Union européenne afin de lutter contre les menaces hybrides, que ce soit dans le domaine cyber, de la désinformation ou du contre-espionnage » [1]. Ces propos de la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, Federica Mogherini, dans sa déclaration du 13 juin 2018 dans le sillage de l'attaque de Salisbury, soulignent la détermination de l'Union pour contrer ce type de menace, devenue pour elle une préoccupation de premier plan. Les menaces hybrides sont entendues comme : « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques),

(1) Commission européenne, Communiqué de presse intitulé « Une Europe qui protège : l'UE s'emploie à développer la résilience et à mieux lutter contre les menaces hybrides », Bruxelles, le 13 juin 2018, IP/18/4123.

susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement soit dépassé ».[2]

(2) Communication de la Commission du 13 juin 2018 sur le rapport conjoint sur la mise en œuvre du cadre commun en matière de lutte contre les menaces hybrides de juillet 2017 à juin 2018 (COM JOIN 2018) 14 final).

Or, menaces hybrides, cyberespace et *fake news* sont intiment liés. Les nouvelles modalités d'attaques russes ne correspondent pas aux nomenclatures établies de l'action cybernétique telles qu'elles ont été théorisées pendant plusieurs années en Europe et aux États-Unis : la Russie a investi le cyberespace comme un lieu de confrontation et les actions qu'elle mène se traduisent par des campagnes cybernétiques offensives[3]. Certaines ont été largement médiatisées lors de l'évocation d'ingérences dans la campagne présidentielle américaine de 2016[4]. L'action se traduit d'un côté par des opérations de désinformation, par la propagation d'informations trompeuses ou absolument fausses et de l'autre, par des opérations de décrédibilisation au travers d'actions sur des cibles symboliques en usant par exemple des fuites de documents[5].

(3) Limonier, K, Colin, G., « Guerre hybride russe dans le cyberespace », *Hérodote*, vol. 166/167, n° 3-4, 2017, p. 145-146.

(4) Sur cette question, voir Troude-Chastenet, P.

(5) Limonier, K, Colin, G., *op. cit.*, p. 156.

Face à cette situation, l'Union a déployé deux types de stratégies complémentaires : une action spécifique à la gestion des menaces hybrides et une autre, plus générale, contre la désinformation en ligne. À ce sujet, la lutte contre les *infox* fait l'objet d'une attention particulière. Elles sont définies comme des « informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public » [6]. Une communication, du 26 avril 2018, rappelle que le Forum économique mondial avait listé la désinformation en ligne comme étant l'une des dix principales tendances des sociétés modernes. Elle souligne que l'exposition des citoyens européens à une désinformation à grande échelle menace la cohérence de la société par un phénomène de « ségrégation de la vérité » [7] (à savoir la polarisation des opinions publiques, c'est-à-dire la cristallisation de points de vue irréconciliables conjuguées à l'affaiblissement des instances politiques et sociales de régulation).

(6) p. 4 de la communication de la Commission du 26 avril 2016 intitulée « Lutter contre la désinformation en ligne : une approche européenne » (COM(2018)236).

(7) Halévi, R. *op. cit.*, p. 41.

Le défi posé par la désinformation en ligne dans le cadre du processus électoral

Le contrôle de la couche sémantique

revêt un aspect crucial dans la lutte contre la désinformation. Depuis quelques années à présent, ce contrôle tend à s'organiser autour de la préservation du caractère loyal et impartial des processus électoraux, qu'ils soient nationaux ou européens.

Les campagnes de désinformation à grande échelle constituent une source d'inquiétude pour l'Union européenne et ses États membres. Comme le précise la communication conjointe de juin 2018[8], la prolifération des *fake news* est un danger, car non seulement elle empêche les citoyens de prendre des décisions en connaissance de cause et de prendre part pleinement au processus démocratique, mais de surcroît, elle répand la méfiance et attise les tensions sociétales. Or, l'exposition des citoyens européens à la désinformation est grandissante, les campagnes électorales étant particulièrement visées comme en témoigne le scandale concernant *Facebook/Cambridge Analytica*. C'est la raison pour laquelle, après avoir établi fin 2017 un groupe d'experts à haut niveau, la Commission européenne a présenté, le 26 avril 2018, sur la base des conclusions de ce groupe une communication recensant les mesures à prendre pour endiguer ce phénomène[9].

(8) Communication conjointe du 13 juin 2017 intitulée « Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide » (JOIN(2017)450 final).

(9) Communication d'avril précitée.

Face à cela, diverses mesures sont préconisées, comme :

1 - L'instauration d'un réseau européen indépendant de vérificateurs de faits, chargé de partager des bonnes pratiques dans ce domaine, qui disposera à l'avenir d'une plateforme européenne en ligne sécurisée.

2 - L'établissement d'un code européen de bonnes pratiques contre la désinformation à l'attention les plateformes en ligne afin, notamment, d'entreprendre plus efficacement de fermer les faux comptes.

3 - Le lancement d'un Forum plurilatéral sur la désinformation. Réunissant les professionnels du secteur concerné, celui-ci constitue le pendant du Forum de l'Union européenne sur l'Internet (chargé de la lutte contre la propagande terroriste en ligne) sur les questions des *fake news*. Il s'est réuni le 29 mai 2018 et a adopté, le 17 juillet 2018, le code de bonnes pratiques destiné aux plateformes en ligne. Facebook, Google et Twitter. Mozilla de même que des annonceurs et le secteur de la publicité ont adhéré à ce code.

Le contrôle de la couche sémantique, un moyen de lutter contre la désinformation

Cette action spécifique de lutte contre la désinformation se développe et se

structure depuis lors. Le 12 septembre 2018, la Commission adopte un train de mesures visant à renforcer la résilience des systèmes électoraux.

Un plan d'action conjoint de lutte contre la désinformation est présenté en décembre 2018[10].

(10) Rapport du 14 juin 2019 de la Commission sur la mise en œuvre du plan d'action contre la désinformation (JOIN(2019) 12 final).

Au cours de ce mois-ci, se tient la deuxième réunion du réseau de coopération en matière d'élections au niveau européen. Ce réseau, qui réunit des points de contact des réseaux électoraux nationaux, vise à lutter contre la campagne de désinformation en assurant la surveillance et le respect des règles dans le contexte électoral, en promouvant la cyber-résilience, et en échangeant des bonnes pratiques sur les éventuels problèmes détectés.

Le mois suivant, conformément au plan d'action de décembre 2018, un système d'alerte rapide vise à faciliter l'échange d'informations entre les institutions de l'UE et les États membres. L'objectif est d'améliorer la circulation des informations sur les campagnes identifiées et de fournir des réponses coordonnées. Ce système est évalué par la présentation conjointe de la haute représentante et de la Commission, à l'automne 2019 en vue de renforcer son fonctionnement.

Une communication conjointe de ces instances est présentée peu après la tenue des élections européennes, qui porte sur la mise en œuvre du plan d'action contre la désinformation. Ce texte, du 14 juin 2019, tire un premier bilan de l'analyse du niveau et l'incidence de la désinformation dans le processus électoral au regard des mesures prévues par le plan. D'après lui, il est positif car il a « contribué à dissuader des attaques et à révéler au grand jour des activités de désinformation ». Il relève qu'« Encouragés par ces actions, de nombreux journalistes, vérificateurs de faits, plateformes, autorités nationales, chercheurs et acteurs de la société civile ont contribué à sensibiliser le public à la manière de contrer la menace. La sensibilisation accrue de la population a compliqué la tâche des acteurs malintentionnés désireux de manipuler le débat public » [11].

(11) p. 2 du rapport du 14 juin 2019 de la Commission sur la mise en œuvre du plan d'action contre la désinformation (JOIN(2019) 12 final).

Un chantier institutionnel en cours et des efforts à poursuivre

Les résultats des efforts menés par les plateformes sont néanmoins en demi-teinte. D'après un rapport de la Commission présenté en juillet 2019[12], il est précisé qu'elles ont pris un ensemble de mesures pour lutter contre la désinformation. Sur base des rapports fournis par Google, Twitter et Facebook,

(12) Dix-neuvième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective (COM(2019) 353 final).

présentés conformément au code de bonnes pratiques, elles ont fait le nécessaire, avant la tenue des élections au Parlement européen, pour signaler aux utilisateurs le caractère politique des publicités diffusées par elles. Pour autant, ce même document identifie des marges d'amélioration, notamment la possibilité pour les chercheurs d'avoir accès aux données brutes détaillées dans le cadre de leurs travaux effectués sur le phénomène de désinformation.

Toujours concernant ce code, la Commission est actuellement en train de procéder à son évaluation globale. Dans l'hypothèse d'une mise en œuvre insatisfaisante, elle envisage une mesure législative. Cette démarche rappelle celle qui concerne la diffusion en ligne de contenus à caractère terroriste. Au regard des résultats insatisfaisants de sa recommandation à ce sujet, elle avait présenté, le 19 septembre 2018, une proposition de règlement, c'est-à-dire un texte de droit contraignant, destiné à pouvoir imposer une série d'obligations aux plateformes, susceptibles d'être juridiquement sanctionnées.

Le contrôle de la couche sémantique entend combattre et prévenir les cybermenaces et la désinformation dans le contexte électoral. La question de ce contrôle n'est cependant pas nouvelle. La lutte contre le racisme avait conduit l'Union à se doter, dans les années 2000, d'un arsenal juridique approprié pour lutter contre l'essor de propos illicites sur les blogs. L'effort de l'Union consistait à faire converger les normes sur cette question de manière à rendre la répression effective.

Pour autant, cette thématique du contrôle est devenue une priorité, notamment au regard du recours par Daesh aux plateformes numériques afin de promouvoir ses idées, recruter de nouveaux combattants et susciter de nouvelles vocations. La lutte contre la propagande terroriste en ligne s'effectue toujours au nom de la lutte contre les contenus illicites. En témoigne cette proposition du 19 septembre 2018, qui prévoit notamment l'obligation faite aux plateformes de retirer dans un délai d'une heure un contenu terroriste, après réception d'une injonction de suppression par une autorité nationale.

Un contrôle de cette couche étroitement lié à la gestion des menaces hybrides

Les chefs d'État et de gouvernement font du contrôle de la couche sémantique une priorité dans leurs conclusions du 21 juin 2019. Au sein d'une rubrique intitulée « désinformation et menaces hybrides »[13], le Conseil européen considère que « le caractère évolutif des menaces et le risque

(13) p. 2 du doc. du Conseil du 20 juin 2019, n° EUCO 9/19.

croissant d'ingérence malveillante et de manipulation en ligne associés au développement de l'intelligence artificielle et des techniques de collecte de données requièrent une évaluation continue et une réponse appropriée ». Ils saluent l'annonce de la Commission d'opérer une évaluation approfondie de la mise en œuvre des engagements pris par les différents signataires du code de bonnes pratiques. À cet égard, les progrès en matière d'intelligence artificielle, notamment en ce qui concerne le *Deep fake*, fait craindre le déroulement récurrent de campagnes massives de désinformation, instrumentalisées par des puissances étrangères. En effet, l'essor de cette nouvelle technologie permettant la génération de fausses vidéos au moyen des outils de l'apprentissage profond, ouvre de nouvelles perspectives en matière de corruption des systèmes électoraux et de déstabilisation de la vie démocratique. À l'heure actuelle, la Haute représentante et la Commission travaillent conjointement en vue d'une part, de mettre sur pied une méthodologie commune visant à analyser et à mettre en lumière les campagnes de désinformation, et d'autre part, de renforcer les partenariats avec des partenaires internationaux, tels que le G7 et l'OTAN.

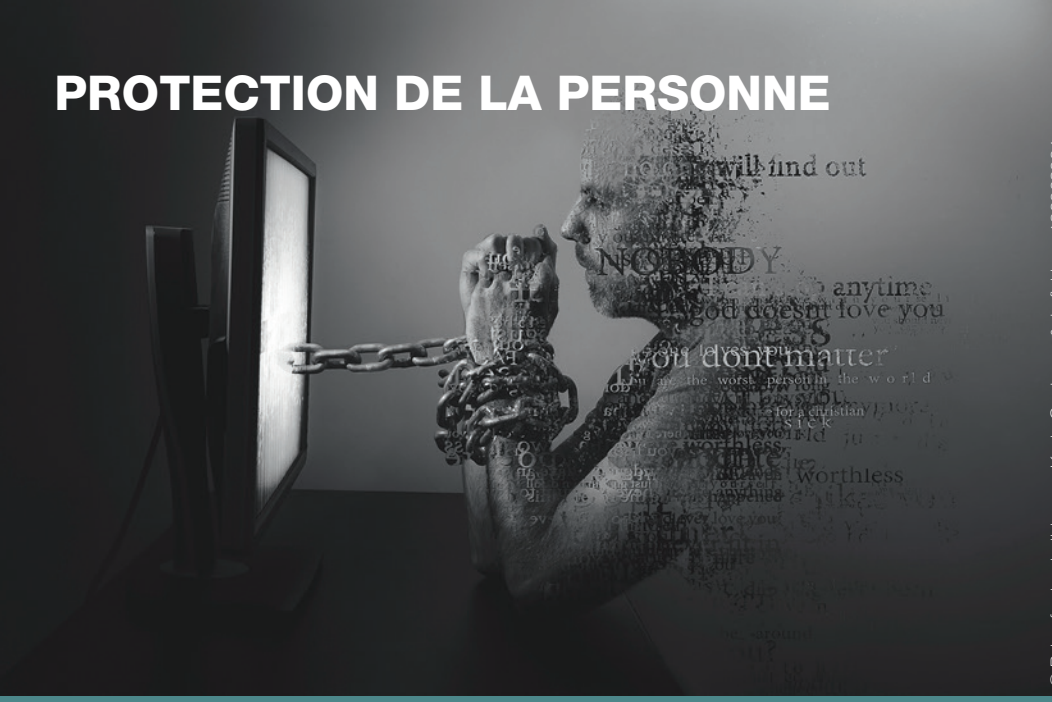
En conclusion, la lutte contre les *infox* est devenue le laboratoire d'un approfondissement de la construction européenne dans un domaine entièrement nouveau. Il importe de noter que ces efforts se conjuguent avec ceux menés sur le plan international, notamment par le Réseau international de vérification des faits (qui travaille étroitement avec le réseau européen indépendant de vérificateurs de faits) et l'OTAN qui apporte son soutien au centre européen d'excellence spécialisé dans la gestion des menaces hybrides[14].

(14) Ce centre est composé d'universitaires et de fonctionnaires spécialistes d e la question de la riposte aux campagnes de désinformation. Il est chargé de la conduite d'un dialogue au niveau stratégique et du lancement de travaux de recherches. Situé à Helsinki, il a également pour mission d'assurer et rapprochement public-privé afin de mettre au point de nouvelles technologies de nature à permettre de lutter efficacement contre ce type de menaces.

L'AUTEUR

Pierre BERTHELET est docteur en droit et chercheur associé au CESICE (Université de Grenoble) / au CERIC (Université de Marseille/Aix-en-P.) et au CREOGN (Gendarmerie - Melun). Il est membre du Comité de rédaction des Cahiers de la sécurité et de la justice, de la communauté d'experts du Conseil Supérieur de la Formation et de la Recherche Stratégiques (CFSRS) ainsi que de l'Association française du droit de la sécurité et de la défense (AFDSD). Il a effectué un postdoctorat à la Haute École internationales (HEI) à l'Université Laval (Québec) relatif à l'accord de sécurité UE-Canada sur le transfert de données passagers aériens et il a écrit plusieurs ouvrages dont un en lien avec le thème de l'article : Chaos International et sécurité globale. La sécurité en débats, (EPU, 2014).

PROTECTION DE LA PERSONNE



© Pain of cyber bullying par Kevin Carden - n° de fichier : 182068024

LA MANIPULATION PAR LA GESTION DE L'ÉMOTION

Les interactions virtuelles confèrent un anonymat et peuvent cacher la motivation subjacente d'une communication. Les utilisateurs créent des réalités au travers d'énoncés à la validation incertaine. La fugitivité et la circonstance de l'échange confine alors à une communication émotive. Les réactions se transforment en productions soigneusement formulées. Cette mise en scène des émotions a parfois pour objectif de manipuler un ou plusieurs interlocuteurs en les fascinant ou en les terrorisant. Cela peut donner un champ aux stratégies discursives des mouvements terroristes qui mettent en œuvre, lors de l'approche de sympathisants potentiels, des scénarios susceptibles de susciter une certaine émotion. Interagissant directement avec son interlocuteur, un manipulateur construit une relation sémantique basée sur un chevauchement d'émotions positives ou négatives articulées sur l'appartenance à une communauté, une relation à l'évènement ou une fascination quant à une imagerie culturelle. L'article de Laura Ascone explore ce champ cognitif peu approché de manière scientifique.

Le recours aux émotions
dans le cyberespace : entre stratégie discursive et manipulation

Par Laura Ascone

Souvent accusé de déshumaniser les relations interpersonnelles, le cyberespace est en réalité le théâtre de nouvelles formes d'expression des émotions. Les réactions émotionnelles, qui sont par nature spontanées, se transforment ici en productions soigneusement formulées. Cette mise en scène des émotions a parfois pour objectif de manipuler un ou plusieurs internautes, que ce soit en les fascinant ou en les terrorisant.

Émotions et cyberespace

LAURA ASCONE

Docteure en Sciences du Langage

L'ouverture au cyberespace et les nombreuses innovations dans la communication ont inévitablement modifié la façon dont l'individu se rapporte au monde et à ceux qui l'entourent. Plus particulièrement, ce sont les notions de temps et d'espace qui ont changé dramatiquement. Dans le cyberespace, la communication médiée par les réseaux a son propre axe du temps. Malgré une apparente instantanéité, les interactions *virtuelles* ne sont pas aussi temporellement fluides que les interactions *réelles*. Si un utilisateur doit attendre que son interlocuteur rédige et envoie le message, l'autre doit attendre que le message soit lu avant de recevoir une réponse. Cependant, les deux utilisateurs ne semblent pas percevoir ce décalage temporel. De même, les interactions *virtuelles* se distinguent des interactions *réelles* sur le plan spatial. Bien que l'utilisateur se trouve face à l'ordinateur dans le monde réel et que les messages soient visibles sur l'écran, les interlocuteurs ne partagent pas le même espace[1].

(1) Kramsch, C. G. (2009). *The Multilingual Subject: what foreign language learners say about their experience and why it matters.* Oxford University Press.

La spontanéité des émotions mise à l'épreuve

Le décalage spatio-temporel, qui caractérise les interactions *virtuelles*, donne la possibilité aux utilisateurs de cacher leur identité ainsi que la motivation subjacente à la communication. Autrement dit, les utilisateurs peuvent créer tout type de réalité et d'identité à travers des énoncés plus ou moins véridiques. En outre, ce décalage influence fortement la façon dont les interlocuteurs interagissent et expriment leurs émotions. Dans le cyberespace, lorsque l'utilisateur a une réaction émotionnelle et qu'il veut la communiquer à son interlocuteur, il tiendra automatiquement compte du contexte dans lequel il est en train de s'exprimer. Il aura donc tendance à moduler l'expression de ses émotions selon son interlocuteur, le type de conversation qu'il est en train de mener et le moyen de communication employé. En outre, la modulation des réactions émotionnelles influence indirectement les réactions de l'interlocuteur et, par conséquent, la conversation même. En d'autres termes, décider de la manière d'exprimer une émotion signifie décider comment agir sur l'interlocuteur, sur la communication et sur l'environnement. Plus particulièrement, l'utilisateur agit sur l'interlocuteur car l'interprétation et la réaction de ce dernier dépendent principalement de la façon dont l'émotion a été exprimée. Kramer *et al.*[2] ont montré comment une émotion exprimée sur *Facebook* influence les émotions des autres utilisateurs. L'exposition à un nombre important de messages positifs amènera les utilisateurs à publier des messages positifs.

(2) Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24), 8788-8790.

Manipulation et recours aux émotions

L'expression des émotions joue donc un rôle crucial dans toute interaction, qu'elle soit *réelle* ou *virtuelle*. Quand l'utilisateur interagit dans le cyberespace, les émotions qu'il ressent se dissipent instantanément, avant qu'il n'ait le temps de les exprimer par écrit. Cette caractéristique vient du fait que les émotions ne durent que quelques millisecondes. Par conséquent, l'utilisateur pourra, plus ou moins volontairement, décider comment verbaliser ses réactions émotionnelles. Ne s'agissant donc plus de l'expression d'une réaction spontanée, la communication *virtuelle* peut être considérée comme une communication émotive. Contrairement à la communication émotionnelle, où l'individu exprime son émotion à l'instant même où il la ressent, la communication émotive est caractérisée par la description de l'émotion une fois qu'elle s'est dissipée[3]. En d'autres termes, la communication émotive se rapproche davantage des notions de performance, de rhétorique et de persuasion[4]. Les émotions peuvent donc

(3) Plantin, C. (2011). *Les bonnes raisons des émotions.* Peter Lang Publishing Group.

(4) Arndt, H., & Janney, R. W. (1991). Verbal, prosodic, and kinesic emotive contrasts in speech. *Journal of pragmatics*, 15(6), 521-549.

être mises en scène afin d'influencer les réactions et le comportement de l'interlocuteur. Le discours de propagande terroriste diffusé dans le cyberespace constitue un exemple évident de cette exploitation, plus ou moins subtile, de l'expression des émotions.

Émotions et propagande terroriste

Le lien entre le discours de propagande terroriste et les émotions peut être retrouvé dans le nom latin *terror*. Ce terme vient de la racine indoeuropéenne ter-, qui veut dire « trembler » et qui marque donc le lien entre le terrorisme et la peur[5]. Le discours djihadiste témoigne de la proximité entre l'action terroriste et la peur. Le 4 juillet 2014, jour où le califat a été réinstauré, Abu Bakr Al-Baghdadi a affirmé qu'il fallait « revenir à l'Islam des premiers âges pour obtenir le pardon d'Allah et retrouver la fierté arabe en inspirant la peur aux infidèles et aux mauvais musulmans ». Autrement dit, selon le leader de Daesh, il importe d'inspirer la peur plus que de tuer les infidèles et les mauvais musulmans. En ce qui concerne le discours propagandiste diffusé dans le cyberespace, la revue djihadiste *Dar al-Islam* constitue une source d'analyse cruciale. Elle nous permet de mieux comprendre les stratégies discursives employées par Daesh. Diffusée à partir du 23 décembre 2014, *Dar al-Islam* compte dix numéros et s'adresse à un public qui a déjà adhéré à l'idéologie djihadiste. Ne s'agissant pas d'une interaction, la revue ne peut pas moduler son discours selon l'interlocuteur. L'éditeur doit donc tenir compte des différents profils qui peuvent avoir accès à ce contenu. Bien que l'expression des émotions joue un rôle central dans le discours propagandiste, il est possible de constater que les émotions sont rarement exprimées directement. Au contraire, l'énonciateur recourra à des scénarios susceptibles de susciter une certaine émotion. Discours et images contribuent ainsi à la mise en scène des émotions afin de renforcer l'adhésion à l'idéologie djihadiste. Si l'exaltation du groupe djihadiste vise à nourrir l'amour pour cette communauté, la condamnation de l'ennemi a pour objectif d'alimenter la haine contre celui-ci.

(5) Di Cesare, D. (2017). *Terrore e modernità*. Torino: Giulio Einaudi Editore.

Émotions et embrigadement

Le discours djihadiste dans le cyberespace ne circule pas seulement à travers des revues officielles. Les réseaux sociaux constituent également des vecteurs de la propagande djihadiste. Contrairement à *Dar al-Islam*, les interactions sur les réseaux sociaux s'adressent à un public qui est en voie de radicalisation. Par conséquent, l'expression des émotions vise à influencer l'interlocuteur afin qu'il adhère à l'idéologie promue. Le clip *Ils te disent*, produit par le gouvernement pour contrer la radicalisation djihadiste dans le cyberespace, montre un exemple de cette manipulation. Après avoir regardé le profil *Facebook* de plusieurs djihadistes, le protagoniste de la vidéo reçoit un message :

1. Salut
Cool les trucs que tu like,
ça t'intéresse ce ki se passe
au Cham en ce moment ?

si ta des questions hésite pas,
la vérité elle est la bas, c'est maintenant
qu'il faut partir !

si tu me donnes ton num j'ai des amis
la bas ki se battent jte met en contact.

Bien qu'il s'agisse d'une reproduction, ce message montre le caractère anxiogène des messages envoyés par des recruteurs. Interagissant directement avec son interlocuteur, l'embrigadeur peut facilement moduler son discours. Il peut également créer une identité *ad hoc* grâce à la nature du cyberespace : la perception que l'on a d'un individu se construit principalement sur les informations que cet individu nous transmet[6]. Le choix de nombreux djihadistes d'utiliser une photo de lion comme photo de profil sur *Facebook* vise à les montrer comme des personnes fortes et courageuses. L'internaute, qui aura tendance à oublier et à se détacher du monde réel qui l'entoure, finira par percevoir comme vrai et réel tout ce qui se passe dans le cyberespace. Ben-Ze'ev[7] définit ce phénomène *detattachment* (« détattachement »). Malgré la distance spatio-temporelle, l'utilisateur ressent un sentiment d'attraction et établit une sorte de relation avec son interlocuteur. L'objectif de cette manipulation d'émotions est de couper l'individu de son entourage réel pour qu'il ne ressente plus d'émotions envers ses proches. De même, à travers l'exposition à des contenus violents, l'embrigadeur djihadiste vise à habituer sa cible à la violence et qu'elle n'ait plus peur de mourir. Autrement dit, l'embrigadeur se sert des émotions pour que la cible ne les ressente plus.

(6) Mantovani, G. (2002). Internet haze: why new artifacts canenhance situation ambiguity. *Culture and Psychology* 8, 307–326.

(7) Ben-Ze'ev, A. (2005). 'Detattachment': the unique nature ofonline romantic relationships. In Y. Amichai-Hamburger (ed.), *The social net: Human behavior incyberspace*, 115–138. New York: Oxford UniversityPress.

© Man reading Quran - par fotofabrika

Le discours suscite des réactions émotionnelles positives et négatives qui peuvent s'alimenter autour d'une appartenance communautaire et du rejet d'un adversaire.

Combinaison paradoxale des émotions dans le discours djihadiste

Bien que le lien entre terrorisme et peur soit évident, le discours terroriste djihadiste ne s'articule pas seulement autour de la peur et des autres émotions négatives. Visant à fasciner aussi ses sympathisants, le discours djihadiste recourt également aux

émotions positives. Réactions émotionnelles positives et négatives s'articulent donc au sein d'un même discours. Dans certains cas, deux sentiments[8] opposés s'alimentent l'un à l'autre. La haine contre l'ennemi mécréant alimente l'amour envers la communauté djihadiste. Et inversement, l'amour pour la communauté alimente la haine contre l'ennemi. Ce chevauchement d'émotions positives et négatives peut émerger aussi en relation à un événement. Une attaque terroriste menée sur le sol occidental suscitera chez la communauté djihadiste des réactions positives telles que la joie, la fierté et de l'adrénaline. En outre, la même attaque pourra susciter des réactions positives aussi au sein de la communauté visée. Les attentats perpétrés sur le sol français, par exemple, ont réveillé des sentiments de solidarité et d'amour.

(8) Contrairement aux émotions, qui ne durent que quelques millisecondes, les sentiments ont une durée plus importante. Ekman (1992) identifie six émotions primaires : joie, peur, colère, surprise, tristesse et dégoût.

Une approche d'analyse des émotions dans le cyberespace

Ce panorama synthétique de l'expression des émotions dans le cyberespace a révélé des éléments qui nécessitent d'être pris en compte lorsque l'on s'apprête à examiner le discours djihadiste diffusé sur Internet. Tout d'abord, il est important d'analyser un texte dans son contexte. Il s'agit donc de considérer le moyen de communication employé et l'impact que ce dernier peut avoir sur le discours, les événements auxquels les interlocuteurs peuvent faire référence, et le point de vue des différents utilisateurs qui participent à la conversation. Plus particulièrement, ce dernier point permet de déterminer si un message exprimant une émotion positive est réellement un contenu positif ou si, au contraire, l'objet de telle émotion constitue un potentiel danger pour la communauté.

En outre, il est nécessaire de considérer que notre discours est imprégné de nos impressions même lorsque l'on n'exprime pas directement nos émotions[9]. Par conséquent, afin d'analyser la radicalisation djihadiste à travers l'expression des émotions dans le cyberespace, nous ne pouvons pas limiter l'étude à l'analyse des émotions uniquement négatives. De même, comme nous l'avons montré, il est important d'étudier non seulement l'expression des émotions, mais aussi comment l'énonciateur suscite, à travers son discours, des réactions émotionnelles chez son interlocuteur.

(9) Shaver, P., Schwartz, J., Kirson, D., & O'connor, C. (1987). Emotion knowledge: further exploration of a prototype approach. Journal of personality and social psychology, 52(6), 1061.

L'AUTEURE

Docteure en Sciences du Langage, Laura Ascone a réalisé sa thèse sur « la radicalisation à travers l'expression des émotions sur Internet » à l'Université Paris Seine. Actuellement, elle effectue un post-doctorat à l'Université de Lorraine dans le cadre d'un projet ANR sur les discours de haine contre les migrants. Ses recherches portent sur l'expression des émotions sur les réseaux sociaux, la propagande djihadiste et le contre-discours, et les messages haineux contre les migrants.

PROTECTION DE LA PERSONNE

ESPACE SÉMANTIQUE ET RÉVOLUTION ANTHROPOLOGIQUE

Les avancées informatiques s'accompagnent d'une révolution anthropologique qui conditionne de celle de nos usages et de nos modèles sociaux. Au sein du cyberespace, la sphère sémantique est un enjeu crucial. Elle est un facteur d'essor économique pour les géants du numérique mais elle touche également aux domaines de la sécurité et de la défense. Les réseaux sociaux et commerciaux permettent à des opérateurs d'exploiter les données personnelles des utilisateurs mais également d'agréger leurs pratiques numériques et sociétales. Des méthodologies permettent ensuite d'affiner un criblage économique et politique des populations. En conséquence, la donnée est devenue une cible que l'on peut acquérir ou pervertir selon les motivations des groupes ou des États qui ont les moyens de s'en emparer légalement ou illégalement.

La sphère sémantique recouvre également une transformation des modes de connaissance, standardisés au travers de grands prestataires, qui façonne la pensée. L'exploitation de la donnée intègre des techniques qui visent à atteindre spécifiquement les cerveaux. Les atteintes à l'information et à l'entendement des citoyens par les Fake-news et autres orientations falsifiées ou orientées des données montrent toute l'importance de l'espace sémantique dans une logique géostratégique et politique.

Les enjeux
de la couche sémantique

Par Olivier Kempf

Une analyse classique du cyberespace le décrit en trois couches. Une couche physique est constituée de tous les matériels nécessaires à son fonctionnement : ordinateurs, câbles (terrestres ou sous-marins), antennes (WiFi, 4G, …), satellites, serveurs, fermes de données, clefs USB voire cartes bleues… Une couche logique comprend tous les logiciels, codes et protocoles qui permettent à ce cyberespace de fonctionner et de communiquer en réseau.

OLIVIER KEMPF

Docteur en science politique
Chercheur associé à la fondation pour la recherche scientifique (FRS)

Enfin, une couche sémantique ou informationnelle, recèle l'ensemble des données et informations qui transitent par ce cyberespace. Au départ, les spécialistes du numérique et du cyberespace se sont surtout concentrés sur la couche logique. Pour beaucoup encore, le cyber réside d'abord dans la capacité à la maîtriser alors que les enjeux portent actuellement sur la couche sémantique.

D'un point de vue économique, l'avantage concurrentiel résidait dans le contrôle d'un service informatique constitué de lignes de codes. Les premiers géants de l'informatique, avant même l'ère de l'Internet, fonctionnaient selon cette logique notamment si nous faisons référence à la lutte entre Microsoft et Apple (Windows contre MacOS), au cours des années 1980.
Il y avait également une lutte sur la couche matérielle, que ce soit du côté des puces (Intel) ou du côté des machines, qu'elles soient de bureau (les PC contre les Macintosh) ou des serveurs.
L'arrivée d'Internet au cours des années 1990 n'a pas fondamentalement changé cette perception. La lutte se déroulait alors

entre des acteurs comme AOL, Yahoo ! Nestcape, E-Bay et Amazon qui tinrent le haut du pavé jusqu'au milieu des années 2000. On assista alors au développement de nouveaux acteurs, comme Google ou Facebook, ce dernier jouant sur le nouveau registre des réseaux sociaux. Notons au passage que les fameux GAFA (voire GAFAM en incluant Microsoft, née en 1975) comprennent des sociétés qui ont été fondées en 1976 (Apple), 1994 (Amazon), 1998 (Google) ou 2004 (Facebook). Hormis Apple, les géants informatiques d'aujourd'hui agissent principalement sur la couche logique, du moins en apparence. En effet, une grande partie de la richesse contemporaine des géants du numérique, qu'ils soient américains ou chinois (les BATX : Baidu, Alibaba, Tencent et Xiaomi), qu'ils soient anciens (les GAFA) ou plus récents (les NATU : Netflix, AirBnB, Tesla, Uber), tient à une certaine maîtrise de la couche sémantique. Par ailleurs, le développement des infox (*Fake news*) et les débats sur la post-vérité et les manipulations de l'information participent à cette montée en puissance de la couche sémantique dans l'appréciation du cyberespace et notamment de ses enjeux stratégiques.

La couche sémantique appartient bien au cyberespace

On pourrait considérer qu'il y a d'un côté un cyberespace, réduit à ses deux premières couches, de l'autre un espace informationnel, qui serait totalement décorrélé. Cela reviendrait à revenir à des notions anciennes comme celle de *guerre de l'information* ou, en remontant plus dans le temps (Guerre froide), comme celle de *propagande* ou de *guerre psychologique*. Cette approche ne tient cependant pas compte du phénomène technique qui accompagne le cyberespace. Les formes anciennes de manipulation de masse tenaient compte d'un système médiatique « à l'ancienne », fondé sur le triptyque du journal imprimé, de la radio et de la télévision. Le contrôle des appareils médiatiques était envisageable, que ce soit par un biais technique ou par un biais financier. Surtout, ces médias traditionnels avaient le monopole de l'information.
La grande vague de ce qu'on a appelé, au milieu des années 2000, le web 2.0 tient à la vogue des blogs et autres réseaux sociaux : désormais, tout un chacun peut émettre une opinion audible au-delà du simple café du coin. Surtout, la quatrième vague de la révolution informatique qui nous emporte depuis le milieu des années 2010 est celle de l'ordiphone (*smartphone).* Comparez ainsi les photos[1] de l'élection de Benoit XVI à celle du pape François : en 2005, la foule est devant la place Saint-Pierre regarde ce qui se passe et attend de voir s'il y a une fumée blanche ou noire. Huit ans plus tard, la même foule brandit des écrans d'ordiphones ou de tablettes qui tous immortalisent l'événement, sachant que les chaînes

(1) Photo chargée sur https://www.tuxboard.com/election-de-benoit-xvi-vs-election-de-francois/

de télé du monde entier ont de bien meilleures images à diffuser.

© Nbc News / Olivier Kempf

Ainsi, le cyberespace a entraîné une révolution anthropologique fondamentale. Il ne s'agit pas simplement de technique mais aussi de pratiques et d'usages. C'est bien pour cela que la couche sémantique a pris une place si importante et qu'elle apparaît pleinement dans le cyberespace et dans tous les enjeux associés de défense et de sécurité. Il paraît donc erroné de séparer un soi-disant espace informationnel du cyberespace.

La donnée, l'énergie du XXIe siècle

La couche sémantique est en effet celle où réside la donnée. Sans ouvrir la discussion sur ce qu'elle est, la question de la distinction de la métadonnée de la donnée brute, par exemple, n'ayant pas reçu de réponse claire et partagée, ni celle sur la distinction entre donnée, formation et connaissance, nous constatons que cet ensemble constitue l'essentiel de la couche sémantique. Observons alors les GAFA pour comprendre que leur vrai modèle économique ne tient pas à leur spécialisation apparente (ici un moteur de recherche, là un téléphone mobile avec son magasin d'applications, ici un réseau social rassemblant des « amis », là un magasin par correspondance) mais à l'exploitation des données de leurs utilisateurs. Leur puissance tient au nombre incroyable de données récoltées auprès d'un très grand nombre d'usagers et selon leurs pratiques numériques. Le couplage de ces deux catégories de données permet d'effectuer un ciblage des comportements extrêmement pointu qui nourrit la vraie ressource économique de ces GAFA, à savoir la publicité associée. Les GAFA sont d'abord des régies publicitaires.

Ces dernières années, le secteur des technologies de l'information a beaucoup discuté des notions d'intelligence artificielle, de *blockchain*, de réalité augmentée, *etc.* Une notion a perdu de sa vogue, celle de données massives (*Big Data*). Or, il faut comprendre que ces données massives constituent, encore aujourd'hui, la principale dynamique des nouvelles puissances que nous observons. Facebook compte 2 milliards d'abonnés et sa population est donc supérieure à celle de la Chine ou de l'Inde. En décembre 2017, le chiffre

d'affaire était de 40 milliards de dollars, soit le 96e rang mondial, devant la Tunisie ou l'Estonie, et supérieur au budget français de la défense. GAFA et BATX sont en train de devenir des nouvelles puissances géopolitiques qu'on ne peut plus ignorer, en comprenant que leur puissance vient de la donnée. D'ailleurs, ces puissances envisagent d'aller plus loin et de développer de nouveaux « services », autrefois l'apanage des États : il en est ainsi du projet de cryptomonnaie Libra, justement proposé par Facebook et un consortium de 28 entreprises mondiales.

En fait, la donnée apparaît comme une nouvelle énergie. Nous avons connu par le passé le charbon, le pétrole, le nucléaire, avec toutes les révolutions économiques et militaires associées. La donnée constitue l'énergie de cette première moitié de XXIe siècle.

La donnée est une cible

Logiquement, la donnée devient une cible de choix qu'il s'agisse de l'acquérir ou de la pervertir.

On peut l'acquérir de manière légale (ce que font tous les GAFA mais aussi tous les acteurs économiques conscients des enjeux et ayant compris que la maîtrise des données était une source de supériorité durable) ou illégale, ce que font la plupart des cybercriminels lorsqu'ils effectuent la première action de toute cyberagression relative à l'espionnage. Or, on réduit trop souvent la cybercriminalité au sabotage qui est pourtant mineur par rapport à l'espionnage ou même à la subversion.

La donnée, ou une donnée enrichie que l'on peut désigner par le terme d'information, peut également être pervertie. C'est par exemple le cas, lorsqu'après une intrusion un agresseur crypte toutes vos données et vous demande une rançon pour pouvoir y accéder (technique du rançonnage – *ransomware*). Ce peut-être également le cas quand un agresseur effectue un défacement de site où l'apparence usuelle de la page est remplacée par un slogan ou par une illustration malfaisante.

Les sociétés Thalès et Verint ont publié en octobre un rapport sur le cybercrime[2]. Après avoir étudié nombre d'organisations cybercriminelles, elles ont dégagé quatre types principaux d'acteurs : les États-Nations, les *hacktivistes*, les cybercriminels et les terroristes. Ils distinguent ces catégories par leurs motivations, plus que par leurs méthodes. Ainsi, les États-nations sont mus par l'espionnage, la déstabilisation politique et le sabotage. Les *hacktivistes* mettent en avant leur idéologie (communautaire, religieuse, politique), la dénonciation de faits jugés inacceptables et l'atteinte à l'image. Les cybercriminels sont attirés par le gain financier. Les terroristes visent le prosélytisme et la destruction de données.

(2) https://www.thalesgroup.com/fr/group/journaliste/press-release/cyberthreat-handbook-thales-et-verint-presentent-leur-whos-who-des 7 octobre 2019.

Sans discuter le bien-fondé de cette répartition, nous constatons qu'à chaque fois, la donnée est soit une cible qu'il faut acquérir, soit qu'il faut affecter. Mais cette répartition laisse aussi entrevoir une autre motivation.

Changer les esprits

En effet, comme nous l'avons remarqué, ce qui caractérise le cyberespace est son omniprésence sociale. Chacun peut s'exprimer (et donc chacun est un émetteur ou un relais), mais chacun, plus que jamais, peut recevoir des informations, en quantité absolument astronomique. Les plus anciens des lecteurs se souviennent de l'encyclopédie *Universalis*: on ne la trouvait qu'en bibliothèque et personne n'avait cela chez soi. On trouvait des succédanés plus populaires, qu'il s'agisse jadis du dictionnaire encyclopédique *Larousse* ou du *Quid* annuel, que l'on trouve désormais tous deux chez les bouquinistes. Tout ceci n'est en rien comparable à ce dont on dispose désormais sur Internet. Quiconque fait une recherche commence le plus souvent par Wikipédia. Facebook, YouTube ou Twitter sont devenus les médias d'informations d'une majorité de la population. La transformation des modes de connaissance a évolué extrêmement brutalement, en à peine dix ans. Il s'ensuit que la façon d'atteindre les cerveaux, au-delà des « informations », a évolué parallèlement. La donnée (ou l'information) devient le véhicule, renouvelé par la technique, pour façonner les esprits des humains. Ce peut être le fait des partis politiques (*scandale Cambridge analytica*) ou des terroristes (l'État Islamique est d'abord une franchise vidéo-politique maîtrisant parfaitement les codes de communication de la jeunesse occidentale). À part les cybercriminels, motivés par le seul appât du gain, les trois autres acteurs ont des motivations qui peuvent les amener à « manipuler » l'information afin de toucher les consciences. Bien sûr, comme dans toute théorie du complot, c'est toujours l'autre qui se trompe et qui manipule l'opinion. Mais sans verser dans cette dialectique en miroir, nous constatons que seul le cyberespace, notamment avec sa couche sémantique, permet d'analyser le phénomène des *infox* et de la post-vérité.

Finalement, nous connaissons une révolution anthropologique avec la révolution informatique; il n'est pas surprenant que nos modèles sociaux et politiques soient sérieusement remis en question. Voici au fond le dernier enjeu porté par la couche sémantique du cyberespace.

L'AUTEUR

Docteur en science politique, Olivier Kempf est chercheur associé à la fondation pour la recherche scientifique (FRS), membre du Conseil scientifique du FIC et consultant en cyber et digital (www.olivierkempf.com).
Olivier Kempf est l'auteur (avec F-B. Huyghe et N. Mazzucchi) de « Gagner les cyberconflits », Economica, 2015, première étude sur la couche sémantique du cyberespace. Il est également l'auteur de : Introduction à la cyberstratégie (Economica, 2012) et Alliances et mésalliances dans le cyberespace (Economica, 2014).

PROTECTION DE LA PERSONNE

© Fotolia 79058628

LE DÉFI D'UNE ASSOCIATION MAÎTRISÉE : INTELLIGENCE ARTIFICIELLE – RELATIONS HUMAINES

La gouvernance des relations humaines en association avec l'intelligence artificielle doit permettre l'expression de nouvelles compétences tout en se situant dans un cadre éthique et déontologique. Nulle décision ne peut être le produit d'une seule solution algorithmique ni être intégrée dans une disposition sans que la personne intéressée en comprenne les paramètres fondamentaux.
La décision en matière de relations humaines, associée à un protocole technologique, ne repose pas sur une dilution de la responsabilité et ne suppose pas de discrimination sous-jacente.
La gestion des données personnelles pose également la question de la responsabilité liée à leur sélection, leur préservation et à leur confidentialité.
En effet, l'hyperconnexion des personnes atténue la différence entre vie personnelle et professionnelle. Elle constitue un enjeu fondamental d'un nouveau modèle social. Elle comporte des risques psycho-sociaux et elle est la porte d'un totalitarisme lié au contrôle sociétal de nos modes de vie par la restriction de nos libertés individuelles et publiques.

I.A. :
l'artifice sans l'intelligence

Questions au Général William Vaquette

C

Comment l'humain doit-il se positionner face à l'intelligence artificielle qui se diffuse partout ?

Nous savons déjà que l'I.A est capable d'imiter le cerveau humain et de faire mieux que lui pour réaliser de nombreuses tâches, dont le nombre évolue d'année en année. Il faut donc que nous nous organisions pour aller dans des secteurs R.H. où elle ne nous est pas supérieure, notamment en puissance de calcul, en capacité de mémorisation, en rapidité d'accès et de traitement des informations.

GÉNÉRAL WILLIAM VAQUETTE

Directeur de projet en charge de la transformation des ressources humaines de la Gendarmerie nationale

Ainsi, pour se préparer au monde de l'I.A, il faut apprendre à bien la contrôler, dans le respect d'un code éthique et déontologique, car la décision R.H. finale doit toujours revenir à l'humain et en aucun cas à la machine, sans jamais sombrer dans la dystopie. L'enjeu n'est donc pas de gouverner les R.H. tout seul, mais de savoir ce que leur gouvernance, en association avec l'I.A., peut améliorer en acquérant de nouvelles compétences pour recentrer le métier R.H sur ce qu'il a de plus précieux : son aspect humain. En effet, comme l'ont si bien écrit deux chercheurs au M.I.T, en juillet 2017, Andrew Mc Afee et Erick Brynjolfsson : « *Au cours des dix prochaines années, l'I.A ne remplacera pas les managers, mais les managers qui utilisent l'I.A remplaceront ceux qui ne le font pas.* ».

Quels sont selon vous les grands enjeux déontologiques de l'I.A ?

On doit se diriger en quelque sorte vers un « permis de conduire IA/RH » pour mieux réglementer, superviser et inspecter ses utilisateurs.

C'est pourquoi, le législateur encadre

le recours aux algorithmes. Ainsi, l'article 10 de la loi du 6 janvier 1978, sur l'informatique, les fichiers et les libertés est ainsi rédigé :

« *Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée* ».

L'article L. 311-3-1 du Code des relations entre le public et l'administration précise quant à lui :

« *Sous réserve de l'application du 2° de l'article L. 311-5, une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande* ».

Saisi par le Sénat, le 16 mai 2018, de la loi relative à la protection des données personnelles dite « *CNIL3* », le Conseil constitutionnel a récemment précisé dans sa décision n° 2018-765, du 12 juin 2018, qu'une administration ne peut prendre une décision concernant une personne sur la base d'un algorithme, sauf et à la condition que celui-ci soit compréhensible par un humain et humainement contrôlé.

© Par Sikov - Adobe stock

Une décision intéressant une personne ne peut être induite par le seul résultat d'un algorithme complexe et segmenté. Il doit être analysé par un décideur formé et contradictoirement avec la personne concernée.

Quelles sont les problématiques à intégrer sur le plan éthique ?

Il est impératif sur le plan éthique d'intégrer les six problématiques[1] essentielles suivantes dans la

(1) Rapport de la CNIL, publié le 15 décembre 2017, sur les enjeux éthiques des algorithmes et de l'intelligence artificielle : « Comment permettre à l'Homme de garder la main ? ».

diffusion de l'I.A. pour atteindre une gouvernance augmentée des R.H. :
– *l'autonomie humaine au défi de l'autonomie des machines* pour faire face aux formes nouvelles de dilution de la responsabilité qu'impliquent des systèmes algorithmiques complexes et très segmentés ;
– *les biais, la discrimination et l'exclusion* qui sont, à l'heure du déploiement des algorithmes du machine learning, le plus souvent inconscients et difficilement repérables ;
– *la fragmentation algorithmique et la personnalisation*, comme par exemple le profilage, pouvant affecter vigoureusement des logiques collectives essentielles à la vie de nos sociétés en matière de pluralisme démocratique et culturel ou de mutualisation du risque ;
– *réinventer un équilibre entre limitation des mégafichiers et développement de l'intelligence artificielle* tout en maintenant l'impératif de protéger les libertés individuelles de chacun, intrinsèque à la législation européenne de protection des données personnelles ;
– *l'enjeu des données fournies à l'IA en termes de qualité, de quantité et de pertinence* par l'alimentation de données sélectionnées avec soin, pertinentes au regard de l'objectif poursuivi en dépit de la tendance à une confiance excessive dans l'entraînement de la machine pour son apprentissage ;
– *l'identité humaine au défi de l'intelligence artificielle par l'apparition de formes d'hybridation entre humains et machines* en appréhendant la nouvelle classe d'objets que sont les robots humanoïdes, susceptibles d'engendrer chez l'homme des formes d'affect.

Quels sont les grands défis de sécurité ?

Il convient de s'interroger plus particulièrement sur les enjeux de la sécurité avec l'I.A alors que les algorithmes sont voués à envahir notre quotidien. Leur piratage pourrait préfigurer les nouvelles attaques informatiques des décennies à venir alors même que ces systèmes n'ont pas été conçus à l'origine pour être déployés en présence d'un « *ennemi* ».

On distingue 3 types de piratages en matière d'I.A :
– le pirate informatique classique dont aucun dispositif actuel n'est à l'abri ;
– le détournement des techniques d'apprentissage des I.A (par exemple, l'attaque massive de certains *agents conversationnels* apprenants qui sont devenus racistes) ;
– le détournement des techniques d'interprétation des I.A.

Ainsi, de sérieuses failles inattendues sont apparues avec les pixels des images. Il suffit, sans véritable difficulté, de modifier la valeur de quelques pixels d'une photographie, que l'œil humain ne distingue pas, et l'algorithme de reconnaissance visuelle confond alors une orange avec un hélicoptère, un singe avec un panda,

un skieur avec un chien ou un chat avec un bus, *etc.* Des chercheurs de l'Université Carnegie-Mellon (États-Unis) sont ainsi parvenus, à l'aide de simples lunettes aux motifs imprimés, à duper totalement une I.A. de reconnaissance faciale. Une équipe de Google vient de faire croire à l'ensemble des I.A. actuelles que les objets ou êtres vivants à côté desquels ils reposent ne sont autres que des … grille-pains.

Selon Johathan Peck[2], spécialiste des mathématiques des réseaux de neurones à l'université de Gand (Belgique), « *ces attaques sont devenues très accessibles* ». Ces illusions d'optique totalement aberrantes pourraient prêter à rire en première approche, et pourtant « *à ce jour, personne ne parvient à expliquer ce phénomène* » avoue Andrew Lyas, théoricien de l'apprentissage machine au M.I.T.

(2) https://www.science-et-vie.com/archives/i.a.-la-faille-inattendue-41754.

Concrètement, qu'adviendra-t-il et quelle responsabilité juridique sera recherchée si un acte de piratage ou une simple erreur technique pousse une voiture autonome à interpréter un « *feu vert* » par un « *feu rouge* » ou, en radiologie médicale, produit une confusion entre une tumeur avec un organe sain ?

N'y a-t-il pas un danger d'hyper-connexion et d'atteintes aux libertés individuelles ?

Sur le plan social, avec le développement du numérique et notamment de l'accessibilité des messageries professionnelles, la frontière entre vie professionnelle et vie personnelle devient de plus en plus poreuse. Le déploiement progressif de l'I.A va réduire d'autant plus cette frontière, par exemple, avec la mise en place d'assistants virtuels qui accompagneront les cadres tout au long de leur journée, en mélangeant contraintes professionnelles et personnelles le soir.

C'est pourquoi, l'ancrage et l'exercice d'un véritable « *droit à la déconnexion* » doit être réaffirmé dans chaque administration par le dialogue social et la mobilisation de nombreux outils qui, pourtant, existent déjà : chartes de bonnes pratiques des outils numériques, plateformes de signalement interne, formation des cadres et agents, limitation informatique des diffusions de courriels, *etc.*

En effet, « *l'hyperconnexion* » constitue un enjeu fondamental d'un nouveau modèle social et un risque majeur face aux dérives possibles et aux risques psycho-sociaux qu'elle engendre.

Nous ne sommes plus dans la dystopie puisque la Chine s'est déjà engagée dans un ambitieux projet de contrôle social bâti sur l'intelligence artificielle permettant de surveiller la vie d'1,4 milliards de chinois dans un nouveau totalitarisme ultra sophistiqué. Elle a ainsi investi de manière pharaonique dans un système généralisé

de « *contrôlocratie* »[3], en cours d'expérimentation locale avant déploiement national en 2020, de contrôle high-tech capable de régir tous les aspects de la vie de ses citoyens tout en réduisant encore plus l'espace de libertés publiques et individuelles.

(3) Néologisme du politologue norvégien Stein Ringer, de l'université d'Oxford.

Il s'agit du traitement informatique dénommé « *crédit social* » collectant des données très précises issues de toutes les empreintes numériques laissées par des personnes au fil des activités familiales, scolaires, médicales, juridiques, commerciales, professionnelles, de loisirs, *etc.* Grâce aux I.A et aux algorithmes, les autorités déterminent ainsi le degré « *d'honnêteté* », de « *fiabilité* », de « *sincérité* » de chaque individu et par conséquent son « *degré de dangerosité prédictive* » vis à vis de l'ordre social chinois.

Dans certaines villes pilotes, les citoyens sont déjà classés en trois catégories : « *fiable* », « *normal* » et « *non fiable* », ce qui combiné avec l'internet chinois[4] et les 680 millions de caméras de reconnaissance faciale, constitue un écosystème de régulation sociale inédit dans l'histoire de l'humanité avec des punitions (exemple : blacklistage pour acheter un billet d'avion) et des récompenses (crédits de services) dans la vie sociale quotidienne.

(4) Surnommé « *La grande muraille numérique* », c'est à dire en réalité un gigantesque intranet sous surveillance et contrôle.

L'AUTEUR

Ancien élève de la 14e promotion du CID, auditeur de la 29e promotion « Beltrame » de l'INHESJ, de la 9e promotion du CHEMI, le général William Vaquette compte 33 années de carrière militaire dans la Gendarmerie nationale. Ancien appelé du contingent dans la gendarmerie, son parcours se caractérise par des expériences très variées dans les domaines du commandement territorial et opérationnel, de la formation, de la diplomatie, du juridique, de la légistique et de la gestion des ressources humaines. Connu comme le « Monsieur retraite » de la gendarmerie depuis 2016, il a également été nommé, le 1er août 2019, directeur de projet en charge de la transformation des ressources humaines de la Gendarmerie nationale.

DOSSIER

L'humain maillon de la cybersécurité

Réflexions sur l'Homme

et le cyberespace : le paradoxe de l'œuf et de la poule…

Par Stéphane Mortier

Sous le prisme du paradoxe de l'œuf et de la poule, il s'agira ici de livrer quelques spéculations sur l'homme et le cyberespace, sur les évolutions sociétales et humaines de notre temps et d'engager une réflexion de fond sur notre monde et celui de demain.

Le cyberespace est une création purement humaine et un artefact. Il est définitivement différent du monde physique naturel car il obéit à des lois d'une toute autre nature.

STÉPHANE MORTIER

Section sécurité économique et protection des entreprises DGGN

Les réseaux numériques sont extensibles à l'infini et sont à la fois de nature très physique (machines, cablages, infrastructures) et de nature abstraite et virtuelle (espace sémantique). Le temps et l'espace y sont comprimés, les attaquants potentiels étant parfois vos proches voisins. C'est ainsi que Philippe Wolf et Luc Vallée définissaient le cyberespace dans le Rapport INHESJ/ONDRP de 2011.

Le cyberespace est donc une création humaine. Il serait alors l'œuf et l'homme la poule…

Avec ses millions de pages connectées, ses ordinateurs en tous genres, ses infrastructures de communication, ses satellites, ses fréquences et les réseaux que ces éléments constituent, le cyberespace repose sur des composants physiques et matériels, bien que ceux-ci engendrent une grande part de virtuel qui échappe à la plupart des utilisateurs. Bref, tout cela confine de façon imagée, toute proportion gardée, à la projection virtuelle et métaphorique d'un « super-cerveau » humain.

Il y a plus de vingt ans, en 1996, dans un article intitulé « *The World Wide Web as Super-Brain : from Metaphor to Model* »,

Francis Heylighen et Johan Bollen de la Vrij Universiteit Brussel (VUB) avaient avancé des propositions intéressantes au sujet du développement du « super-cerveau » et de ce qui lui permet d'apprendre, sans omettre de signaler que ce n'est pas le cerveau en soi qui pense, mais les utilisateurs du web. En effet, le pouvoir de ce « super-cerveau » réside bien dans le lien ténu qu'entretient le web avec ses utilisateurs, un lien autoréférentiel. Les algorithmes se sont également développés, ce qui – par analogie avec le cerveau humain – renforce les liens fréquemment utilisés, et affaiblit ceux qui le sont moins fréquemment. À l'aide du principe de la transitivité, la construction de nouveaux liens peut être automatisée. Mais rien de cela ne signifie que ce « super-cerveau » peut en fait penser indépendamment des utilisateurs qui le constituent. Cela pose entre autres choses la question des développements futurs en matière d'intelligence artificielle.

Ce qui nous intéresse ici, c'est bien la construction du cyberespace par l'homme et la manière dont elle amène l'homme à être lui-même le matériau de construction. L'homme architecte de l'édifice, matériau et référent de sa construction ! Une lecture sociologique s'impose puisque le cyberespace, création humaine par excellence serait alors une construction sociale, un lieu de libertés mais aussi de conflictualités et d'asservissement.

Une construction sociologique identitaire

La sociologie de l'action d'Alain Touraine offre une grille de lecture particulièrement intéressante. En effet, dans ce courant de pensée, un mouvement social se définit par trois principes : l'identité (au nom de qui parle l'acteur), l'opposition (à quel adversaire il s'oppose) et la totalité (pour le contrôle de quel enjeu il se mobilise). Appliqués au cyberespace, ces trois principes donnent la lecture suivante :

– **L'identité :** De qui s'agit-il ? Qui a créé le cyberespace ? Bien que le terme soit issu de la science-fiction (Gibson, Neuromancien, 1983), ce sont bien les Bob Kahn, Vinton Cerf et autre Louis Pouzin avec des projets comme ARPANET, Cyclades,…qui en sont les pionniers emblématiques. Il s'agissait bien de systèmes de partage d'informations et de documents, ayant pour objectif initial de faciliter le quotidien. Le système en se développant a produit des mots, des concepts, des idées nécessaires à sa légitimation au plus grand nombre. Le système s'auto-alimente alors par les contributions des utilisateurs. *L'œuf deviendrait-il petit à petit la poule… ?* L'identité du cyberespace s'auto-alimente des comportements des utilisateurs qui ensuite sont influencés par le cyberespace. Il s'agit en somme d'une forme d'autoproduction, l'autopoïèse (du grec **auto** soi-même, et **poièsis** production, création) étant

la propriété d'un système de se produire lui-même, en permanence et en interaction avec son environnement, et ainsi de maintenir son organisation (structure) malgré son changement de composants (matériaux). C'est donc bien une construction collective qui influe sur la construction de l'ensemble lui-même. Pour Alain Touraine, l'identité de l'acteur ne peut pas être définie indépendamment du conflit réel avec l'adversaire et de la reconnaissance de l'enjeu de la lutte (*La production de la société*, 1993). Cela correspond totalement à la position de l'acteur dans le cyberespace, acteur d'un système qui le façonne lui-même en retour.

– **L'opposition :** Qui est l'adversaire ? À qui s'oppose l'acteur ? « *Même si le conflit est limité par son enjeu immédiat et les forces qu'il mobilise, on ne peut parler de principe d'opposition que si l'acteur se sent confronté à une force sociale générale en un combat qui met en cause des orientations générales de la vie sociale* » (La production de la société, 1993). Force est de constater que l'homme a construit un système, un environnement, qu'il peine à maîtriser alors qu'il en est un acteur de plus en plus impliqué, qui s'autonomiserait, en quelque sorte, en un nouvel ordre émergent. Les orientations de la vie sociale sont systématiquement influencées par les comportements des utilisateurs du cyberespace et notamment par l'utilisation des données personnelles. L'utilisation des acteurs par d'autres acteurs, parfois et souvent non-identifiés, du cyberespace engage des oppositions, voire des luttes, pour lesquelles les acteurs se mobilisent. Les *fake news* en sont un exemple particulièrement édifiant. Le nombre incalculable de cyberattaques en est un autre alors qu'elles sont elles-mêmes menées par d'autres acteurs dits aussi « cybercriminels » *L'œuf et la poule se confondent peu à peu…*

– **La totalité :** Pourquoi lutte-t-on ? C'est la recherche d'une orientation générale de la société qui guide l'action des acteurs. De nombreux activistes sont en quête d'une autre forme de représentation, de vie, d'existence et c'est dans le processus même de l'action qu'ils vont trouver de nouvelles formes d'expression, tant virtuelles que réelles : le processus construira un nouveau modèle idéal. Si ce modèle est proche du chaos pour les cybercriminels, il vise l'harmonie la plus totale pour d'autres et dans les deux cas, il y a bien une recherche d'orientation générale de la société. Le cyberespace est alors l'outil utilisé par les acteurs et généré par eux, pour eux, dans le sens de leur action.

Dans tous les cas, on assiste à la construction d'un sujet collectif, en termes d'organisation systémique. Le sujet, c'est la constitution de réseaux et l'acteur est

le réseau. Le cyberespace fonde le mouvement (des acteurs), mais sans le cyberespace ce mouvement n'existerait pas. C'est la combinaison du monde réel et, physique avec le cyberespace, à la fois physique, abstrait et virtuel, qui tisse des réseaux dont les acteurs sont eux-mêmes des acteurs-réseaux, vecteurs d'intelligence collective. En d'autres termes, l'acteur a créé l'outil (le cyberespace) et est devenu lui-même, chemin faisant, l'outil de son propre outil ! *Plus d'œuf mais deux poules…*

Ce paradoxe peut aisément être illustré par un exemple concret, comme le *Big Data* (dont la tentative francophone de substitution sémantique par mégadonnées a échoué, et ce n'est pas anodin). Le *Big Data*, est entendu comme un ensemble de données de tous formats, soumis à des algorithmes de traitement qui corrèlent ces données entre-elles pour en extraire des résultats. Ceux-ci impacteront la prise de décision ou la mise en place d'actions.

L'ensemble des données qui seront traitées émanent bien des acteurs ou de leurs actions, de leurs comportements dans le monde réel et virtuel. L'acteur agit généralement de façon à améliorer son environnement (bien-être personnel ou familial, rationalisation des process, avantages financiers, allègement des tâches, …). Il tente donc de combattre et d'écarter ce qui fait obstacle à sa vision d'une société meilleure ou plus avantageuse pour lui. Il ne le fait généralement pas seul, même s'il n'est pas organisé avec d'autres acteurs (plusieurs acteurs poursuivent les mêmes objectifs, sans pour autant se connaître personnellement, physiquement). Le système étant alimenté par ses propres données traitées par des algorithmes, l'acteur va recevoir en retour des résultats qu'il ne soupçonnait généralement pas. Ils vont alors influencer son comportement et générer de nouvelles données que les algorithmes traiteront également, et ainsi de suite. Le principe de totalité est alors mouvant et en perpétuelle redéfinition. La question est de savoir si c'est l'acteur qui alimente le système ou l'inverse, l'acteur devenant alors l'outil ? *Ni poule ni œuf ?*

© Par Gunnar Assmy - Fotolia - 62348117

Le cyberespace est un « Léviathan » qui dévore ceux qui l'ont créé pour générer un ordre nouveau, lui-même en perpétuelle redéfinition.

Prenons un autre exemple qui est celui de l'utilisation de l'ingénierie sociale. Si l'acteur n'alimentait pas le système en données (réseaux sociaux, blogosphère, …), l'utilisation de celles-ci à des fins malveillantes ne serait pas possible. Or, la victime d'une escroquerie dont le mode opératoire comporte de l'ingénierie sociale est bel et bien victime de sa participation au système. Elle est l'outil du système qu'elle a elle-même contribué à créer ! Il n'y a plus de distanciation entre l'acteur et l'outil, l'engagement étant total par rapport à celui-ci et même dans celui-ci, au point qu'une (confusion s'opère entre les deux pour ne faire plus qu'un. *À la fois œuf et poule !*

Pour comprendre et aborder ce phénomène des interrelations homme/cyberespace, la recherche-action semble être une méthode adéquate. Le processus impulsé peut être appréhendé comme une dynamique d'apprentissage individuelle et collective d'un savoir, dans et par l'action, permettant le développement des capacités réflexives des acteurs. Ce type de recherche trouve en effet ses fondements dans la perception des contextes et situations particulières des praticiens, en l'occurrence dans l'utilisation que chacun fait de l'outil, du cyberespace. On peut retenir deux caractéristiques de la recherche-action :

– Elle repose principalement sur l'idée que pour connaître une réalité sociale, il faut participer à sa transformation. Non seulement l'acteur participe à la construction du cyberespace mais il se construit également lui-même par le cyberespace : l'un et l'autre sont alors transformés ;

– Elle est performante dès qu'il s'agit de travailler sur des dynamiques multidimensionnelles, interdisciplinaires, des systèmes d'interactions, ce qui correspond totalement au cyberespace, à ce réseau dont l'acteur est le fondement.

Une méthodologie développée en centre de recherche

Cela correspond à une méthodologie développée dans le cadre de la Gendarmerie nationale, plus particulièrement par les chercheurs rattachés au centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN). Il s'agit de « l'intelligence de sécurité territoriale[1] ». Delpeuch, Jaffré et Ross y indiquent que les chances de succès des stratégies et tactiques dans le domaine de la sécurité publique dépendent, dans une large mesure, de la qualité de leur conception, qui est elle-même tributaire du niveau de connaissance de leur environnement que les unités de gendarmerie ont été capables d'acquérir. Mieux les gendarmes appréhendent le contexte dans lequel s'inscrit leur action, mieux ils comprennent les problèmes qu'ils ont à traiter et plus ils

(1) https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Manuel-d-intelligence-de-securite-territoriale-Demarche-de-resolution-de-probleme

sont capables de prendre de bonnes décisions. Le terme « intelligence » renvoie aux structures organisationnelles (telles que les unités et personnels spécialisés dans le traitement de l'information), aux dispositifs techniques (tels que les systèmes d'information et de communication) et aux méthodes professionnelles (telles que les techniques d'analyse criminelle) qui servent à étayer le travail d'information et de réflexion des gendarmes.

Nous avons en quelques lignes refait une lecture des missions de la gendarmerie par la sociologie de l'action !
Le gendarme, acteur de la sécurité publique, façonne son environnement pour optimiser son action sur les facteurs d'insécuirté, tout en étant lui-même imprégné en retour de l'environnement qu'il a présidé à construire.

Ces quelques réflexions se veulent volontairement disruptives et quelque peu provocatrices. Il s'agit bien entendu d'une remise en cause de l'homme social dont les combats sont aujourd'hui lissés dans un système qui dépasse tout un chacun et qui tente de gommer les aspérités qui faisaient de l'homme d'antan un être vivant si caractéristique. Optimisme ou pessimisme ? Ni l'un ni l'autre très probablement, mais c'est le constat d'une considérable évolution de notre monde post-moderne. Un nouveau monde que nous nous devons de repenser, qui pose la question des paradigmes usités actuellement et de leur reconfiguration progressive.

Nos modes de réflexion, d'analyse, faits d'explications souvent causales et linéaires ne doivent-ils pas être remplacés par une démarche de compréhension systémique et paradoxale du sens, et par une prise en compte accrue de l'engagement sociétal des acteurs de la société qui est la leur aujourd'hui : le cyberespace ? Nos grilles de lecture passées ne sont-elles pas devenues obsolètes ? L'homme d'aujourd'hui, l'homme du XXIe siècle, l'homme de l'ère numérique n'est-il pas un homme nouveau, un *homo cyberneticus*, un maillon du « meilleur des mondes », un « Big Brother » volontaire, un cyber-citoyen libertaire ou un transhumaniste ? *Plus d'œuf, plus de poule, un substitut à déterminer !*

L'AUTEUR

Stéphane Mortier est affecté à la section « sécurité économique et protection des entreprises » de la DGGN. Docteur en Sciences de gestion, de l'Université Paris 1 Panthéon-Sorbonne, diplômé en sciences politiques, en sociologie et en politique internationale de l'Université libre de Bruxelles, il est également diplômé de l'École de Guerre Économique.

Comment penser
la cybersécurité au service des générations futures ?

Par Solange Ghernaouti

« La guerre est la grande affaire des nations ; elle est le lieu où se décide la vie et la mort ; elle est la voie de la survie ou de la disparition » Sun-Tzu[1].

(1) Sun Tzu et autres stratèges. *Les sept traités de la guerre*, traduit du chinois et commenté par Jean Lévi. Collection Pluriel, Hachette Littératures, 2008, p. 87.

Cet article a vocation à mettre en évidence la difficulté ontologique à penser une cybersécurité au service de l'humain alors que les technologies du numérique servent des objectifs de rationalité économique et sont au service des pouvoirs économique et politique et de la guerre.

SOLANGE GHERNAOUTI

Experte internationale Directrice du Swiss Cybersecurity Advisory & Research

Le numérique au cœur des guerres

Internet et le cyberespace constituent une extension des lieux d'expression du pouvoir et des rapports de force traditionnels exercés au travers des théâtres de la terre, la mer, l'air et l'espace extra atmosphérique.
Au XXIe siècle, la guerre se déroule aussi dans les territoires virtuels du cyberespace. L'informatique est au cœur des guerres idéologique, culturelle, scientifique, économique et politique. Cette nouvelle forme de guerre par l'information et le code informatique permet de « soumettre l'ennemi sans ensanglanter sa lame » [2], pour reprendre l'expression du célèbre général chinois Sun-Tzu (Ve siècle avant J.-C.).

(2) *Ibid.* Chapitre III, p. 97

Internet peut être instrumentalisé pour infliger des dégâts à l'ennemi sans l'envahir physiquement ni géographiquement, mais en réduisant son pouvoir dans les domaines stratégique et opérationnel, dans les mondes physique et virtuel. L'informatique contribue

à « projeter » du pouvoir et à contraindre l'adversaire dans ses dimensions civile et militaire.

Gagner et préserver des parts de marché passe par l'espionnage économique et industriel, l'intelligence économique, la cybersécurité, la surveillance des télécommunications et les cyberattaques. Le point commun entre tous ces modes opératoires de cybercombat est qu'il est difficile de déterminer leur origine, d'en identifier les acteurs et d'attribuer clairement la responsabilité aux puissances qui les ordonnent. Le cyberespace procure une couche d'isolation protectrice que l'on peut rapprocher là encore des préceptes du maître chinois qui affirmait : « ... qui connaît l'art de se rendre invisible et de tout voir ne rencontrera pas d'ennemi ... »[3].

(3) *Ibid.* Chapitre XXVI « Arcane du dragon », p. 396.

Cinq facteurs stratégiques pour penser et gagner la guerre

Selon Sun-Tzu, la guerre est subordonnée à cinq facteurs : le climat, la topographie, l'organisation, le commandement et la vertu. Toujours actuels, ils peuvent être transposés au cyberespace.

Les usages numériques, les vulnérabilités matérielles, logicielles et humaines, les acteurs de l'écosystème numérique ainsi que le moment opportun peuvent être constitutifs du climat. Les territoires numériques, les infrastructures matérielle et logicielle informatique et télécom, y compris celles du *Darknet*, font parties de la topographie.

La chaîne d'approvisionnement logistique de l'écosystème numérique, le cycle de vie des systèmes, les services et produits (fabrication, diffusion, maintenance, recyclage, destruction), les modèles économiques de déploiement et de captation de valeur, sont des dimensions de l'organisation. Cela comprend les capacités à influencer, à mobiliser, à déstabiliser et à rallier des acteurs pour effectuer des actions allant dans le sens de la défense de certains intérêts. La faculté de mobiliser des communautés de cybercombattants, de patriotes, de dissidents, d'hacktivistes, de consommateurs (e-commerce, jeux en ligne, réseaux sociaux, ...), en s'appuyant sur des dispositifs d'information et de désinformation (*fake news*, ...) peuvent être considérée comme des leviers d'actions de lutte, d'attaque et de défense.

« Le commandement dépend de la perspicacité, de l'impartialité, de l'humanité, de la résolution et de la sévérité du général » [4].

(4) *Ibid.* p.92.

Ces attributs, hormis celui d'humanité, pourraient s'appliquer aux logiciels d'intelligence artificielle (algorithmes d'aide à la prise de décision

ou de prise de décision) dans un contexte de commandement militaire et d'armement. De plus en plus d'armes intègrent des capteurs, des logiciels d'analyse, de téléguidage, de géolocalisation, d'aide à l'identification des adversaires, d'aide au tir de précision et à la priorisation des actions de tir. C'est tout un arsenal de missiles, fusils-mitrailleurs, drones, robots de détection d'engins explosifs, de reconnaissance, ou de munitions « intelligentes », qui existe et renforce l'assurance d'atteindre les cibles en faisant souvent plus de dégâts que des armes traditionnelles. Tout ceci vient compléter les tenues de combat intelligentes et les exosquelettes (*smart suit, smart gun, smart soldier*). Les technologies de l'information se métamorphosent en co-combattants[5], véritables équipiers des soldats et officiers, tant sur le théâtre des opérations que sur les sites et dans les chaînes de commandement. L'intelligence artificielle contribue à l'automatisation de la prise de décision, avec comme horizon la possibilité de prendre la décision de tuer sans intervention humaine, pour ouvrir le feu et riposter. (Approche rejetée par le ministère des Armées français).

(5) Notion de cohabitation homme-robot (cobotique).

L'intelligence artificielle au service du *hard power*

Au service du *hard power*, l'intelligence artificielle promet efficacité et performance en augmentant la puissance de frappe et la distance de tir, ce qui réduit d'autant l'exposition aux risques de son détenteur.

Comme l'illustre la figure 1, la résolution et la sévérité du Général deviennent relatives à :

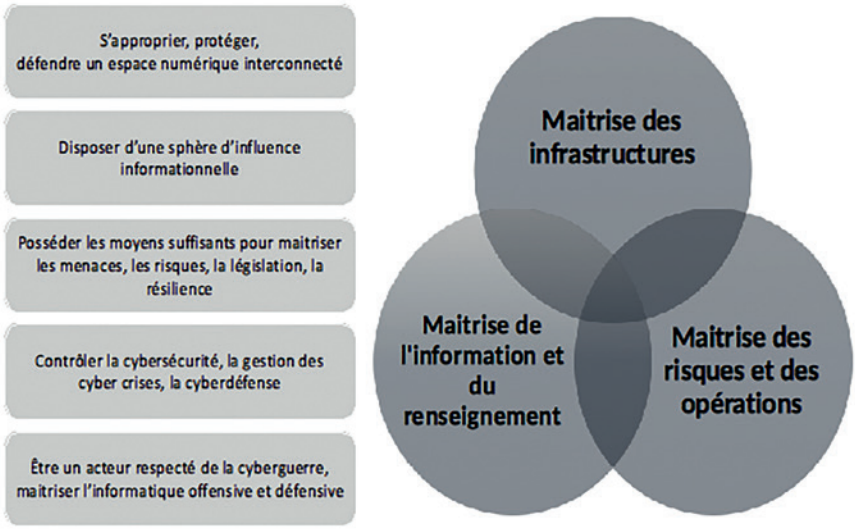
– sa maîtrise des infrastructures numériques et des infrastructures énergétiques.

– sa compétence en recherche et développement en informatique.

– sa capacité à former et entraîner ses troupes, à planifier et à conduire des opérations et des cyberopérations.

– ses dispositifs de renseignement et d'analyse.

– ses moyens de cybersécurité et de cyberdéfense, la robustesse et la résilience de ses infrastructures informatiques.



Les principaux facteurs clés de succès.

De la vertu

La soumission volontaire aux GAFAM reflète le concept de vertu qui, selon Sun-Tzu, « assure la cohésion entre supérieurs et inférieurs et incite ces derniers à accompagner leur chef dans la mort, comme dans la vie, sans crainte du danger » [6].

(6) *Ibid.* p.91.

Par exemple, les nouvelles manières de communiquer peuvent participer à des actions d'endoctrinement, de manipulation psychologique, d'activisme ou de marketing de la guerre.

(7) *Ibid.* p.15.

La vertu, est une qualité qui, selon Montesquieu et comme le rappelle Jean Lévi[7], fait référence à la force morale conférée à une nation par ses mœurs, ses institutions et son régime politique. Elle est une disposition à faire le bien et à éviter le mal. Elle est liée au mérite de l'homme, à son courage, à sa sagesse. Cela pourrait englober les capacités du numérique à préserver le vivant et ses conditions de vie sur Terre (paix, climat,...).

La force de frappe numérique transforme les rapports de force

(8) *Ibid.* Chapitre II, p.95.

Sun Tzu affirme qu'« un général avisé s'emploie à vivre sur l'ennemi » [8].

C'est précisément ce que font les acteurs hégémoniques du Net puisqu'ils développent leur puissance et leur pouvoir à partir des usages numériques qui autorisent la captation et l'exploitation des données et des méta données. Les pouvoirs politiques, militaires et économiques des États sont liés à leur capacité à contrôler les technologies de l'information. Le tableau 1 présente les avantages stratégiques de la maîtrise du numérique dans les rapports de force du XXIe siècle.

Vers un technobiocide ?

Médiée par la technologie, chaque action permet d'instaurer une distance entre le monde concret et l'humain. La distance géographique et émotionnelle, délivre l'humain de faire la guerre et de connaître l'horreur des champs de bataille. C'est ce qu'autorisent également les cyberattaques sur des systèmes d'information d'infrastructures vitales. Poussée à l'extrême, la « technologisation » de la guerre traditionnelle, les nouvelles formes de guerres cybernétiques pourraient conduire, non seulement à des technogénocides, mais aussi à des technobiocides[9], du fait du risque de destruction globale de l'écosystème par la technologie. Dans le cyberespace, les activités relevant d'actes de guerre, au sens traditionnel du terme, sont complexes à identifier et à contrôler, car il est difficile :

(9) Risque qui existe depuis la bombe atomique, mais qui pourrait advenir sans elle !

– de connaître l'ennemi[10], d'attribuer avec certitude l'origine des cyberattaques et donc de riposter ;

(10) L'ennemi connaît sa cible, les données dont il a besoin pour lui nuire sont disponibles (réseaux sociaux, Darknet, ...).

– de faire respecter le droit humanitaire et celui de la guerre ;

– d'organiser des opérations d'envergure sans y impliquer des militaires.

L'intelligence artificielle au service de l'humain et des générations futures ?

La cybernétique, dont l'origine renvoie à l'art de gouverner, est en train de s'imposer et de prendre le commandement de toute chose, de tout acte. Le numérique instaure un nouvel ordre du monde. L'intelligence artificielle, avec ses capacités à prendre des décisions ou à y contribuer, dans une logique de performance et de rationalité économique, se situe dans le prolongement du transfert des capacités de l'humain vers la machine. Elle entraîne une perte de compétences, une réduction d'autonomie et une dépendance, voire une addiction aux systèmes. L'intelligence artificielle en réduisant l'erreur et en donnant l'illusion qu'elle supprime l'incertitude conduit à une normalisation des comportements et à la ruine de la diversité. Elle permet de prédire et d'orienter des choix pour consommer et faire faire. Des prédictions et propositions engendrent des manipulations psychologiques et pilotent les actions. Les fausses informations

(*infox*) peuvent renforcer le pouvoir de manipulation. L'intelligence artificielle, dont la finalité est déterminée par ses concepteurs et propriétaires, a des modes opératoires, qualité et sécurité opaques et souvent incontrôlables.

Perspectives

Lorsque les données et le code informatique sont une arme de guerre et l'intelligence artificielle du matériel militaire, il devient nécessaire de s'interroger sur le type de société dans laquelle nous voulons vivre. Est-ce celle d'une meilleure connaissance du réel et des consciences éclairées ? Celle de la gestion algorithmique, de la surveillance et du contrôle permanent ? Celle du culte des machines ou encore celle du plein pouvoir du techno-libéralisme ?

L'obligation de subir le numérique nous donne le droit d'en connaître la finalité (pour quels bénéfices et renoncements et pour qui ?). C'est alors que nous pourrons réellement penser « l'humain au cœur de la cybersécurité » et réaliser des solutions pragmatiques et efficientes.

Il est impossible de faire l'économie de l'analyse des impacts de l'écosystème numérique, du contrôle des données, des mesures de cybersécurité et de cyberdéfense pour les générations futures. Comme pour le changement climatique, c'est elles qui en paieront le prix.

L'AUTEURE

Solange Ghernaouti, docteure en Informatique de l'Université Paris Sorbonne, ancienne auditrice de l'Institut des Hautes Études de Défense Nationale, est professeure de l'Université de Lausanne, directrice du Swiss Cybersecurity Advisory & Research Group et présidente de la Fondation SGH –Cybermonde. Experte internationale en cybersécurité et cyberdéfense, écrivaine, analyste prospectiviste, classée parmi les 20 femmes qui font la Suisse, elle est membre de la Commission suisse pour l'UNESCO, de l'Académie suisse des sciences techniques et Chevalier de la Légion d'honneur.

L'approche statistique

au service de l'humain : mieux comprendre les risques cyber pour une société plus résiliente

Par Marie Kratz

Les coûts humains et financiers de la cybercriminalité ont augmenté de façon exponentielle depuis l'énorme faille de sécurité chez Equifax, le 7 septembre 217[1]. Cet exemple de violation de données montre combien le risque cyber peut provoquer une chute importante du cours boursier d'une entreprise (-35 % en une semaine) et une atteinte à sa réputation. Un autre exemple est celui de SingHealth, le plus grand groupe de soins médicaux de Singapour, qui a subi une violente attaque cyber[2]. On pourrait multiplier les exemples illustrant la fragilité de nos systèmes face à des hackers déterminés. Même si la société, les individus, les compagnies, et les politiciens sont de plus en plus conscients de l'importance grandissante du risque cyber, pour ce dernier, nous sommes encore loin d'avoir atteint le niveau de compréhension et d'évaluation des risques financier ou de catastrophe naturelle.

MARIE KRATZ

ESSEC Business School
Centre de Recherche Econo-financière et Actuarielle sur le Risque
CREAR – Paris Singapore

(1) L'exploitation de cette faille a affecté pas moins de 148 millions de personnes. Les données incluaient, entre autres, numéros de cartes de crédit, de permis de conduire, de sécurité sociale, de téléphone, dates de naissance, et adresses emails. http://fortune.com/2018/09/07/equifaxdatabreach-oneyearanniversary/

(2) Avec un vol de données personnelles de 1,5 millions de patients soignés dans les cliniques de ce groupe de santé entre mai 2015 et juillet 2018.

Comprendre les risques cyber en vue d'établir des stratégies de cyber-sécurité : un défi certain

Le manque de données statistiques fiables, les pertes sur des éléments intangibles difficiles à mesurer, les constants développements informatiques rendent la modélisation complexe. De fait, de par sa nature émergente, il est difficile d'appliquer au risque cyber les techniques traditionnelles d'analyse de risque.

Le risque cyber est un **sujet multidisciplinaire** par nature, sur lequel chercheurs en criminologie, en communication, en droit, en informatique, en finance, en gestion des risques, en sciences actuarielles et sciences des données, devraient collaborer pour en obtenir une image réaliste et pouvoir ainsi établir des stratégies de protection des individus, de la société au sens large.

C'est dans ce contexte qu'un partenariat a été mis en place entre l'ESSEC-CREAR (Centre de Recherche Econo-financière et Actuarielle sur le Risque) et le PJGN (Pôle Judiciaire de la Gendarmerie Nationale). Étant donné la complexité du sujet, il est fondamental de confronter et rapprocher des **approches qualitatives et quantitatives**[3]. C'est sans aucun doute le moyen le plus productif pour comprendre la dynamique d'un risque évoluant dans un environnement changeant si rapidement. Se limiter à l'une ou à l'autre de ces approches, ou, pire, les opposer, reviendrait à n'avoir qu'une version fragmentée de la réalité ou à réduire le problème au lieu de le simplifier. Dans tous les cas, cela restreindrait notre capacité à explorer la pleine complexité de ce phénomène. Il faut combiner ces approches et apprendre les uns des autres pour envisager des solutions appropriées.

(3) Living in a stochastic world and managing complex risks (disponible en ligne : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2668468). Voir aussi les deux articles de presse de M. Dacorogna, M.Kratz et P. Lecomte : "Managing risk is about raising society's resilience", The Business Times, Singapore, Dec. 2015 ; 'Changing times require new tools for risk management', Asia Insurance Review, Dec. 2016

(4) Conférence du 3 juin 2019 organisée par la PJGN : « Pôle analyse : Peut-on évaluer les risques Cyber ? »

(5) Conférence du 26 au 27 juillet 2019 organisée par Société Actuarielle de Singapour SAS-ERM et l'ESSEC-CREAR : « Cyber Risks : threats and opportunities for the Asia Pacific Insurance Industry » ; http://crear.essec.edu/conferences/4th-sasermesseccrear-conference

(6) Forage de données, explorations de données ou fouilles de données, ce sont les traductions possibles du data mining en Français. En règle générale, le terme Data Mining désigne l'analyse de données depuis différentes perspectives et le fait de transformer ces données en informations utiles, en établissant des relations entre les données ou en repérant des patterns.

C'est dans cet état d'esprit que nous avons démarré la **collaboration** avec le PJGN. Nous avons pu aborder l'analyse de la base de données conséquente, constituée par le PJGN, grâce à un échange de connaissances et d'expériences importantes entre criminologues, informaticiens et statisticiens-probabilistes. Dans cette perspective, la tenue de conférences (nationales[4] ou internationales[5]) offre également un forum essentiel pour l'échange d'informations et d'idées sur la cybercriminalité.

L'exploration de la qualité des données par différentes méthodes est une autre façon de collaborer. Le PJGN a commencé à développer des méthodes de data-mining[6] pour vérifier la pertinence des champs renseignés dans la base. CREAR a abordé ce problème par une approche statistique des risques extrêmes. Par exemple, l'analyse des montants des plaintes et de leurs distributions a permis de détecter des valeurs mal renseignées. Le but est d'arriver à une base de données contenant aussi peu que possible d'erreurs.

Elle pourra alors, dans un second temps, être mise à la disposition de la communauté des chercheurs pour élargir le champ des approches pour son analyse.

La Statistique au cœur de la Société

On a souvent tendance à opposer l'humain à la statistique, pourtant cette dernière a été développée précisément pour **permettre à l'humain de mieux appréhender et maîtriser son environnement**. Elle est là pour servir à dégager des lignes de forces et à mieux comprendre les facteurs contribuant aux phénomènes étudiés. Des tables de mortalité inventées au XVII[e] siècle par Halley, aux études randomisées de l'efficacité des médicaments, la statistique se met au service de l'amélioration de la qualité de vie.

Avec l'avènement des nouvelles techniques d'intelligence artificielle, qui combinent la statistique et la puissance de calcul, il sera possible d'accompagner par exemple le travail des enquêteurs en leur offrant un outil de plus dans leur panoplie.

Nous comptons développer des outils pour améliorer la saisie des données et leur pertinence, pour assurer le suivi de l'évolution de la criminalité cyber et pour quantifier correctement les risques auxquels elle nous confronte. La collaboration de tous (criminologues, informaticiens et mathématiciens) sera une fois de plus nécessaire pour traduire en termes compréhensibles les résultats de statistiques et modèles qui peuvent être parfois très complexes à interpréter (on assiste déjà au développement de logiciels d'analyse des résultats obtenus par les réseaux de neurones, afin d'obtenir une explication compréhensible pour les humains !).

La modélisation des risques cyber

Alors que la modélisation mathématique d'un phénomène consiste à comprendre le processus sous-jacent (ou structure dynamique) de ce phénomène, au travers de sa réalisation, son but est d'aller au-delà de cette réalisation (les données) **pour extrapoler, généraliser et obtenir des perspectives significatives pour les comportements futurs**, et ainsi être capable de déduire des scénarios possibles. L'évolution très rapide des technologies de l'information rend difficile la modélisation du risque cyber. De plus, à cause de sa complexité humaine, il ne peut pas être modélisé de la même manière qu'un risque de catastrophe naturelle. Dans l'analyse du risque de catastrophe naturelle, la localisation géographique constitue le facteur crucial, alors que l'analyse d'un risque cyber dans une situation donnée met en jeu plusieurs facteurs : les motivations des cybercriminels, les caractéristiques des cibles, les motivations de l'utilisateur, les protocoles de sécurité, *etc.* **Une fois l'intensité potentielle de la cybercriminalité reconnue, il est important de combiner les données historiques et des méthodes fondées sur une approche de risque systémique**. Là aussi, cela nécessite la collaboration avec des experts de différentes disciplines pour prendre en compte les multiples

facteurs en jeu et interpréter modèles et résultats.

(7) M. Kratz. S'adapter au nouvel environnement des risques: peut-on assurer le risque cyber ? ESSEC Knowledge Avril 2019 et Reflets Magazine Juin 2019.

Cyber-résilience ou cyber-sécurité[7] ?

Alors que le terme de « cybersécurité » est aussi vieux que les ordinateurs eux-mêmes, le terme de « cyber-résilience » est apparu récemment et prend de plus en plus d'importance. La cybersécurité est focalisée sur la sécurité seule, mais les organisations ont besoin d'une stratégie plus large qui inclut leur capacité à survivre à une attaque et la possibilité d'assurer une partie des risques inévitables. On pourrait se demander si au fond la résilience n'est pas la même chose. Pas vraiment ! Il existe une différence substantielle de sens entre les deux. Le terme de sécurité renvoie à la défense, la protection, la précaution, tandis que celui de résilience fait référence au flottant, à l'élastique, au malléable, à ce qui est facile à renouveler et protecteur. En d'autres termes, la cyber résilience qualifie la capacité d'une organisation à se rétablir et à continuer d'exercer son activité lorsqu'elle subit une cyber-attaque.

Il est donc primordial de développer et de mesurer au niveau de l'individu, des compagnies et en général de la société, cette résilience aux risques cyber afin de développer des stratégies de cyber-sécurité. Le futur de cette résilience sera dans la combinaison de mesures de sécurité, de redondances dans les systèmes informatiques et de couvertures assurantielles pour assurer la survie et le fonctionnement du système.

Enfin, pour améliorer la cyber-sécurité, il faut prendre conscience qu'on doit aller au-delà des solutions technologiques et des investissements, vers la mise en place d'une législation sur ce sujet. Il faut admettre que les pays les plus développés économiquement constituent toujours des cibles privilégiées mais que le renforcement de leur arsenal juridique augmente leur résilience. La RGPD est un pas dans ce sens.

En revanche, les pays ayant un outillage juridique faible peuvent servir de « paradis numérique », c'est-à-dire constituer un point de faiblesse dans notre dispositif en l'absence d'accords de coopération, en permettant des rebonds vers des cibles lucratives et de ne pas laisser de traces numériques.

L'AUTEURE

Marie Kratz est Professeure à l'ESSEC Business School dont elle dirige le centre de recherche sur le risque, CREAR, et la filière actuariat ESSEC-ISUP. Titulaire d'un doctorat en Mathématiques Appliquées (UPMC-Paris 6 & Center for Stochastic Processes, UNC Chapel Hill – Postdoc à Cornell Univ.) et d'une HDR, elle est également Actuaire Agrégée de l'Institut des Actuaires. Marie Kratz mène ses recherches dans le domaine des probabilités, de la statistique, de l'analyse et la gestion des risques, avec une spécialisation en théorie des valeurs extrêmes, domaines clefs pour les applications qu'elle développe à l'ESSEC et avec des partenaires internationaux, tant académiques que professionnels.

De la Résilience humaine

à la résilience collective face aux cybercrises avec la BEPA-Cyber

Par Florence Esselin

« Ce que j'ai fait, je te le jure, jamais aucune bête ne l'aurait fait ».

C'est ainsi qu'Henri Guillaumet résuma à son ami Antoine de Saint-Exupéry, venu à son secours, son héroïque survie dans l'hiver de la Cordillère des Andes, marchant sans arrêt cinq jours et quatre nuits pour regagner la civilisation après la panne de son Potez 25 de l'aéropostale[1].

(1) Image du musée de la poste https://www.argentina-exceptionvoyage/aeropostale/accident-guillaumet-andes

FLORENCE ESSELIN

Conseiller expert en numérique et sécurité du numérique
Mission numérique de la Gendarmerie nationale

« Après deux, trois, quatre jours de marche, on ne souhaite plus que le sommeil. Je le souhaitais. Mais je me disais : Ma femme, si elle croit que je vis, croit que je marche. Les camarades croient que je marche. Ils ont tous confiance en moi. Et je suis un salaud si je ne marche pas ».

© Musée de La Poste

Par le livre qu'il lui dédie, Terre des Hommes, Saint-Exupéry rapporte le témoignage de son ami, lui rend hommage et fait perdurer le souvenir de ce héros discret, pionnier de l'aéronautique moderne. C'est l'éclairage qu'il nous apporte sur les ressorts de la résilience humaine qui nous intéresse ici plus particulièrement.

Car même si cette extraordinaire aventure eut lieu dans les années trente, elle a ceci de commun avec notre présent qu'elle est le fait de pionniers rompus à une nouvelle technologie de l'époque – l'aéronautique – qui ouvraient de nouvelles voies de communication, de commerce et de transport, raccourcissaient les délais et surmontaient les obstacles naturels pour le progrès d'un monde en pleine transformation...

Une résilience fondée sur le chevauchement d'un torrent numérique

Les psychologues définissent la résilience humaine comme « le fait de rebondir, de se reconstruire après un ou des traumatismes » (cf. Jacques Lecomte). Elle exprime la capacité d'un individu à faire face à des situations difficiles ou génératrices de stress ; pour le neuropsychiatre Boris Cyrulnik, c'est « l'art de naviguer dans les torrents ». Or, la transformation numérique de nos sociétés modernes y projette les êtres humains :

– un torrent d'informations, qu'aucun individu n'est plus en capacité d'absorber, qui se déverse à une telle vitesse qu'on n'accorde plus le temps nécessaire à la vérification de ses sources, ni à son exploitation pour une réflexion dans la durée ;

– un torrent de sollicitations, ayant pour but de récupérer de la donnée auprès des individus avec leur accord ou même à leur insu, par des capteurs divers. Ils peuvent aller du compte « gratuit » d'un réseau « social » incitant à y exposer les moindres instants de sa vie privée, à la montre connectée qui, mieux que le médecin traitant, connaît notamment le rythme cardiaque et les efforts consentis par l'individu qui la porte et qui, souvent, aurait besoin qu'on lui remette les pendules à l'heure dans le domaine de la protection des données à caractère personnel.

Dans les cinq prochaines années, il est prédit que le nombre d'objets connectés dépassera le nombre d'humains sur terre. On avance aussi que l'intelligence artificielle va supplanter l'intelligence humaine, notamment en médecine et dans les métiers du droit. Aujourd'hui, aucun étudiant ne peut plus raisonnablement considérer que ses études lui donneront accès à un métier pérenne. Sa seule certitude est qu'il devra s'adapter sans cesse à l'évolution de la technologie, sinon s'orienter à temps vers des métiers qui ne seront pas encore conquis totalement par les machines ou inventer de nouveaux métiers. Qu'adviendra-t-il de lui en cas d'échec ? Qu'en sera-t-il de ses parents, encore moins préparés que lui aux innovations et aux tempêtes du cyberespace ? Faut-il réellement se réjouir des progrès technologiques qui vont permettre d'évaluer dès la naissance – et même avant – le coût des opérations

chirurgicales, des traitements et des prothèses qui devront équiper un individu tout au long de sa vie ? [2] Faut-il se réjouir de la perte de libre arbitre du conducteur de véhicules automobiles fortement assistés et bientôt remplacés par des véhicules autonomes ?

Il y a de quoi ressentir un fort stress devant la transformation numérique que nous commençons à connaître au XXIe siècle, d'autant que seule une infime partie de la population est en capacité d'en comprendre les ressorts techniques, économiques, géopolitiques et stratégiques. Il est probable que ce stress sera moindre pour les enfants du XXIe siècle, habitués tout petits à porter des mouchards pour renseigner en temps réel leurs parents inquiets pour leur sécurité, mais exposant avec fierté sur Internet leur moindre activité.

(2) Google Has Released an AI Tool That Makes Sense of Your Genome - AI tools could help us turn information gleaned from genetic sequencing into life-saving therapies. by Will Knight, MIT Technology Review, Dec 4, 2017; "Grâce à la data, nous allons vers une médecine prédictive" – Lavinia Ionita, https://experiences.microsoft.fr/business/intelligence-artificielle-ia-business/medecine-predictive-lavinia-ionita/

Give me your tired, your poor,
Your huddled masses yearning
to breathe free,
The wretched refuse
of your teeming shore.
Send these, the homeless,
tempest-tossed to me,
I lift my lamp beside the golden door!

Envoyez-moi vos fatigués, vos pauvres,
Envoyez-moi vos cohortes qui aspirent
à vivre libres,
Les rebuts de vos rivages surpeuplés
Envoyez-les-moi, les déshérités,
que la tempête m'apporte,
De ma lumière, j'éclaire la porte d'or !

Emma Lazarus, 1883, Le Nouveau Colosse – Sonnet gravé au pied de la statue de la Liberté

Une exposition maximale qui comporte des risques

Balivernes ! Penseront certains. On ne s'oppose pas au progrès, sous peine de nager à contre-courant. Nous sommes donc d'accord pour reconnaître dans le progrès actuel du numérique, un torrent au sein duquel tout individu devra trouver la force de nager pour vivre et s'épanouir.

Dès à présent, ce torrent n'a rien d'un long fleuve tranquille : la cybercriminalité y est omniprésente, on doit appliquer un minimum de règles de sécurité pour y éviter les ennuis, car il n'y existe pas encore de balisage de zones dangereuses, à part le bas-fond que constitue l'Internet obscur (darknet), pas plus qu'il n'y a de maîtres-nageurs ou de sauveteurs, sauf dans les zones protégées de quelques entreprises et institutions capables de se doter de ces talents rares.

Pour le moment, les conséquences des cyberattaques pour les particuliers restent limitées à l'exposition de leurs données personnelles voire intimes (captation de conversations privées sur ordiphone, piratage de la webcam ou de l'assistant virtuel installé dans le salon), la facilitation de larcins et d'escroqueries par l'exploitation des informations publiques (comme indiquer sur un réseau social son prochain départ en vacances, tandis que l'adresse du domicile à visiter par les cambrioleurs est rappelées sur le même réseau), l'extorsion d'argent par divers moyens comme les rançongiciels, le phishing, les escroqueries aux faux placements ; si « plaie d'argent n'est pas mortelle », comme dit le dicton, en revanche le cyberharcèlement et l'exposition aux pédophiles en ligne peuvent entraîner des séquelles plus graves pour leurs victimes.

Dans la lutte contre le cyberharcèlement, par exemple, l'article de Marlène Dulaurans et de Jean Christophe Fedherbe, « *De la victime au prédateur : les sciences humaines et sociales pour repenser le phénomène du cyberharcèlement* », nous rappelle la nécessité « d'étudier les comportements spécifiques attachés au cyberharcèlement et [d'] identifier les stratégies d'influence et de manipulation enclenchées par les prédateurs lorsqu'ils commettent leurs exactions », ce qui est l'objet de leur projet de recherche CyberNeTic.

Au-delà de la compréhension du phénomène, on peut s'interroger sur la façon dont une victime de cyberharcèlement peut se réconcilier avec les outils technologiques qui ont été les armes de ses bourreaux, pour reprendre sa nage dans le torrent du numérique.

Comprendre les caractéristiques d'une situation critique

La compréhension des phénomènes cyber apparaît alors comme un facteur facilitant – si ce n'est une condition – la résilience

des victimes de cyberattaques.

En effet, sans paraphraser les travaux de psychologues tels que Jacques Lecomte (*La résilience, se reconstruire après un traumatisme)* ou Boris Cyrulnik *(La trilogie de la résilience : Un merveilleux malheur - Les vilains petits canards - Le murmure des fantômes*), on peut toutefois exposer quelques principes qu'ils ont identifiés, concernant la résilience humaine, et qui s'appliquent également dans le contexte du cyberespace et des traumatismes qui peuvent affecter des victimes de cybermalveillances et de cyberattaques.

Tout d'abord, Jacques Lecomte affirme que « trois éléments sont essentiels pour la reconstruction psychologique des personnes ayant subi un ou plusieurs traumatismes : le lien, la loi symbolique et le sens ». Par le lien, on comprendra la possibilité de s'appuyer sur d'autres personnes. Par loi symbolique, on comprendra la démarche de l'individu, exposé au stress et à la souffrance, consistant à se fixer des objectifs et à élaborer une stratégie pour y parvenir. Le sens est le motif de se battre.

Dans de nombreux cas rapportés par ces spécialistes, l'expérience de leur vulnérabilité a été au cœur de la survie des individus.

Saint Exupéry rapportait déjà l'illustration de ces principes dans la survie de Guillaumet, qui s'épanchait auprès de son ami.

On peut trouver le sens et la loi symbolique dans l'analyse faite par Saint Exupéry : « *Il sait qu'une fois pris dans l'événement, les hommes ne s'en effraient plus. Seul l'inconnu épouvante les hommes. […] Sa grandeur c'est de se sentir responsable. […] Responsable de ce qui se bâtit de neuf, là-bas, chez les vivants, à quoi il doit participer. Responsable un peu du destin des hommes, dans la mesure de son travail. […] Être homme c'est précisément être responsable* ».

Enfin, un détail nous intéressera encore dans cette survie « impossible » : Guillaumet eut un moment la tentation de se laisser mourir, pour ne plus souffrir. Mais il réfléchit au fait que sa femme, veuve, ne toucherait rapidement son assurance vie qu'à la condition qu'on retrouvât son corps, ce qui ne serait pas possible compte-tenu du relief s'il restait à l'endroit où il s'était couché, épuisé ; il se releva pour changer d'endroit et ne s'arrêta plus de marcher jusqu'à son salut.

Voilà bien un exemple de l'utilité de la connaissance des caractéristiques techniques d'une situation critique dans la résilience humaine.

L'état de la résilience collective face à une cybermenace

(3) Club des Experts de la Sécurité de l'Information et du Numérique www.cesin.fr

Les témoignages des membres du CESIN[3], réunis le 15 novembre 2019 sur le sujet de la

gestion de crises cyber, tendent à confirmer que la résilience des organisations victimes de cyberattaques majeures suit des principes similaires.

En effet, l'un des principaux enseignements est l'effet fédérateur d'une crise, qu'elle soit simulée ou réelle. Elle contraint des personnes, qui se côtoient d'ordinaire sans travailler ensemble, à se battre de concert contre une agression touchant le collectif. La lutte pour sortir de la crise devient un projet fédérateur comme rarement il y en a dans une entité.

La crise peut donc être ressentie par chaque individu comme ayant *in fine* un effet positif, à condition que la communication et l'organisation de la gestion de crise soient efficaces. Cette efficacité passera par la clarification de la situation et par l'expression de la vérité, pour instaurer la confiance. On retrouve donc ici simultanément le lien social qui permet de surmonter la crise collectivement et la satisfaction de trouver une raison de se battre ensemble. Celle-ci apparaît d'autant plus évidente dans certains secteurs tels que la santé, où l'enjeu du combat dépasse la survie de l'entreprise en s'étendant à la santé des patients, voire à leur vie.

Lever l'incertitude de la situation est l'objectif prioritaire commun à toutes ces expériences : il faut déterminer le plus vite possible dans quelle mesure l'attaquant a pu pénétrer dans le système d'information, se ménager des portes dérobées et piéger le système pour actionner des charges destructrices dès qu'il en sera expulsé. C'est une des conditions à l'élaboration d'une tactique de réponse adaptée concernant toute l'entité. L'effort des spécialistes en sécurité du numérique ne porte pas seulement sur le diagnostic et la compréhension rapides du phénomène sur un plan technique, il consiste aussi à communiquer clairement avec les non-spécialistes pour lever leurs inquiétudes et incertitudes et pour mieux les associer à la résolution de la crise.

Il est alors recommandé de se doter d'outils de communication préparés avant que ne survienne une cybercrise et de les tester pendant des exercices pour mieux les maîtriser.

BEPA-Cyber ou l'évaluation de la dangerosité

(4) Pour "Base d'Estimation des Potentiels d'Attaques cyber"

Parmi ces outils, la BEPA-cyber[4], échelle de dangerosité des cybermenaces élaborée par un groupe de réservistes de la Gendarmerie nationale, commence à faire ses preuves. Initiée en 2012 et régulièrement améliorée, elle a fait l'objet de plusieurs publications dont un article de la revue de la gendarmerie nationale du 4e trimestre 2013 (revue n° 248, pages 112 à 125). Les principes restent valides mais l'application a été simplifiée par l'adoption d'une

grille permettant d'additionner simplement les valeurs de 0 à 2 de chacun des cinq critères retenus et en supprimant l'emploi des logarithmes peu usités. L'idée initiale était de créer une échelle internationale pour communiquer auprès des populations sur la gravité des cybermenaces à l'instar de l'échelle INES créée pour communiquer sur les incidents nucléaires, ou de l'échelle de Richter utilisée pour informer de la force des séismes.

Niveau BEPA-Cyber =
Origine + Précision + Sophistication + Visibilité + Fréquence

	0	1	1,5	2
Origine	Individu isolé peu compétent en informatique agissant pour son propre compte	Individu isolé compétent en informatique mais sans expertise SSI	Individu isolé expert OU Bande organisée de niveau de compétence faible à moyen	Groupe d'individus experts, organisés, dotés de moyens potentiellement importants.
Précision	«au hasard» sur le cyberespace	orientée vers un continent, une union d'états ou les intérêts nationaux	ciblant des victimes présentant des caractéristiques communes	visant précisément une personne (physique ou morale)
Sophistication	Outils d'attaque triviaux	Outils élaborés génériques prêts à l'emploi	Outils sophistiqués, adaptés au contexte	Outils hautement sophistiqués
Visibilité	Menaces diffusées avant l'attaque.	Attaque constatée immédiatement par ses effets sur le SI.	Attaque discrète laissant des traces sans perturber le SI	Attaque laissant très peu ou pas de traces visibles
Fréquence / Persistance	Aléatoire	Récurrent et irrégulier	Récurrent et régulier	Permanente / Continue pendant un moment

La grille BEPA.

Cette échelle BEPA-Cyber propose de coter de 0 à 10 la dangerosité d'une cybermenace, d'après le profil succinct du ou des attaquants supposés (critère « d'origine »), les outils mis en œuvre ou les vulnérabilités exploitées par l'attaquant (critère de « sophistication » des moyens d'attaque), la discrétion de l'attaque (critère de « visibilité » de l'attaque), la persistance de l'attaque (critère de « fréquence » et de « persistance ») et l'étendue de l'attaque en type et localisation des victimes (critère de « précision » relatif au périmètre des cibles attaquées).

Certes, lors de la découverte d'une attaque bon nombre de ces éléments sont encore inconnus ; durant le traitement de la crise certains éléments peuvent être réexaminés en fonction des hypothèses validées ou contredites. Toutefois l'outil présente

l'avantage de sortir du jargon des informaticiens et des "cybercombattants" pour adopter des termes simples, compréhensibles par tous ; il incite à répondre à cinq questions primordiales :

– Les vulnérabilités exploitées et les outils d'attaque utilisés sont-ils triviaux ou plus ou moins élaborés ?

– Est-ce que l'attaque visible masque une manœuvre plus insidieuse, une attaque persistante avancée ?

– Est-ce une attaque ciblée ?

– Quel type d'attaquant pourrait en être l'auteur ?

– Est-ce que cette attaque est susceptible de se reproduire régulièrement ?

Ces questions contribuent à éclairer la situation et à orienter la tactique de défense. De surcroît, la base d'estimation des potentiels d'attaques cyber (BEPA-cyber) permet de rechercher des attaques passées aux caractéristiques similaires ; si l'on prend garde à ne pas faire d'amalgame abusif avec la situation vécue, ceci peut renseigner sur des cas proches et inspirer des actions de défense, ou du moins concrétiser par des exemples une situation encore mal identifiée.

La BEPA-cyber contribue ainsi à la communication et à lever l'incertitude d'une situation de crise.

Hors crise, en synthèse d'un audit, elle permet également d'estimer la difficulté de mise en œuvre d'une attaque réussie contre le système audité. C'est aussi un outil de sensibilisation aux risques cyber, mettant en évidence en quelques questions les types d'attaques auxquelles une petite entité peut être exposée.

Témoignage d'Éric B. (RC) qui emploie la BEPA-Cyber : « Fort heureusement nous avons peu d'attaques ciblées mais pour chaque analyse je propose la BEPA-cyber d'une part en communication téléphonique, point de suivi d'un incident, et d'autre part lors de la remise du rapport dans son abstract. Ainsi, d'un coup d'œil - et c'est le but – on voit si c'est un "séisme" ou pas.

La BEPA-Cyber est utilisée et bien accueillie mais encore trop peu connue y compris par le CERT avec lequel je travaille ; mais j'en fais la promotion dès qu'il y a une attaque ou une mini analyse à mener et j'échange avec les mots clés que je connais par cœur maintenant : visibilité, sophistication, origine, *etc.* Cela permet d'être clair et précis.

Cependant, un point de vigilance sur la note : sans vouloir faire peur, il faut être prudent. Avec l'expérience, je note au plus juste - le système de résilience joue sur la sophistication. »

L'approfondissement de ses possibles applications a révélé un outil efficace pour la résilience nationale face aux menaces cyber :

– Un indicateur concis pour l'information rapide des autorités en cellule de crise,

– Un référentiel ordonné des cyberattaques rendues publiques, utilisable par les journalistes comme par les responsables sécurité des systèmes d'information à fin de sensibilisation,

– Un outil d'autodiagnostic de cybersécurité pour les entités dépourvues de spécialiste (PME/PMI, professions libérales et particuliers notamment),

– Un outil de repérage des guides et des produits de sécurité pour permettre une orientation autonome des utilisateurs vers des mesures et produits de sécurité adéquats,

– Un indicateur de vulnérabilité des systèmes audités pour les rapports d'audit,

– La classification des alertes de sécurité pour une priorisation plus efficace de leur prise en compte,

– L'analyse macroscopique rapide des risques, notamment pour des homologations simplifiées, *etc.*

Ces travaux ont reçu dès 2014 le soutien du directeur général de la Gendarmerie nationale, du Commandant de la Cyberdéfense et du préfet délégué à la DMISC. Le directeur général de l'ANSSI s'est également montré intéressé par cet outil. Les présentations de la BEPA-Cyber par ses inventeurs au FIC et au sein d'associations de professionnels de la sécurité numérique (dont le CESIN) ont suscité un intérêt dépassant le périmètre interministériel et son emploi par des responsables sécurité d'organismes bancaires, d'assurance et d'établissements publics culturels notamment.

La revue stratégique de cyberdéfense, demandée par le Premier ministre et publiée le 12 février 2018 par le secrétariat général de la défense et de la sécurité nationale, a apporté une certaine reconnais sance à ces travaux. En effet, celle-ci souligne la nécessité « d'adopter un schéma de classement des cyberattaques » (cf. chapitre II.5.3 : « Définir une doctrine d'action ».) facilitant la réaction des autorités « dans le tempo de la crise ». Elle explique que l'État français cherche à établir ce schéma de classement en transposant une échelle de qualification d'impacts des cyberattaques récemment élaborée par les services américains - qui s'avère mal adaptée à nos besoins nationaux - en y adjoignant, « afin de définir plus précisément la gravité d'une attaque », au moins cinq critères[5]

(5) Les critères mentionnés sont un critère «d'intensionnalité», un critère de «dangerosité» relatif à «la nature des cibles», un critère «d'attribution» c'est-à-dire «la nature de l'attaquant», un critère «de massivité ou de volumétrie», et un «critère de récurrence».

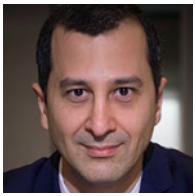
caractérisant les cyberattaques indépendamment de leurs impacts. Ceux-ci sont similaires aux cinq critères de la BEPA-Cyber définis pour caractériser la dangerosité des cybermenaces, indépendamment des impacts propres à chacune de leurs cibles.

On peut donc estimer que la France était un précurseur en la matière grâce aux travaux d'un groupe de réservistes citoyens de la cyberdéfense de la Gendarmerie nationale et que cette reconnaissance officielle de la pertinence de la BEPA-Cyber justifie sa mise en œuvre à l'échelle nationale et sa diffusion internationale.

Remettre l'humain
au cœur de la cybersécurité

Par Yuksel Aydin

Dans la lutte contre les diverses formes de cybercriminalité, la solution logicielle est devenue un domaine d'investissement conséquent, parfois au détriment de l'humain dont certains envisagent de relayer l'activité, voire de la remplacer par des processus automatisés. En effet, la puissance de calcul de l'informatique impressionne, le développement de l'intelligence artificielle est prometteur en matière de détection et de réaction aux attaques, l'informatique quantique annonce une remise en cause de paradigmes qui subjugue, notamment dans le domaine de la cryptographie. Si d'aucuns annoncent déjà la substitution dans le domaine de la cybersécurité de pans entiers d'activités humaines par des applications, d'autres ont depuis longtemps propagé un discours culpabilisateur à l'égard des employés : l'humain serait le maillon faible de la cybersécurité. Cette vision déshumanisée de la cybersécurité rentre pourtant en contradiction avec une approche pragmatique dans laquelle chaque employé peut constituer un relais efficace de la politique de sécurité.



YUKSEL AYDIN

Directeur
de la cybersécurité
Maison Christian
Louboutin

En matière de sécurité opérationnelle, l'intelligence humaine est nécessaire, irremplaçable. Les systèmes d'information (SI) d'une entreprise sont constitués d'un ensemble de couches technologiques complexes (poste de travail, serveurs, Linux, Windows, iOS, cloud computing, site web, base de données, authentification, Wi-Fi, sphère applicative etc.). Il ne peut être raisonnablement demandé à une solution logicielle de savoir gérer la sécurité de toutes ces technologies, de faire face à l'inconnu en permanence et de savoir s'adapter sans cesse. C'est pourtant ce

que l'on demande à un expert en sécurité informatique.

En matière de stratégie de défense et de sécurité, la protection de l'information se conçoit globalement dans un environnement où la surface d'attaque est devenue considérable.
Ainsi, tout ordinateur, tout téléphone portable est un point d'accès à une information ou à un système d'information.
L'expérience montre qu'au lieu de dénigrer le comportement de l'utilisateur, l'entreprise gagne systématiquement en valorisant l'action individuelle et en faisant participer localement chaque employé à une chaîne d'alerte générale de l'entreprise.

C'est cette entreprise sous ses différentes facettes (culture, histoire, organisation, métiers, jeu de responsabilités, ses réussites et ses souvenirs difficiles, *etc.*) qu'il faut savoir comprendre. La politique de sécurité et les actions qui en découlent sont spécifiques à un secteur d'activité et à une entreprise car il n'existe pas de « copier-coller » efficace dans le domaine de la cybersécurité. Un discours utile s'adapte à son interlocuteur et on sensibilise différemment un agent comptable, un informaticien ou un membre du comité exécutif.

De la filière spécialisée à l'ensemble des employés d'une entreprise, la cybersécurité constitue un challenge collectif. Grande ou petite mesure, chaque employé a un rôle à jouer : il est temps de remettre l'humain au cœur de la cybersécurité.

I- L'humain, clef de voûte de la filière en charge de la cybersécurité

A – L'expert en cybersécurité : un ensemble de compétences variées et non substituables

La constitution d'une filière spécialisée en sécurité appelle un ensemble de compétences vastes et complexes qui sont difficiles à acquérir. Pour le comprendre aisément, plaçons-nous du côté d'un hacker[1]. Lorsqu'un pirate se fixe pour objectif de rentrer dans un système d'information, il déroule une première phase de repérage. Durant celle-ci, il va recueillir un ensemble d'informations très éparses telles que des points de connexions de l'entreprise sur l'Internet (ex. liste des adresses IP publiques) et la litanie des technologies utilisées, accessibles sur les offres d'emploi, les CV en ligne et autres réseaux sociaux, *etc.*

(1) Ex. à travers la méthodologie du NIST : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

À partir de ces informations, le cybercriminel déterminera le ou les vecteurs qui lui permettront de rentrer dans le SI. Une fois dans celui-ci, le pirate entre alors dans une nouvelle phase : la découverte et la cartographie du réseau. Pour ce faire, il comparera le plus souvent l'éventail des technologies présentes avec des bases

de données de vulnérabilités accessibles gratuitement sur Internet.

Cette description simplifiée de l'approche d'un hacker donne une idée du niveau requis pour être en mesure d'exercer avec efficacité des fonctions en cybersécurité, en particulier :

– Connaître et comprendre des domaines vastes de l'informatique afin de les sécuriser ;

– Avoir une capacité d'adaptation pour faire face à des situations imprévisibles ;

– Pouvoir prendre des mesures à fort impact, de manière ad hoc, dans des conditions d'urgence et sous pression, tout en en mesurant les éventuels effets de bord.

Si un outillage adapté (système de monitoring, d'alerte, d'investigation, SIEM, *etc.*) est utile et nécessaire à l'activité d'un expert en cybersécurité, il ne peut se substituer à lui sauf à encourir très rapidement des effets de bord dévastateurs comme par exemple : une suppression automatique de fichiers professionnels sains par un système de protection réagissant incorrectement, une indisponibilité durable d'un SI considéré à tort comme malveillant, des flots d'alertes inutiles aboutissant à l'abandon de la surveillance, *etc.*

L'entraide professionnelle revêt un intérêt particulier car elle permet d'informer l'expert en cybersécurité des menaces en cours, voire de l'aider en cas d'incident. La constitution d'une chaîne humaine de solidarité et de confiance, d'amitié, prend ici tout son sens. La participation à une association professionnelle permet alors à l'expert en cybersécurité de nouer et renforcer des liens avec des partenaires qui sauront l'épauler et le conseiller dans les moments clefs.

B – La constitution d'une filière opérationnelle qualifiée

Sur le plan national, le développement d'une large gamme de formations, de diplômes et certifications a été favorisé, notamment à l'initiative des services de l'État (ministères, centre de formation de la SSI, services de renseignement) et d'associations telles que le CESIN, le CLUSIF, l'OSSIR, le Forum des compétences, le GITSIS, l'ARCSI, CyberEdu, etc.

Malgré la pénurie de candidats, l'offre de formation est aujourd'hui présente au sein des filières scolaires, permettant ainsi à l'excellence française d'être reconnue internationalement. Ainsi, plus de 100 formations longues sont aujourd'hui dispensées par des établissements d'enseignement supérieurs[2]. Toutefois, cette offre de formation reste à développer pour ceux qui sont déjà inscrits dans la

(2) « Présentation au ministère des Armées », Thomas CLOCHON et Yuksel AYDIN, 2018.

vie active et elle constitue un frein, notamment dans le cadre d'une réorientation ou reconversion professionnelle, en raison de son manque d'adéquation avec des besoins de formations et des parcours professionnels en défaut de visibilité sur le long terme et sur les possibilités d'évolution de carrière.

Au sein de l'entreprise, la filière en charge de la cybersécurité est en cours de constitution. Il s'agit d'une fonction pérenne, amenée à se développer en parallèle au recentrage des processus de production autour des SI. Toutefois, cette filière est assez mal comprise et mal définie au sein des organisations car elle est encore trop souvent confondue, voire cantonnée, au métier d'informaticien.

L'organisation de la cybersécurité (définition des fonctions, recrutement, formation, plan de carrière etc.) est alors dévolue au Directeur de la cybersécurité, amené à associer les ressources humaines dans une démarche longue de constitution de la filière.

C – La fonction de Directeur de la cybersécurité

La fonction de responsable de la cybersécurité est actuellement en mutation. Né au sein des services informatiques, le RSSI quitte durablement la direction des services informatiques (DSI) des entreprises, ayant atteint un niveau de maturité fonctionnelle et organisationnelle. De responsable au sein de la DSI, il devient Directeur de la sécurité des systèmes d'information[3] (DSSI) couvrant l'ensemble des besoins de l'entreprise en la matière.

(3) « La professionnalisation des métiers en charge de la cybersécurité », Yuksel AYDIN, rapport du ministère de l'économie et des finances, 2018.

Le DSSI est notamment en charge de définir une politique transversale en matière de cybersécurité, d'élaborer une stratégie de mise en œuvre de cette politique et de prendre la direction des opérations en cas d'incident grave. De plus, il dispose d'un rôle de conseiller du dirigeant, permettant notamment à ce dernier de contrebalancer et de « challenger » les orientations présentées par le DSI.

Enfin, le risque numérique a pris une place prépondérante au sein des entreprises. La gestion et l'acceptation du risque résiduel sont de plus en plus encadrées par diverses réglementations et règles de conformité (RGPD, PCI-DSS[4], LPM-OIV, etc.) faisant peser sur le comité exécutif une responsabilité conséquente, parfois pénale. C'est dans ce cadre que le comité exécutif est nécessairement amené à se doter d'un DSSI, seul à même de le conseiller et de porter à sa connaissance des analyses qualifiées

(4) https://www.pcisecuritystandards.org/

Le DSSI par sa connaissance de la vie de l'entreprise peut proposer des stratégies transversales de sécurité des systèmes d'information aux décideurs et aux utilisateurs

et impartiales sur le risque cyber.

Le rôle et l'approche du DSSI varient sensiblement, parfois considérablement, selon l'entreprise dans laquelle il exerce[5]. Comprendre l'entreprise, sa gouvernance interne, son histoire, son secteur d'activité est fondamental. Penser que l'on pourrait appliquer les mêmes recettes de la même manière un peu partout serait une erreur : on passerait alors à côté de ce qui est important à protéger ; on n'associerait probablement pas les bonnes parties prenantes ; on ne trouverait pas la juste tonalité et la juste approche pour appliquer sa stratégie.

Prenons l'exemple de la sensibilisation et du contrôle. Certains secteurs profes-

(5) « https://www.ey.com/fr/fr/services/advisory/ey-consulting-tribune-rssi », Hervé SCHAUER et Yuksel AYDIN, 2018.

sionnels sont traditionnellement encadrés. Dans l'administration ou dans le secteur de la finance, la culture de contrôle est solidement ancrée dans les mœurs ; l'annonce d'un audit en sécurité ne sera certainement que le énième du trimestre (Bâle III[6], Sarbanes-Oxley Act) et n'étonnera pas. D'autres secteurs comme ceux de l'audiovisuel et du luxe, seront davantage réceptifs à des séances de sensibilisation.

(6) https://www.bis.org/publ/bcbs189.pdf

Cette capacité à appréhender les aspects uniques de son entreprise, de savoir coordonner et associer les responsables clefs, de comprendre, dans une certaine mesure, la psychologie de l'entreprise, seront des facteurs déterminants de réussite ou d'échec de sa mission.

II – La cybersécurité est l'affaire de tous

A – La nouvelle transformation des DSI : offrir des SI et un usage sécurisés

Une fois les SI mis en production, les mesures à mettre en œuvre pour les sécuriser peuvent être coûteuses et nécessiter un accompagnement au changement du responsable applicatif et des équipes concernées. Pour abaisser le coût et augmenter le niveau de sécurité, il est préférable de prendre en compte la sécurité en amont, dès la conception.

D'une part, les méthodologies IT classiques (COBIT1, ITIL etc.) constituent une base utile, saine, en particulier en matière de gestion de cycles et des mises à jour, qu'elles soient fonctionnelles ou de sécurité. D'autre part, la délivrance de formations dédiées à la sécurité propre au métier concerné (ex. sécurité des SCADA) apportera alors au chef de projet et aux développeurs un savoir-faire important.

La diffusion de méthodologies et d'une technicité en sécurité apportent donc un niveau de protection plus important pour un coût davantage maîtrisé. Incidemment, le niveau qualitatif des SI est globalement plus satisfaisant car les vulnérabilités ne sont parfois que le reflet de malfaçons techniques plus générales et plus profondes.

Une surface conséquente de vulnérabilités pourrait être couverte à travers une gouvernance renouvelée entre services informatiques et les utilisateurs finaux. En effet, la manière dont l'application sera utilisée est à prendre en compte en amont, de manière à prévoir un usage simplifié de la sécurité. En effet, est-ce à l'utilisateur d'appliquer des mises à jour ou peut-on automatiser cette fonction nativement lors du développement ? Est-ce à l'utilisateur de faire preuve d'ingéniosité et d'une mémoire académique pour définir une myriade de mots de passe complexes ou peut-on

lui fournir un logiciel de gestion de mots de passe ? Ainsi, l'écoute des besoins et la prise en compte de l'utilisation en amont permettraient de réduire considérablement la surface d'attaque. Pour ce faire, des échanges réguliers entre l'informaticien et l'utilisateur sont à mettre en place, de la conception de l'application jusqu'à sa livraison, et même au-delà.

B - La formation et la sensibilisation régulières de tous les employés : un besoin pérenne de l'entreprise

L'entrée au sein de l'entreprise est de plus en plus conditionnée par le respect de mesures relatives à la protection de l'information et des SI, le plus souvent au travers de la charte d'utilisation des outils informatiques à laquelle le contrat de travail fait référence. En cas de manquement, l'entreprise a la possibilité de prononcer des sanctions, voire, dans les situations les plus graves, d'engager la responsabilité de l'employé et de mettre un terme à sa collaboration.

Lors de la prise de poste, une première sensibilisation est utile. Cette formation est généraliste ou peut être davantage spécialisée si les fonctions de l'employé le conduisent à manipuler des informations sensibles (données confidentielles, à caractère personnel, etc.) ou à gérer des SI qui soutiennent ces informations.

L'organisation d'une sensibilisation annuelle de l'ensemble des employés à la sécurité est devenue un exercice nécessaire, voire un passage obligé par certaines mesures de conformité (ex. SWIFT[8]). L'agence européenne de la cybersécurité[9] (ENISA) et le ministère US de l'Intérieur[10] (DHS) organisent chaque année un mois de sensibilisation en octobre. Cet événement permet aux entreprises de s'inscrire dans une dynamique internationale et d'en bénéficier.

(8) https://www.swift.com/myswift/customer-security-programme-csp/security-controls?t-l=en

(9) https://cybersecuritymonth.eu/

(10) https://www.dhs.gov/national-cyber-security-awareness-month

La manière dont sont préparées et déployées les formations et la sensibilisation sont déterminées en fonction des analyses de risques (qu'est ce qui est réellement à protéger ? Quelles sont mes vulnérabilités ? etc.) et de la culture de l'entreprise. Ainsi, l'univers de la finance et du luxe disposent généralement de plusieurs points (offices, boutiques, datacenters, etc.) à travers le monde entraînant davantage de déplacements des collaborateurs à l'étranger. Il conviendra, par exemple, de dispenser davantage des conseils sur les accès WI-FI gratuits (aéroports, hôtels, *etc.*) et l'utilisation d'un filtre de confidentialité.

En outre, la protection de l'information dépasse le cadre de l'entreprise et concerne les prestataires amenés

à interagir avec le SI ou le patrimoine informationnel.

À ce titre, une sécurité contractuelle est à établir pour poser les conditions de fonctionnement et de comportement des prestataires (ex. accès VPN à partir

L'AUTEUR

Yuksel Aydin est Directeur de la cybersécurité de la Maison Christian Louboutin. Ayant exercé des fonctions de gouvernance et de coordination de réseaux de RSSI, Yuksel Aydin est notamment l'auteur de politiques de sécurité, d'analyses de risques et de plan de continuité d'activité d'entreprises et d'administrations des secteurs de la finance, de l'industrie et de l'Internet.

L'humain et la stratégie
de lutte contre la cybercriminalité

Par Jean-Nicolas Robin

Lorsqu'il s'agit de s'intéresser à la lutte contre la cybercriminalité et plus largement à la sécurité de l'espace numérique, il est souvent fait référence, à juste titre, à des solutions techniques. Celles-ci sont au cœur du système numérique et leurs perfectionnements permettent de filtrer un grand nombre d'attaques et de prévenir par la même occasion les actes de cybercriminalité. Néanmoins, en complément de ces solutions techniques toujours plus innovantes, l'humain et particulièrement son action préventive et sa réaction face à l'utilisation des réseaux numériques semble être une arme, voire l'arme principale, de lutte contre la délinquance numérique.

JEAN-NICOLAS ROBIN

Docteur en droit
Juriste AVOXA
Rennes

C'est par des actions de prévention et de formation (I) mais aussi par la capacité à gérer la crise et à actionner les leviers juridiques (II) que doit se construire une stratégie globale de lutte contre la cybercriminalité qui allie la technique, le juridique et l'humain.

Le propos se concentre sur la stratégie à mettre en place au sein d'une entreprise mais le volet préventif s'applique aussi aux particuliers, aux associations et de manière générale à tous les utilisateurs et/ou consommateurs du numérique.

I – La prévention des risques numériques

La prévention en matière de cybersécurité se fonde principalement sur deux leviers que sont l'éducation à la cybersécurité et la structuration de l'entreprise.

A- L'éducation à la cybersécurité

Faire connaître les risques numériques est, selon nous, certainement la première des actions à mener pour lutter plus efficacement contre la cybercriminalité. L'objectif est clair,

il s'agit d'initier et de protéger l'utilisateur afin d'éviter qu'il ne devienne la porte d'entrée des cyberattaquants.

Pour ce faire, plusieurs actions préventives peuvent être menées autour de la sensibilisation du public aux risques. Il s'agit véritablement d'éduquer l'utilisateur aux outils numériques et aux signaux faibles devant alerter. La difficulté de l'exercice réside dans la nécessité de trouver le consensus entre la volonté d'illustrer les risques sans créer un effet de « peur généralisée » des outils numériques qui, lorsqu'ils sont utilisés avec la sécurité adéquate, sont efficaces et indispensables au quotidien de chacun.

À titre d'exemple, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) a mis en place un guide de sensibilisation reprenant douze principes essentiels à respecter pour tenter de prévenir les risques numériques. Il peut être pertinent de les reprendre pour les illustrer avec des exemples venant de l'entreprise (sécurité des mots de passe, Wifi, usage professionnel et personnel d'un équipement numérique).

L'éducation à la cybersécurité est une prévention en continu, c'est-à-dire qu'elle doit se faire tout au long de l'année, en complément de formations et/ou de tests visant à évaluer la maturité des collaborateurs (test de *phishing* par exemple).

Ces mesures d'éducation à la cybersécurité ne peuvent aboutir sans une bonne structuration de l'entreprise.

B- La structuration de l'entreprise

Dans de nombreuses structures, privées ou publiques, le risque numérique est important du fait de l'absence d'harmonisation des pratiques de sécurité. Il s'agit par exemple de la manière de communiquer avec les tiers (mails sécurisés, prise de contact par téléphone avec la question de l'identification) mais aussi de l'organisation générale de la structure, à savoir la politique de sécurité des systèmes d'information (PSSI).

Mettre en place une PSSI n'est souvent que le dernier maillon d'une chaîne qui commence par l'adhésion de l'ensemble des collaborateurs et des cadres dirigeants à la nécessité d'appliquer des règles de sécurité informatique. Très souvent, il s'agit de mettre en avant le caractère protecteur de la PSSI dans le cadre du développement de la structure et de ses innovations. Néanmoins, il s'agit surtout de pédagogie et de communication pour faire passer le message de la prévention des risques numériques.

En complément de la prévention, la stratégie de lutte contre la cybercriminalité passe aussi par un accompagnement dans la conduite des actions répressives, par le recours à la voie judiciaire mais aussi par l'aide à la décision dans le cadre d'une gestion de crise.

II – La gestion active des incidents cyber

La principale problématique n'étant plus de savoir s'il va y avoir une attaque mais quand elle sera mise en œuvre, l'apport de l'humain est alors essentiel dans le cadre des actions correctives et répressives qui peuvent être menées. Il s'agit d'une part de la gestion de la cellule de crise et d'autre part du déclenchement des différentes procédures judiciaires.

A- L'humain au cœur de la gestion de crise

La gestion de crise est l'ensemble des moyens humains, juridiques et techniques permettant à une structure de faire face aux impacts affectant la structure attaquée. Pratiquement, elle consiste à prendre les mesures nécessaires pour stopper l'attaque cyber, analyser les failles pour les corriger et remettre le système en état de fonctionnement.

L'aspect humain est indispensable pour cette phase de réaction, notamment dans le cadre de la communication. En effet, il s'agit de communiquer avec différentes instances (obligations de déclarations d'incident à la CNIL et/ou ANSSI) mais aussi d'informer les victimes et de préserver la réputation de la structure. Une communication interne doit être organisée à destination des collaborateurs de la structure attaquée. Il s'agit, là aussi, d'informer sur les conséquences de l'incident et sur les mesures à prendre dans le cadre de sa résolution.

B- La gestion des procédures judiciaires et des responsabilités

L'attaque menée sur les moyens numériques de l'entreprise peut revêtir une qualification pénale, à savoir un acte de cybercriminalité. Les articles 323-1 et suivants du Code pénal prévoient la répression des atteintes aux Systèmes de Traitement Automatisés de Données (STAD). Déposer plainte donne alors la possibilité de réaliser des investigations pouvant amener vers une procédure pénale (poursuite, instruction) s'accompagnant de différents actes d'enquête.

La difficulté à laquelle se confronte nombre d'entreprises est la longueur des procédures. En effet, le temps judiciaire n'est pas le même que celui de l'entreprise et l'impérativité d'un redémarrage du système numérique de la structure est souvent primordiale face à un incident cyber.

Au sein de la police ou de la gendarmerie, des unités chargées de la lutte contre la cybercriminalité avaient été créées afin de conduire des enquêtes judiciaires pour identifier les auteurs d'actes de cybercriminalité. Des dispositions législatives, notamment la loi du 3 juin 2016, ont largement renforcé les capacités des services d'enquête pour gagner en efficacité et rapidité.

Au-delà du dépôt de plainte, il est nécessaire de s'interroger sur les responsabilités

encourues par les différents intervenants dans et en dehors de l'entreprise. Il s'agit, par exemple, de savoir si les procédures de vérification et de sécurité en interne ont été réalisées ou de rechercher les responsabilités contractuelles d'un sous-traitant. Sur ce point, la pratique montre qu'en général, les contrats ne contiennent pas de clauses précises sur les responsabilités en cas d'incident numérique. La réglementation européenne sur la protection des données (RGPD) a pourtant imposé aux différents responsables de traitement de données une obligation de sécurité mais celle-ci ne porte que sur les données à caractère personnel et ne prend pas en compte l'ensemble des actifs immatériels de l'entreprise.

Finalement, la lutte contre la cybercriminalité place la personne au cœur des préoccupations puisqu'il s'agit à la fois de sécuriser ses actions mais aussi de la protéger d'attaques pouvant avoir des répercussions importantes. Même si le volet pénal concerne les atteintes aux biens (notamment les articles 323-1 et suivants du Code pénal), la répression des infractions a pour objectif premier d'assurer la paix sociale et donc « le vivre ensemble », élément intrinsèquement humain. Ainsi, en complément de toutes les techniques développées dans le cadre de la cybersécurité, c'est désormais autour de l'humain qu'il faut « s'équiper » pour faire face et réagir.

L'AUTEUR

Docteur en droit et titulaire du Certificat d'Aptitude à la Profession d'Avocat (CAPA), Jean-Nicolas Robin est passionné par les nouvelles technologies et le numérique. Après avoir réalisé un mémoire de Master 2 sur le blanchiment à l'ère du numérique (Univ Rennes I), il a écrit une thèse de doctorat portant sur « La matière pénale à l'épreuve du numérique » (Univ Rennes I dir. Prof Ghica Lemarchand et M. Doare). Juriste au sein du cabinet Avoxa Rennes, il intervient dans le pôle droit des contrats et apporte ses compétences dans le domaine de la cybersécurité, de la protection des données à caractère personnel mais aussi en droit du sport.

Il a, par ailleurs, été assistant de justice au sein de Tribunal de grande instance de Vannes (2015-2017).

Jean-Nicolas Robin enseigne depuis plusieurs années la procédure pénale et le droit du numérique dans différentes structures (Institut Catholique de Rennes, Ecoles d'informatiques, Master Droit du numérique).

Auditeur jeunes de l'Institut des Hautes Etudes en Défense Nationale (2017 - Session Jeunes n°102), il s'intéresse aux questions de sécurité intérieure et de cybersécurité et plaide pour un rapprochement entre les sphères technique et juridique en matière de cybersécurité.

Femmes de la cybersécurité : la volonté de protéger autrui

Par Nacira Salvan

La protection numérique occupe une place grandissante dans les préoccupations des citoyens, des collectivités, des entreprises ou des institutions. Les métiers de la cybersécurité doivent-ils rester un no(wo)man's land ? Nacira Salvan, Présidente Fondatrice du CErcle des Femmes de la CyberSécurité ne le croit pas ; femme de conviction, experte depuis 25 ans pour ce sujet, elle constate que les lignes bougent… enfin.

Pour convaincre, nous avons besoin d'afficher des succès. En premier lieu, j'aimerais faire référence à l'action du Centre de lutte contre les criminalités numériques de la Gendarmerie nationale (C3N) qui a mis fin à une infection malveillante agissant en sourdine : plus de 950 000 machines affectées par *Retadup*[1] ont ainsi été désinfectées. Bien entendu, le CEFCYS a relayé cette réussite sur les réseaux sociaux et auprès de sa communauté. Le thème de la protection d'autrui fait écho aux attentes exprimées par les Femmes de la Cybersécurité lorsqu'elles parlent de leurs métiers.

NACIRA SALVAN

Présidente du CEFCYS

(1) https://www.zdnet.fr/actualites/retadup-le-coup-de-main-d-avast-pour-demanteler-le-botnet-39889659.htm

Pour preuve, lors de l'un de nos derniers colloques, des adhérentes ont témoigné des raisons qui les avaient poussées à faire carrière dans ce secteur ; plusieurs verbatim m'ont interpellée, tels que : « *Comment soigner des patients, sans les protéger des dangers numériques ? Mon métier a du sens* »… « *J'aime protéger les gens du mal, poursuivre les cybercriminels et continuellement apprendre* »… « *J'aime construire des programmes de sécurité, ou être au cœur d'un incident de sécurité ; mon métier est de trouver des réponses pour agir*

et protéger »… « *La cybersécurité consiste essentiellement à protéger les personnes contre les dommages et, lorsqu'une personne est victime, à découvrir qui l'a fait* »… Toutes évoquent le sens de leur action : protéger autrui.

Nous avons décidé de récapituler ces témoignages dans un ouvrage intitulé : « *Je ne porte pas de sweat à cagoule, pourtant je travaille dans la cybersécurité* » [2]. Ce livre, qui sera présenté au FIC, propose une approche inédite : c'est un plaidoyer en faveur des jobs et des parcours de formation possibles dans la cybersécurité, dès la formation initiale et tout au long de la vie professionnelle ; il contient une foule d'informations et de références utiles pour guider les jeunes en phase de choix, les parents soucieux de l'avenir de leurs enfants, ainsi que les professionnels de l'orientation. L'ouvrage témoigne aussi de la variété des métiers exercés par les femmes de la cyber et présente des visages auxquels on peut s'identifier. 20 *cyberwomen* évoquent ainsi leurs parcours, leurs convictions, leurs métiers sur des sujets variés comme la gestion de crise cyber, la blockchain et la cybersécurité, la sécurité de l'Internet des objets, le hacking éthique ou la cybersécurité dans l'industrie 4.0, la sensibilisation à la cybersécurité… il valorise des entreprises qui recrutent ou qui ouvrent les métiers de la cybersécurité aux femmes.

(2) Edité chez JePublie – janvier 2020.

L'état d'urgence en matière de besoin de compétences cyber : la maison brûle-t-elle vraiment ?

En moins de 5 ans, la digitalisation de la société a changé la donne : l'internet des objets, la mobilité, le cloud, les GAFA … ont profondément restructuré notre paysage technologique et économique. Certes, nous en voyons des bénéfices mais, dans le même temps, ils ont augmenté la vulnérabilité des systèmes et fragilisé les organisations. La montée exponentielle des cyberat-

taques à tous niveaux, individuels ou collectifs, est un fait partagé. Comment protéger les institutions, les collectivités, les entreprises, les citoyens ? C'est la question. Les pare-feux, les réglementations tel que le RGPD ou la directive NIS[3] sont de frêles remparts face aux assauts. Les cybercriminels ont compris le profit qu'ils pouvaient tirer de nos failles (souvent humaines) et de nos défauts d'organisation collective. Nous protéger signifie désormais améliorer nos capacités d'organisation, imaginer les scénarios d'attaque, informer… En fait, les réponses ne sont plus seulement d'ordre technologique.

(3) Le 10 mai 2018, la directive européenne Network and Information Security (NIS) est entrée en vigueur. La directive NIS a pour objectif de renforcer la sécurité des réseaux et des systèmes d'information dans l'Union, afin d'améliorer le fonctionnement du marché intérieur. Pour ce faire, les « opérateurs de service essentiel » et « fournisseurs de service numérique » devront mettre en œuvre, à leurs frais, les mesures pour identifier, prévenir, traiter et gérer, voire notifier, les risques et incidents de sécurité des réseaux et des systèmes d'information utilisés dans le cadre de leurs activités.

(4) Etude Kaspersky Lab – 2017 - https://www.kaspersky.fr/about/press-releases/2017_most-women-give-up-a-career-in-cybersecurity-before-the-age-of-16
Etude (ISC)2 2018 - https://www.isc2.org/-/media/7CC598DE43046919 5F81017658B15D0.ashx

Force est de constater que le temps presse. Les femmes ne représentent que 11 % de la population du secteur[4]. Dans le même temps, selon *Cybersecurity Ventures*, il y aura jusqu'à 3,5 millions de postes vacants en Europe d'ici 2021. À l'instar de ceux de la Santé, des Media, de l'Enseignement ou de la Justice, les métiers Cyber conjuguent technicité et convictions et les opportunités à saisir sont incroyables. Et c'est là que le bât blesse : Rien qu'en France, Orange Cyber Défense estimait l'année dernière à 1 000 le nombres de postes pourvus sur les 6 000 ouverts[5]. Dans ce contexte très tendu de recrutement, les femmes qui représentent la moitié de la population active sont… exclues ou s'auto excluent de ces emplois ! C'est un paradoxe incroyable et une absurdité.

(5) Michel Van Den Berghe, Directeur Général chez Orange Cyberdéfense. https://www.lemonde.fr/connaitre-et-comprendre-les-metiers-de-demain/article/2018/01/19

Informer, partager les expériences pour combattre les idées reçues

La formation est-elle la réponse magique ? C'est une réponse majeure, mais pas la seule. Encore faudrait-il que les femmes soient convaincues de leur place dans ce secteur. Peu guidées, pas assez informées, les femmes se détournent de la cyber. Plus globalement, sous le poids culturel des stéréotypes, les talents féminins désertent le numérique.

La filière de la cyber est victime d'un stéréotype selon lequel les sciences et le numérique conviendraient davantage aux hommes qu'aux femmes.
Ces dernières ressentent le « syndrome de l'imposteur » : une sensation de ne pas être légitimes dans ces domaines, qui les empêchent de se projeter dans les formations et les emplois cyber.
Ce phénomène est propre à la société

européenne ; il est intéressant de noter qu'en Asie, au Moyen-Orient ou en Russie, il en est tout autrement. ainsi que l'analyse Isabelle Collet dans le récent ouvrage « *les oubliées du numérique* » [6].

Parmi les causes du désamour, les stéréotypes occupent une place de choix. Selon une étude de Kasperksy Lab[7] réalisée auprès de 4 000 jeunes, un tiers des femmes pensent que les professionnels de la cybersécurité sont des geeks. Selon ce même cliché, l'informaticien est un homme, solitaire, asocial, peu soucieux de son apparence, passionné par la technique, plus à l'aise avec les machines qu'avec les êtres humains… Un portrait popularisé auprès du grand public à travers les films, les séries TV ou la presse….,[8 9]

La cybersécurité manque également d'organisations en mesure de montrer leur volonté d'ouverture de ces métiers aux femmes. Ce manque de mixité, conjugué à la pénurie générale de compétences, pose problème : comment faire face à la transformation digitale et à la montée des cybermenaces si plus de la moitié de la population ne s'y intéresse pas, est exclue ou s'auto exclut de la filière ? Les métiers de la cybersécurité doivent-ils rester un *no(wo)man's land* ? Non.

En conséquence, avant même de former et recruter, il faut d'abord combattre les a priori. Changer les mentalités ne prendra pas obligatoirement un temps fou. Mais les structures éducatives, les familles, les médias… doivent cependant changer de prisme. Il est évident que le modèle doit changer, car les stéréotypes négatifs et les problèmes de communication nuisent à tout le monde.

Pour faire évoluer les mentalités, chacun doit faire sa part : il faut démultiplier les actions d'information dès le lycée, car nous savons désormais que c'est à 16 ans que les *a priori* se cristallisent, et « évangéliser » les femmes actives en quête de réorientation. Le CEFCYS, comme d'autres associations et/ou les entités éducatives, s'investissent sur le sujet. Il nous faut trouver les mots, les arguments qui vont convaincre les femmes d'entrer dans le cyber. Le CEFCYS regroupe plus de 200 adhérentes qui, issues de tous les secteurs, ont choisi de s'orienter ou de se réorienter dans la cyber. Quelque part, ce sont des pionnières. Nous encourageons nos adhérentes à partager leurs expériences, à prendre la parole et à participer

(6) « les oubliées du Numérique » par Isabelle Collet , informaticienne et enseignante-chercheuse à l'université de Genève– Edition Le Passeur octobre 2019.

(7) Etude Kasperksy Lab 2017. https://www.kaspersky.fr/about/press-releases/2017_most-women-give-up-a-career-in-cybersecurity-before-the-age-of-16.

(8) www.onisep.fr - Séquences pédagogiques - Mixité des métiers et numérique http://www.onisep.fr/Pres-de-chez-vous/Hauts-de-France/Amiens/Informations-metiers/Le-numerique/Le-dossier-pedagogique/Mixite-des-metiers-et-numerique

(9) Médias et Culture Geek : Généalogie d'un lien intime par claudemussou ·18/09/2018 https://inatheque.hypotheses.org/1904.

Les besoins du marché nécessitent de mobiliser les compétences, sans discrimination de sexe, en luttant contre les a priori et en informant les postulantes éventuelles de l'existence de cette orientation professionnelle, profitable en termes de responsabilités et de curiosité intellectuelle.

à des événements tels que la Nuit du *Hacking* où les hommes constituent la grande majorité des participants.

La lumière au bout du tunnel ?

Dans les formations, les mentorats et le coaching que j'anime régulièrement, les femmes optent de plus en plus pour les métiers de l'audit ou de la gouvernance. Ce sont des signes encourageants. Les programmes de formation conduits par des écoles, les grandes entreprises, ou des centres tels que le C3N ont évolué pour attirer plus de femmes…Les « tech girls day » montent en puissance et commencent à produire des effets. Il s'agit de faire découvrir le numérique aux jeunes filles hors la présence des garçons…. L'idée a fait ses preuves aux Etats Unis et monte en puissance en France. Le CEFCYS et d'autres associations comme « ELLES BOUGENT » ou « STARTHER » ont entrepris de faire bouger les lignes en partenariat avec des entreprises moteurs parmi lesquelles : Cisco, Deloitte, Nokia, Bouygues Telecom, Capgemini ou encore GRT Gaz… Des ateliers, généralement d'une demi-journée sont destinés à des jeunes filles de la 3e à la terminale pour les sensibiliser aux métiers des domaines numériques et scientifiques.

Concernant la formation post bac, le CEFCYS a signé un partenariat avec la *Wild Code School* pour former 15 femmes à la cybersécurité. J'ai travaillé durant l'été avec l'école sur le contenu du programme pédagogique. La première session est entièrement consacrée aux aspects techniques pour former à des métiers de « pentesteuse »[10] et «d'analyste cybersécurité ».

(10) Un pentester est un professionnel de la sécurité informatique. Son rôle : contrôler la sécurité des applications (mobiles, back end des sites web qui enregistrent des données confidentielles comme les numéros de cartes bancaires par exemple…) et des réseaux informatiques (réseaux industriels : chaîne de montage aéronautique…) en opérant des tests d'intrusion (attaques contrôlées). D'où son nom : pentester est la contraction de «penetration test».

Ce sont des profils extrêmement demandés et malheureusement très rares sur le marché.

Il est vrai que certains emplois cyber exigent des compétences en informatique, en programmation ou en ingénierie de réseau. Mais un grand nombre d'emplois en cybersécurité demandent plus de compétences humaines que techniques : une pensée analytique, des capacités à travailler en équipe, des aptitudes en matière de communication et de leadership. Elles peuvent toutes être apprises dans des domaines autres que ceux de la technologie. La sécurité des systèmes d'information repose beaucoup sur les *process*.

Conclusion

Les métiers de la cyber font partie de ces milliers d'emplois « nouveaux », que les femmes et de façon plus large des jeunes diplômé.es doivent investir dès à présent. Les lignes bougent… encore trop lentement.

Y a-t-il une façon « spécifiquement féminine » d'exercer le métier de la cybersécurité ? Le débat est ouvert, mais nous ne l'engageons pas ici… Ce qui est certain, ainsi que le souligne le cogniticien Émile Servan Schreiber dans son ouvrage[11], c'est que la mixité et les visions complémentaires concourent au succès des projets. En situation de crise, les équipes mixtes fournissent davantage de créativité et d'innovation. La mixité est un enjeu majeur dans toutes les organisations.

(11) Émile Servan-Schreiber, spécialiste de l'intelligence collective & des marchés prédictifs, Docteur en Psychologie Cognitive, auteur de « Supercollectif. La nouvelle puissance de nos intelligences » Fayard 2018.

J'invite les femmes qui s'intéressent de près ou de loin à ce domaine à franchir le pas vers la cybersécurité, car elles peuvent s'épanouir et seront heureuses de servir les proches, la société, le pays et tout l'écosystème.

L'AUTEURE

Docteur en Informatique, Nacira Salvan, est certifiée CISSP, ISO27001 LI, ITIL Foundation3 et plus d'une quinzaine de certifications techniques sur plusieurs technologies sécurité du marché. Elle a exercé plusieurs métiers de la cybersécurité : conseil stratégique en SSI, responsable réseau/sécurité en charge du maintien en condition opérationnelle et de sécurité, directrice de projet SSI, responsable d'équipe architecte Sécurité, directrice cybersécurité, RSSI et RSSI opérationnel. Elle est conférencière et intervenante à l'UNESCO, pour la protection de l'enfance contre le danger du net, et également membre et ambassadrice en France pour l'organisation européenne #SaferInternet4EU. Membre du conseil de l'UFR d'informatique et mathématique de Paris 5, elle enseigne au master Cybersécurité de l'université Paris Descartes.

Présidente et fondatrice du CEFCYS et membre du Conseil Women4Cyber. Élue parmi les 100 personalités les plus influentes en Frances dans le domaine de la Cybersécurité par l'usine nouvelle.

L'initiative « Women4Cyber »

Par Anne Le Hénanff

Face à l'inquiétant constat que les ressources humaines et le nombre d'experts sont déjà aujourd'hui insuffisants dans le secteur de la cybersécurité et prenant en compte la sous-représentation des femmes dans la filière en Europe, ECSO (European Cyber Security Organisation)[1] a lancé, le 22 janvier 2019, l'initiative « Women4Cyber », fortement soutenue par Mariya Gabriel, alors commissaire européenne en charge de la société et l'économie digitales.

(1) https://ecs-org.eu/about

ANNE LE HÉNANFF

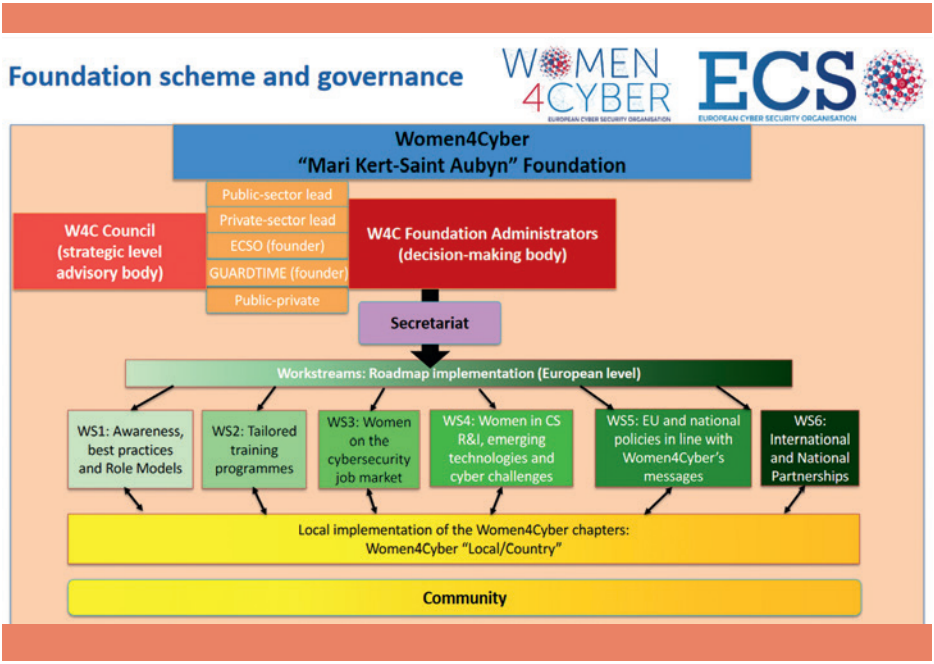
Pour le Women4Cyber

ECSO, ayant à son origine un contrat de partenariat public-privé sur la cybersécurité avec la Commission européenne, a pour mission de structurer un écosystème européen de cybersécurité en rassemblant en son sein différents types d'acteurs, y compris les administrations publiques nationales et régionales, les grosses entreprises, les PMEs, les universités et centres de recherche, *etc.* C'est dans la lignée de cette mission holistique qu'ECSO a créé Women4Cyber.

Membres fondatrices de l'initiative, 30 femmes d'Europe détenant des compétences de haut niveau des secteurs public, privé, académique ou associatif, ont été invitées à accompagner la structure avec l'ambition de proposer plusieurs actions communes ou individuelles au niveau européen, ainsi que et surtout dans leur propres pays :

– rassembler et fédérer les énergies dans chaque pays mais également au niveau du territoire européen pour valoriser la filière cybersécurité,

– trouver les actions pertinentes pour donner l'envie aux jeunes filles et aux femmes



© woman4 cyber

de s'engager professionnellement dans la filière trop souvent perçue comme masculine et peu attractive,

– adapter des actions dans chaque pays membre, en complémentarité des mesures déjà engagées par les écosystèmes nationaux,

– relayer les actions de Women4Cyber dans chaque pays par des opérations de communication et de participation à des événements dédiés (FIC,….)

– nouer des partenariats avec les universités, les écoles, les cabinets de recrutement et tous acteurs du secteur pour faire évoluer les pratiques et adapter les techniques,

– faire des recommandations et des propositions stratégiques à la structure de gestion de la fondation pour mener des actions pertinentes et agiles,

– valoriser dans chaque État et en Europe les « success story » professionnelles de femmes dans le domaine de la cybersécurité.

Aujourd'hui, Women4Cyber est portée par une structure légale officielle, la fondation

© ECSO

Le prix a été remis à Nina Hyvàrinen, membre du Conseil Women4Cyber, et au Secrétaire général de l'ECSO, Luigi Rebuffi, sur la scène de la conférence Cyber Security Nordic 2019.

« Women4Cyber Mari Kert-Saint Aubyn » qui est régie par un plan d'actions et une charte comprenant des objectifs stratégiques tels que l'accompagnement de l'environnement éducatif, la bonne connaissance du marché de l'emploi mais également l'intégration dans les réseaux et les communautés existantes.

La fondation comprend en son sein le Women4Cyber Council, un organe ad hoc de discussion qui fournit les recommandations stratégiques nécessaires à la fondation. Toutes les membres fondatrices de l'initiative ont été invitées à faire partie du Conseil qui a été lancé le 23 septembre dernier, à Rome, à l'occasion de sa première réunion. Luigi Rebuffi, secrétaire général d'ECSO, fait partie de l'organe d'administration de la fondation et il est membre du Conseil.

La fondation « Women4Cyber Mari Kert-Saint Aubyn » est prête à mener toutes les actions opérationnelles lui permettant d'atteindre son objectif et faire de l'Europe un espace motivant et ambitieux pour les femmes de la cyber. À cet effet, il lui est impératif de profiter du soutien de la communauté, que ce soit

au niveau de la promotion ou au travers de donations qui permettront la mise en place d'actions concrètes. Pour ses efforts, Women4Cyber s'est récemment vue décerner le « 2019 Cyber Security Nordic Award », un prix destiné à augmenter la visibilité et l'importance de la cybersécurité au niveau international à travers la promotion de la cyber expertise et de cyber experts.

Toutes les informations sont disponibles sur le site d'ECSO https://ecs-org.eu/workinggroups/news/women4cyber.

Women4Cyber est également présente sur les médias sociaux.

Cybersécurité :
l'humain à l'épreuve du numérique

Par Myriam Quéméner

Alors que le numérique envahit notre quotidien, à travers l'irruption des réseaux sociaux, des objets connectés, de l'intelligence artificielle, il est pertinent de s'interroger sur la place de l'humain dans ce nouvel écosystème numérique. Malgré une impression d'élimination de l'humain et le risque de son abdication devant les réseaux et les machines, il survit parfaitement tant dans le fil des innovations numériques qu'au niveau des dérives qu'il induit avec le développement, par exemple, de la cybercriminalité.

MYRIAM QUÉMÉNER

Magistrat, docteur en droit

L'humain, créateur de numérique

Big data, intelligence artificielle, machine learning, robots, les usages du numérique envahissent notre quotidien à une vitesse fulgurante si bien qu'on a tendance à penser que l'homme va progressivement disparaître.

En analysant les évolutions progressives du numérique, on constate d'abord un désir d'élimination de l'humain à travers l'image du cyborg[1] qui remplace l'homme puis, vers les années quatre-vingt, apparaît un « avatar » animé par un humain et enfin, on assiste actuellement à l'intégration du numérique par des consommateurs que l'on peut qualifier « d'humains augmentés ».

(1) Georges, Fanny. « A l'image de l'Homme » : cyborgs, avatars, identités numériques », *Le Temps des médias*, vol. 18, no. 1, 2012, pp. 136-147.

Aujourd'hui, le numérique est utilisé sous les formes les plus variées, allant du smartphone, aux objets connectés et à l'intelligence artificielle. Les objectifs du numérique sont d'améliorer la vie des citoyens, l'humain restant au centre des évolutions, mais on note aussi une ambivalence qui inquiète,

par exemple, avec le risque de remplacer l'homme ou de lui nuire.

La société numérique crée une véritable disruption[2] au niveau de la place de l'homme dans ce nouvel écosystème. Indépendamment de la personne physique, il existe aussi désormais une personne virtuelle, constituée par une masse de données sans cesse collectées à son sujet, qui est l'objet de toutes les convoitises. Dans ce contexte hyperconnecté, les outils numériques sont de puissants vecteurs de capture d'information qui s'affranchissent des frontières et des réglementations locales de protection de la vie privée. Face aux risques encourus par la diffusion sauvage d'informations, personnelles et sensibles, ou leur exploitation dans un but lucratif, l'individu connecté doit accepter d'assumer ses responsabilités, réagir et se montrer circonspect en limitant au strict nécessaire les informations qu'il met à la disposition de la société numérique.

(2) M. Quéméner « Le droit face à la disruption numérique », Gualino Lextenso 2018

© human resources management concept - Adobestock - n° de fichier : 265414925

L'humain connecté est responsable de la qualité des informations personnelles qu'il distille lors de sa pratique du Net. Il doit intégrer qu'une ingénierie sociale peut conduire à des usages illicites ou néfastes de ses données personnelles dans son environnement professionnel ou privé.

À y voir de plus près, on constate que les hommes sont toujours au cœur du numérique, qu'ils l'utilisent positivement ou négativement en dérivant vers la cybercriminalité. Il conviendra ainsi de présenter l'action humaine dans le développement des usages numériques au travers d'une ingénierie sociale.

La société exprime une peur croissante face à des technologies, parfois mal comprises, comme l'intelligence artificielle. Pourtant, nous ne sommes pas « dépassés » par le numérique, les programmes informatiques ne réalisant que ce pour quoi ils ont été conçus : la technologie ne nous échappe pas pour suivre sa « volonté ».

Si l'humain est au centre du numérique, ses interactions variées avec ce domaine posent des questions éthiques cruciales qui font l'objet de travaux de recherches. Il faut intégrer, dès le développement d'applications, une démarche fondée sur ces réflexions éthiques. On constate aussi qu'un équilibre doit être trouvé entre le numérique et l'humain.
Les déclarations récentes du secrétaire d'État au numérique, en réponse aux inquiétudes du Défenseur des droits dont le rapport souligne les risques de l'e-administration pour le citoyen, font état de la promesse de réintroduire de l'humain dans les démarches administratives.

Dans le cadre de l'entreprise, le numérique s'est développé afin d'accroître la performance et la productivité.
En effet, les outils numériques mis en place ont pour fonction principale de libérer du temps pour des activités génératrices de valeur ajoutée. La transformation numérique permet aux collaborateurs d'être plus performants grâce aux technologies.

L'humain au cœur des projets numériques

La mise en place d'une culture numérique au sein des entreprises est indispensable car le principal obstacle à la transformation numérique est la réticence des salariés au changement. En effet, les ressources humaines sont à la fois le frein et le moteur des évolutions en matière numérique.

Si la transformation numérique semble être une évidence, dans la mesure où elle permet d'améliorer les compétences des collaborateurs, il n'est pas question d'opposer l'homme et la machine mais plutôt de réussir à associer ces deux éléments pour obtenir une collaboration efficiente. C'est donc dans l'humain et ses capacités qu'il faut investir.
L'homme est la clé de la réussite de la transition numérique, d'autant plus que le développement des qualités humaines (gestion du stress, confiance en soi, créativité…) ne peut être mis en valeur que par celui des nouvelles

technologies. Le numérique facilite une nouvelle organisation du travail plus transparente, susceptible de placer l'innovation au service de l'humain en libérant les salariés de tâches dépourvues d'intérêt et répétitives. Ils peuvent dès lors se consacrer à des activités plus intellectuelles et accéder à davantage d'informations.

En outre, des outils, comme les réseaux sociaux d'entreprise, permettent de rendre plus fluide la circulation de l'information, ce qui améliore le quotidien d'un contexte professionnel. De surcroît, en décloisonnant les services par le biais de la digitalisation, les interactions entre les salariés sont plus fortes et permettent ainsi à l'entreprise de s'ouvrir davantage vers l'extérieur.

La recherche permet de construire les conditions d'une véritable coopération entre l'humain et le numérique. C'est le cas, notamment, lors de travaux sur l'interaction de personnes avec les systèmes numériques et la prise en compte de modèles du comportement humain dans les algorithmes qui pilotent ces systèmes. Le rapport Villani[3], consacré à l'intelligence artificielle, et le rapport au Sénat, dédié aux données de santé[4], préconisent l'introduction d'un principe de « garantie humaine » du numérique en santé, avec une supervision humaine de toute utilisation du numérique et un contact humain pour transmettre les informations. Il est souhaité qu'il soit précisé « qu'une faute ne peut être établie du seul fait que le praticien n'aurait pas suivi les recommandations d'un algorithme, quand bien même celles-ci se révéleraient exactes ». Il est également défendu une exigence de transparence des algorithmes et d'effectivité du consentement du patient.

Au niveau de la justice, la démarche est la même. La justice ne sera jamais rendue par des robots mais le numérique et l'intelligence artificielle peuvent être une véritable aide à la décision pour les magistrats[5]. Le numérique doit rester au service de l'humain, en exécutant les tâches qui lui ont été assignées avec un encadrement éthique.

(3) Rapport de Cédric Villani : donner un sens à l'intelligence artificielle (IA), http://www.enseignementsup-recherche.gouv.fr

(4) Rapport de MM. Gérard Longuet, sénateur et Cédric Villani, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques n° 401 (2018-2019) - 21 mars 2019, https://www.senat.fr

(5) Rapport réalisé par *Lêmy Godefroy, Frédéric Lebaron, et Jacques Levy-Vehel* « Comment le numérique transforme le droit et la justice : vers de nouveaux usages et un bouleversement de la prise de décision ? » mission de recherche droit et justice, juillet 2019.

(6) Rapport 2019, Ministère de l'intérieur www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019.

Le facteur humain, moteur de la cybercriminalité

Si la cybercriminalité[6] peut revêtir l'aspect d'attaques purement techniques, elle est

aussi le fait de défaillances humaines. Celles-ci sont liées à des techniques de manipulation, comme l'ingénierie sociale définie par un « ensemble de procédés de manipulation psychologique ou d'exploitation comportementale (…) dont le but est l'incitation inconsciente à amoindrir, contourner ou supprimer les mesures de sécurité d'un système informatique[7] ».

(7) M. Quéméner, « Criminalité économique et financière à l'ère numérique ». Paris : Economica, 2015, p.87.

L'ingénierie sociale utilise les technologies comme vecteurs mais exploite le facteur humain pour, par exemple, susciter des escroqueries aux faux ordres de virement, des fraudes en entreprise, un cyberespionnage, des vols de données ou des manipulations boursières et d'informations. L'ingénierie sociale permet, par une mise en confiance, d'obtenir de l'argent de la personne ciblée. Cette technique est au cœur du procédé utilisé pour les fraudes aux faux ordres de virement internationaux (FOVI), dites « au président » ou « au changement de coordonnées bancaires », dont sont victimes les entreprises.

L'ingénierie sociale est une « pratique » qui sert à exploiter « l'aspect humain et social de la structure à laquelle est lié le système informatique ». Elle permet à celui qui s'en sert, de gagner la confiance de sa cible pour en obtenir des informations sensibles mais aussi un bien, un service, l'accès à un système ou à un espace physique ou virtuel déterminé ou encore pour l'amener à adopter un comportement spécifique voire s'abstenir de faire quelque chose. Ladite cible ne se rend pas compte de l'intention de son interlocuteur ou de l'impact de cette requête.

L'ingénierie sociale tire profit de l'usager, maillon faible de la cybersécurité, pour faciliter des cyberattaques qui peuvent rentrer dans le champ infractionnel couvert par la cybercriminalité. Elle est en même temps liée à la sécurité par l'ensemble de ses facettes physique, logique, informatique et informationnelle.

L'ingénierie sociale constitue un ensemble de compétences et de techniques pour tirer profit des vulnérabilités humaines.

Il importe alors de prendre en compte leur maîtrise pour cerner le profil de ceux qui les emploient à des fins illicites. Il est donc essentiel de développer des formations et des stratégies en matière de cybersécurité afin d'anticiper ces risques numériques.

(8) Voir comptes-rendus chaire – l'Humain au défi du numérique, https://www.collegedesbernardins.fr

Conclusion et perspectives

Il est fondamental en conséquence d'impulser une véritable culture et un humanisme numérique[8] afin

d'en comprendre les avantages
et les inconvénients car, finalement,
c'est l'homme qui crée le numérique
et donc ce dernier doit être
à son service et non son ennemi.

L'AUTEURE

Myriam Quéméner, magistrat judiciaire, après un détachement au ministère de l'Intérieur, comme conseiller juridique en matière de cybercriminalité, occupe actuellement la fonction d'avocat général près la cour d'appel de Paris.

Elle est chargée du contentieux économique et financier et assure la veille juridique en matière de droit du numérique pour le parquet général de la Cour d'appel.

Docteur en droit, elle est membre de la chaire Cyber de Saint-Cyr.

Elle a publié récemment « le droit face à la disruption numérique » aux éditions Gualino Lextenso (2018) et pour Le Lamy : Droit pénal des affaires la délinquance numérique.

La crise cyber
dans les organisations en insistant sur la dimension humaine

Par Delphine Chevallier

La fréquence des crises cyber augmente. De quelques-unes par an, nous en sommes à plusieurs par semaine. Elles sont brutales quant à leurs impacts sur les activités, le niveau de vulnérabilité s'étant considérablement accru avec la montée en puissance de la digitalisation, mais aussi extrêmement violentes pour les individus qui doivent y faire face. Ce dernier aspect, l'humain, n'est encore qu'insuffisamment pris en considération car les expériences individuelles et collectives ne sont que trop peu partagées et nous n'avons pas encore assez forgé de repères pour pouvoir les affronter avec sérénité.

DELPHINE CHEVALLIER

Directrice ThaliaNeoMedia

Les interruptions informatiques provoquent chez les victimes un niveau de stress extrême

Lorsqu'un incident informatique majeur se produit, comme une cyber attaque, une interruption de réseau ou un dommage matériel, les individus se retrouvent comme jamais auparavant dans une situation qui les désoriente. Le stress qui en découle atteint de façon surprenante des niveaux extrêmes. Voici quelques paroles que j'ai entendues ces derniers mois de la bouche de celles et ceux qui en avaient fait l'amère expérience : « Cela m'a rendu hystérique de ne plus pouvoir accéder à mes données », « J'étais d'autant plus énervé que mes clients et partenaires continuaient eux à travailler normalement, à s'envoyer des e-mails et moi, j'étais complètement bloqué. Je me suis senti complètement exclu et surtout impuissant », « J'ai perdu deux ans de ma vie », « Cela m'a presque rendu fou lorsque j'ai réalisé que je ne pouvais plus travailler », « Je n'avais aucune idée de ce que je pouvais faire pour avancer dans mon travail ».

Les mots sont particulièrement forts. Comment en est-on arrivé là ?

Une hyper dépendance croissante aux outils digitaux qui nous a affaiblis

Les outils digitaux ont pris une telle place dans nos vies personnelles et nos interactions professionnelles que nous nous retrouvons dans une situation de vulnérabilité nouvelle.

Le monde digital a créé un niveau de dépendance : s'il n'est pas unique, nous sommes aussi devenus extrêmement dépendants des ressources énergétiques par exemple, il est sans précédent du fait de la rapidité avec laquelle nous avons transformé nos modes de fonctionnements, notre façon de travailler et d'effectuer certaines tâches qui désormais ne se réalisent que grâce aux outils digitaux, avec peu d'efforts, dans les organisations mais aussi dans nos vies personnelles.

Quel que soit le vocabulaire utilisé (outils digitaux, systèmes d'information, outils technologiques), il s'agit d'utiliser une machine pour effectuer une action, au lieu d'utiliser nos mains ou des outils présents dans le monde réel, voire notre cerveau ! L'utilisation de machines a envahi exponentiellement la communication entre êtres humains désormais « numérisée », le stockage de données désormais « virtualisé » et le traitement de données désormais « digitalisé ».

Ces pratiques ont pour conséquence un « désapprentissage » à marche forcée : combien de numéros de téléphone sommes-nous encore capables de retenir par cœur ? Sommes-nous encore capables de trouver notre chemin dans la rue ou sur la route sans Google Maps ou notre GPS ? Sommes-nous encore capables de lire pendant plus de 15 minutes sans nous arrêter un long texte au lieu de zapper de quelques lignes d'une information à une autre dans le flot sous lequel nous noient les réseaux sociaux ?

Lorsque tout s'arrête, que les machines nous jouent un bien sale tour en s'arrêtant de fonctionner, nous voici replongés « en arrière », dans un monde du « ici et maintenant », bien concret et réel, notre bureau, les collègues qui travaillent dans le bureau d'à côté, le papier et le crayon. Une réalité avec laquelle nous avons, consciemment ou non, mis une distance avec le développement de ce monde que nous disons « virtuel » et sans lequel nous nous sentons désormais perdus.

Quand il faut se résoudre à traverser le désert digital

Quelle expérience lorsqu'une interruption majeure du fameux réseau ou des fameux systèmes se produit, lorsqu'un logiciel dit malveillant s'introduit pour prendre en otage ou détruire nos données, lorsqu'un bug vient perturber un logiciel ! Comme nous nous retrouvons faibles et perdus lorsque la machine « ne répond plus » car cet événement nous renvoie à la difficulté à réactiver des « savoir-faire » qui nous paraissent déjà anciens, voire oubliés.

En effet, à l'heure de la soi-disant artificialisation de l'intelligence, on ne peut que constater une rapidité à désapprendre des façons de faire qui avaient, pour certaines, pris des

millénaires à être acquises : communiquer, écrire et parler, se souvenir, se concentrer, penser... On pourrait s'en moquer, se dire que les temps changent et que ce processus n'est qu'une énième étape dans l'évolution de notre humanité. Cependant, le pouvoir qu'a pris le monde digital sur nos capacités intellectuelles est peut-être bien plus perfide et lourd de conséquences que nous ne l'imaginons.

Plongés brutalement dans l'inimaginable d'une grande déconnexion, les individus n'échappent pas à un cheminement dans un processus de transition psychologique dont la durée s'étale sur plusieurs jours. Cette transition démarre par une période d'inaction, liée à une sidération et une incompréhension, qui s'accompagne d'un refus de la situation : « Non ce n'est pas possible, les systèmes vont repartir ». Pour une majorité d'individus, plusieurs jours seront nécessaires pour se remettre en action et une colère monte…

Lorsque la situation sera intimement acceptée, l'opportunité s'ouvre enfin d'une prise de conscience intime de la nécessité de développer des comportements désormais inédits pour se remettre à travailler, en mouvement et en action. C'est dans cette phase que le groupe, face à l'adversité, exprime sa solidarité : lorsque le réseau flanche, le lien humain a une capacité étonnante à se reconstituer. Le retour de la motivation, couplée avec la solidarité, forme un terreau favorisant le développement d'une l'ingéniosité permettant de réapprendre des gestes anciens ou de se débrouiller « avec les moyens du bord ».

À quelle vitesse sommes-nous capables de réapprendre ce que nous avons si facilement et rapidement désappris ? Quelle énergie devons-nous déployer pour transitionner à rebours vers les gestes anciens ? Ce processus de réinvention, n'est-il pas supérieur à celui d'apprentissage en amont ? Comment garder la main, le contrôle, en toutes circonstances sur ce qui nous permet d'interagir ? C'est bien parce que ce niveau d'énergie demandée est très fort que face à la machine qui ne fonctionne plus nombre d'individus peuvent devenir « hystériques ».

© Par Peshkova - Adobestock - 271569184

Le maintien d'une praxis en mode dégradé et la restauration de mécanismes mentaux hors processus digitalisés permettent d'élaborer de nouveaux processus dans un contexte solidaire et de minimiser l'impact de l'interruption de services digitalisés.

Ne serait-il pas moins onéreux de conserver ce comportement, ce geste qui a mis de longues années à s'ancrer en nous en continuant de le pratiquer régulièrement pour assurer la continuité de nos activités ? Comme le souligne Andy Bochman de l'INL Lab, dans le numéro d'avril-mai 2019 de la Harvard Business Review : « Le seul moyen de (..) se

protéger est de faire (..) ce qui peut sembler être un pas en arrière sur le plan technologique, mais qui est en réalité un pas en avant judicieux. L'objectif est de réduire voire d'éliminer la dépendance (..) aux technologies numériques et à leurs connexions Internet. Le prix (..) en vaudra la chandelle par rapport au coût potentiellement dévastateur que nous pourrions payer en continuant comme si de rien n'était. »

Vers l'ère d'une nouvelle indépendance numérique

Pour les organisations, s'assurer de la capacité des individus à traverser sans trop de dommages de telles crises, qui ne manqueront pas d'arriver, est une nécessité vitale. Si les équipes sombrent dans l'inertie en se laissant submerger par le chaos, c'est la pérennité même de l'entreprise qui se joue. Le point de départ est sans nul doute d'accepter sa vulnérabilité et de refuser la dépendance en identifiant, avec les équipes, les activités pour lesquelles un maintien des savoir-faire manuels ou en mode dégradé sera essentiel pour maintenir la continuité des affaires. Engager toutes les forces vives de l'organisation dans ce processus est indispensable pour que les équipes, à tous niveaux, conservent une capacité minimum à travailler, autant que faire se peut, en cas d'incidents.

Rassurée par cette tout nouvelle indépendance, une organisation s'en trouvera renforcée, grâce à ses ressources les plus précieuses, des femmes et des hommes aux capacités augmentées. Pour compléter ces réflexions, je vous invite à lire « Cyberattaque »[1], l'histoire vraie, vue au travers des yeux des opérationnels, de l'attaque NotPetya, de Juin 2017, qui décrit de façon précise et avec un brin d'humour ce processus par lequel passe une organisation plongée brutalement dans le chaos du blackout et dont les équipes vont développer des trésors d'ingéniosité pour maintenir leur entreprise à flot.

(1) « Cyberattaque - Plongez au coeur du blackout ! » Texte : Angeline Vagabulle, Dessins : Renard, Préface : Général Marc Watin-Augouard. Ed. Thalia NeoMedia/DG Les Funambulles, 2018.

L'AUTEURE

Delphine Chevallier démarre sa carrière en tant que consultante en organisation IT, puis auditrice financière pour les secteurs public, artistique et les PME. Elle occupe ensuite les fonctions de direction générale d'un orchestre de chambre et d'un festival de musique contemporaine. En 2000, elle intègre la direction des Ressources Humaines d'un grand cabinet de conseil pour participer à la définition de la stratégie RH, la structuration du département et la direction de nombreux programmes dans le contexte de mondialisation des activités. En 2011, elle crée puis dirige au niveau mondial l'université interne d'une firme de services professionnels. Fin 2018, elle fonde sa propre société, Thalia NeoMedia, dans l'édition et la formation, avec pour objet de créer avec les experts des univers engageants des partages de connaissances et d'expériences, à l'heure où les besoins d'apprentissages de tous s'accélèrent et se diversifient.

Elle est diplômée de l'ESCP Europe, en droit, en mathématiques appliquées aux sciences sociales et en stratégie digitale.

Le bruit au service de la confidentialité

Par Thierry Berthier

L'exploitation de bases de données massives contenant des informations à caractère personnel se heurte souvent au risque de désanonymisation et de réidentification des utilisateurs ayant fourni leurs données. Si les solutions intégrant des composantes d'apprentissage automatique participent bien à la création de valeur par la donnée, elles amplifient également le risque de réidentification à partir des données d'entraînement sur lesquelles le modèle statistique se construit. La confidentialité différentielle apporte alors un certain nombre de réponses au problème de réidentification dans un contexte d'apprentissage automatique.

THIERRY BERTHIER

Chaire de cyberdéfense & cybersécurité CREC Saint-Cyr Hub France IA

Les progrès réalisés en apprentissage automatique (Machine Learning : ML) permettent de concevoir des applications performantes pour l'aide à la décision, l'analyse prédictive, la classification de données ou la détection d'anomalies et fraudes.

La mise en œuvre de composantes ML s'appuie sur une phase initiale d'apprentissage construite à partir d'un ensemble de données appelé « dataset d'entraînement » et susceptible de contenir des informations à caractère personnel.

Une fois cette phase d'apprentissage réalisée, la composante ML est utilisée en phase d'exploitation pour effectuer des tâches de classification automatique ou de régression sur de nouveaux jeux de données de grands volumes. L'efficacité des composantes ML est alors directement liée à la qualité des données utilisées, lors de l'entraînement, et à leur adéquation avec celles qui interviendront en phase de production. La question de la protection

des données personnelles intervient tout au long du processus d'apprentissage automatique. Sans traitement particulier des données d'apprentissage, le risque de réidentification est important et augmente significativement avec le nombre de requêtes réalisées par la suite sur la base exploitée. Les techniques de confidentialité différentielle (*differential privacy*), quand elles sont applicables, apportent un certain nombre de réponses au problème de réidentification et plus largement au respect « différentiel » de la vie privée.

Le risque de réidentification des données d'entraînement d'un modèle

Dès 2001, une étude menée par Latanya Sweeney, Directrice du Harvard's Data Privacy Lab, montrait qu'il était possible de réidentifier un individu dans 87 % des cas à partir d'une base de données en ayant seulement accès qu'à trois types de données : le genre, la date de naissance et le code postal[1]. En 2019, la préservation de l'anonymisation des données et le respect de la réglementation (RGPD) obligent les éditeurs à repenser les processus de requêtes effectuées sur les bases de données en exploitation. Les concepteurs de solutions, embarquant des composantes ML, doivent ainsi orienter leurs développements en privilégiant la « privacy by design » sans sacrifier la performance de leurs produits. Il s'agit là d'un véritable défi algorithmique !

(1) L. Sweeney, *Simple Demographics Often Identify People Uniquely.* Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

Dans le secteur de la santé, les algorithmes d'apprentissage automatique s'appuient souvent sur des données issues des dossiers médicaux des patients. La question du maintien de la confidentialité et de la non réidentification de ces patients se pose donc de manière centrale. Plus précisément, si un modèle a été entraîné avec des données provenant de plusieurs sources avec plusieurs niveaux d'anonymat, à quel point ce modèle expose-t-il ses données d'entraînement ? Est-il possible de modifier le processus d'apprentissage pour forcer le modèle produit à respecter un certain niveau de confidentialité ?

De récentes expérimentations ont mis en lumière les vulnérabilités de nombreux modèles existants à différents niveaux. En particulier, des études empiriques ont montré l'existence d'un phénomène de mémorisation involontaire par le modèle entraîné, d'exemples intervenant durant la phase d'entraînement. Cet effet indésirable est d'autant plus marqué lorsque le modèle dispose d'une grande capacité d'apprentissage. C'est le cas notamment avec les réseaux de neurones. Ainsi, un réseau de neurones entraîné sur du texte anglais a mémorisé des mots aléatoires comme des mots de passe,

(2) Carlini, N., Liu, C., Kos, J., Erlingsson, _U., Song, D. : The secret sharer : Measuring unintended neural network memorization & extracting secrets. arXiv preprint - arXiv : 1802.08232 (2018)

insérés dans le jeu d'entraînement puis a permis leur restitution[2]. L'exploitation de ces vulnérabilités fonctionnelles spécifiques au processus d'apprentissage induit de nouvelles menaces, avec à la clé de nouvelles campagnes de fuites de données.

Deux types d'attaques de rétro-ingénierie, réalisées à partir d'un modèle entraîné, font désormais l'objet d'intenses recherches : l'attaque d'appartenance et l'attaque par reconstruction. L'attaque d'appartenance consiste à deviner efficacement si une donnée particulière a été utilisée ou non durant la phase d'entraînement d'un modèle. L'attaque par reconstruction consiste à reconstruire une donnée d'entraînement ou certains de ses attributs. De telles attaques peuvent être conduites soit en disposant des paramètres complets du modèle (on parle alors de *white box attack*), soit en disposant seulement d'un accès au modèle par des requêtes d'inférence (on pose des questions précises au modèle dont les réponses permettront la reconstruction de la donnée d'entraînement. On parle dans ce cas de *black box attack*). La mise en œuvre potentielle de ces deux types d'attaques porte atteinte à la confidentialité des données d'entraînement et ouvre la voie à des détournements incompatibles avec les exigences de protection de l'anonymat.

Lorsqu'une technologie devient incontournable, ses vulnérabilités intrinsèques sont immédiatement découvertes puis exploitées. Une technique de sécurisation et de correction de tout ou partie des failles de sécurité existe souvent déjà quelque part ou ne tarde pas à émerger de travaux en cours. C'est précisément le cas avec l'approche de confidentialité différentielle (differential privacy : DP) appliquée à l'apprentissage statistique.

La confidentialité différentielle pour préserver l'anonymisation des données

Les mesures conventionnelles de maintien de la confidentialité s'articulent selon trois approches du contrôle : l'accès à l'information, le flot d'information et l'utilisation de l'information. Parmi les approches classiques de la communication privée, on trouve ainsi l'anonymisation par suppression des identifiants (k-anonymisation) ou l'assainissement par communication d'un échantillon de données. Pour autant, ces techniques ne garantissent pas totalement le respect de la vie privée. Elles peuvent être mises en défaut par certaines attaques et ne sont pas applicables à tous les contextes d'architectures et de traitement des données. La parcimonie des données favorise la réidentification. Elle implique, avec une forte probabilité, que deux profils présents dans une base ne sont jamais similaires à plus de X pour cent. Autrement dit, si un profil peut être apparié à 50 % à un profil présent dans une base, alors l'attaquant connaît avec une forte probabilité la vraie identité

du profil. En 2008, des algorithmes probabilistes efficaces capables de casser l'anonymisation ont été développés et exploités avec succès[3]. Le contexte de requêtes réalisées lors d'un sondage illustre bien également les difficultés à maintenir l'anonymat des réponses des participants.

(3) A ; Narayanan, V. Shmatikov : Robust de-anonymization of large sparse datasets, Proc. 29th IEEE Symposium on Security and Privacy, 2008.

(4) Dwork, C., McSherry, F., Nissim, K., A. : Calibrating noise to sensitivity in private data analysis. In : Theory of cryptography conference. pp. 265{284. Springer (2006).

Introduit en 2006 par Cynthia Dwork, Mc Sherry, Nissim et Smith[4], le concept de confidentialité différentielle rassemble des méthodes qui protègent les données à caractère personnel contre le risque de réidentification tout en maintenant la pertinence des résultats de requêtes. À l'intersection de plusieurs disciplines mathématiques (data sciences, optimisation, probabilités, cryptographie), la confidentialité différentielle permet (en théorie) l'exploitation statistique de données individuelles agrégées sans compromettre la vie privée des individus concernés. L'idée directrice issue des travaux de Cynthia Dwork est la suivante : la confidentialité différentielle est obtenue en appliquant un procédé qui introduit de l'aléa dans les données tout en maintenant leur potentiel d'exploitation.

La définition suivante permet de mesurer théoriquement le niveau de confidentialité différentielle d'un algorithme et d'évaluer son respect « différentiel » de la vie privée.

Définition de la confidentialité différentielle (Dwork, Mc Sherry, Nissim et Smith)

Deux ensembles de données D et D' sont dits voisins s'ils ne diffèrent que par un seul élément.

Un algorithme probabiliste M. est dit ε - différentiellement privé si pour tous ensembles de données D, D' voisins et tout évènement S : Proba [M (D) ε S] $\leq$ exp (ε) . Proba [M (D') ε S

Concrètement, plus la valeur de ε est proche de zéro et plus la confidentialité de l'algorithme est forte. Dans ce cas, substituer une donnée par une autre donnée a très peu d'incidence sur la sortie produite par l'algorithme. Une valeur de $\varepsilon = 0$ signifie que chaque donnée n'a aucune influence sur le résultat produit par l'algorithme. Dans le cadre de l'apprentissage automatique, l'algorithme considéré est le processus d'entraînement et la sortie est le modèle produit. L'enjeu est de construire un modèle utile (performant une fois mis en production) reposant sur des informations issues du dataset d'entraînement sans révéler trop d'information sur chaque exemple particulier.

Donnons un exemple devenu classique d'algorithme satisfaisant la confidentialité

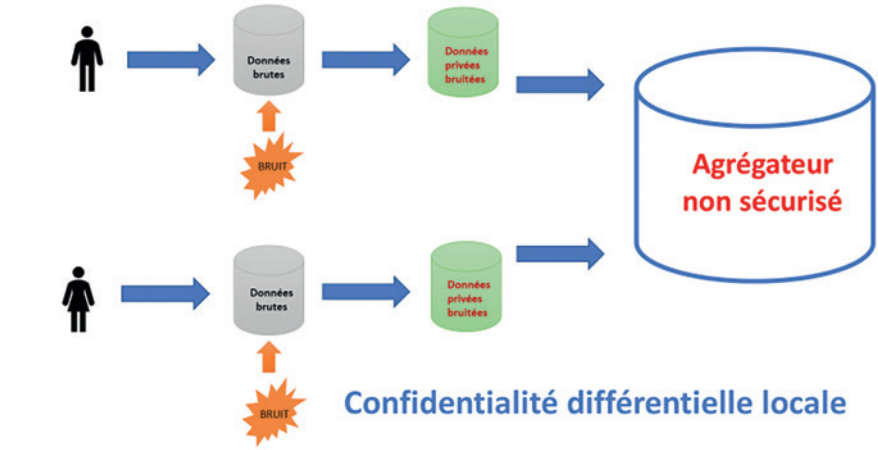
différentielle et pour lequel la valeur de ε est égale à log (3). Supposons que l'on cherche à estimer la proportion de consommateurs de drogues dans une population. L'approche classique consiste à poser directement la question à un échantillon représentatif de la population. L'inconvénient majeur de la méthode directe est que la réponse d'un individu sondé compromet sa vie privée. Une approche « Differential Privacy » s'appuie sur le processus suivant : pour chaque individu interrogé, on effectue un tirage à pile ou face. Si l'on obtient pile, l'individu répond sincèrement. Si l'on obtient face, on lance une seconde pièce pour répondre au hasard à la question du sondage : face donne la réponse « oui, je suis consommateur » et pile donne « non, je ne suis pas consommateur ». De cette façon, chaque individu peut réfuter sa réponse en prétendant qu'elle est due au hasard. Quant au sondeur, s'il dispose d'un échantillon assez large, il peut facilement retrouver une estimation fiable de la proportion de consommateurs de drogues à partir de la fréquence de réponses positives qu'il observe.

Cet exemple met en lumière plusieurs propriétés fondamentales du concept de Differential Privacy. La première propriété (positive) est la robustesse face au post-traitement : il n'est pas possible de compromettre la vie privée de l'individu sondé en analysant sa réponse.

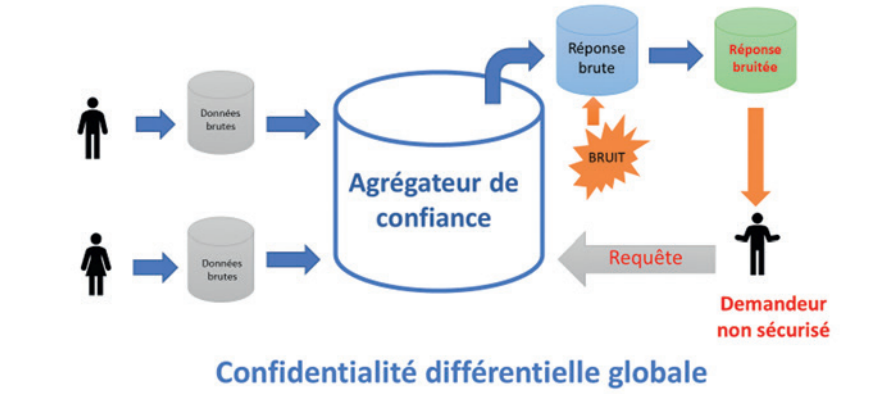
Une seconde propriété (négative) est celle de composition. Intuitivement, si l'on répète 100 fois le sondage décrit sur la même personne, on obtiendra une estimation fiable de sa vraie réponse. Une troisième propriété remarquable (positive) est celle du sous-échantillonnage : si un individu a une probabilité strictement inférieure à un d'être inclus dans l'étude, alors sa vie privée est davantage préservée.

Concevoir un algorithme satisfaisant la propriété de confidentialité différentielle n'est pas toujours possible. Lorsque celui-ci donne une réponse déterministe qui dépend des données, c'est en général impossible sans modifier le format des réponses. La solution consiste à introduire du bruit aléatoire dans la réponse retournée.

La confidentialité différentielle offre une garantie forte de maintien de l'anonymat en s'appliquant à un algorithme et non à un résultat. C'est là toute la force de ce procédé qui reste toutefois complexe à mettre en œuvre. L'ajout de bruit a en effet tendance à dégrader les performances du modèle. Il faut donc trouver un équilibre subtil dans la construction de l'algorithme sous-jacent. De plus, il n'est pas possible de certifier qu'un modèle vérifie la propriété de confidentialité différentielle sans avoir accès à l'algorithme qui l'a construit.



Modèle de flux de données sous confidentialité différentielle locale.



Modèle de flux de données sous confidentialité différentielle globale.

La première figure correspond à un modèle local de confidentialité différentielle dans lequel les données brutes produites par les utilisateurs sont bruitées avant d'être collectées au sein d'un agrégateur externe dont la confiance n'est pas prouvée. L'agrégateur reçoit des requêtes extérieures *a priori* non sécurisées puis fournit des réponses construites à partir des données bruitées.

La seconde figure correspond à un modèle global de confidentialité différentielle dans lequel l'agrégateur est réputé comme une composante de confiance. Ce dernier reçoit des requêtes provenant d'utilisateurs extérieurs potentiellement malveillants. Il produit des réponses brutes qui sont ensuite bruitées avant d'être envoyées au demandeur. Dans les deux modèles, un attaquant éventuel exploitant les réponses à des requêtes bien choisies est confronté à la présence de bruit dans les réponses lors de sa tentative de désanonymisation des données collectées.

Si la confidentialité différentielle fournit des garanties formelles contre la réidentification, elle reste complexe à implémenter en conservant les performances initiales du modèle. Les laboratoires de recherche des géants du numérique Apple et Facebook utilisent l'approche différentielle pour garantir à leurs utilisateurs que leurs données conservent un peu d'anonymat. Google vient de publier la première librairie C ++ open source d'algorithmes de confidentialité différentielle destinée aux utilisateurs de bases de données massives[5]. Enfin, la décentralisation du traitement des données offre une approche complémentaire de la confidentialité différentielle, potentiellement efficace contre le risque de réidentification.

(5) Librairie Differential Privacy Google : https://github.com/google/differential-privacy/

En conclusion…

Les enjeux de confidentialité différentielle vont devenir centraux dans le déploiement de solutions embarquant de l'apprentissage statistique entraîné sur de grands corpus de données. Le principal défi technologique sera celui de l'exploitation de la donnée d'apprentissage à caractère personnel sans sacrifier sa « privacy » et sans dégrader la qualité du modèle engendré. En définitive, l'utilisateur qui consent à fournir ses données personnelles doit toujours rester informé sur le modèle, sur ses performances et sur ses risques.

L'AUTEUR

Thierry Berthier est Maître de conférences en mathématiques. Il est chercheur associé au CREC Saint-Cyr et à la Chaire de cyber défense Saint-Cyr. Expert en cybersécurité & cyberdéfense, il est membre de l'Institut Fredrik Bull. Il copilote le groupe « Sécurité Intelligence Artificielle » du Hub France IA .

Il est par ailleurs cofondateur des sites VeilleCyber, SécuritéIA et fondateur du blog Cyberland.

Il est l'auteur de l'ouvrage « From digital traces to algorithmic projections » publié en 2018 aux éditions ISTE Wiley & Elsevier.

Liens :
http://cyberland.centerblog.net/
https://veillecyberland.wordpress.com/
https://iasecurite.wordpress.com/

Le chiffrement
pour protéger les données des humains

Par Gérard Peliks

De tout temps, l'humain a essayé de protéger ses informations utilisées, stockées et transmises, que ce soit le lieu de ses territoires de chasse et de cueillette il y a quelques dizaines de milliers d'années, ou, dans une époque plus moderne, ses données numériques sensibles. Parallèlement, il a essayé de prendre connaissance de l'information détenue par d'autres, même s'il n'y était pas autorisé. Ajoutons qu'à notre époque où le numérique entre dans la vie de tous les jours, garantir la confidentialité et l'intégrité de ses données sensibles est une assurance toujours indispensable et parfois vitale.

GÉRARD PELIKS

ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

La cryptologie à l'usage du grand public

Pour assurer la confidentialité et l'intégrité des données, le génie humain n'a eu de cesse que de faire évoluer la cryptologie, science des messages cachés, pour l'adapter aux technologies de pointe et souvent les précéder.

À l'ère du numérique, préserver la confidentialité des données sensibles est le but de la cryptographie ou « *chiffre de défense* ». On chiffre les données, avec un algorithme et une clé de chiffrement, pour les rendre incompréhensibles, et on ne les déchiffre que si on possède le même algorithme et la clé de déchiffrement. Mais si on est en possession d'un message chiffré et qu'on ne possède pas la clé de déchiffrement, la cryptanalyse intervient pour retrouver le message en clair. On parle alors de « *chiffre d'attaque* ».

Pour établir l'**intégrité** des données, on utilise aussi les technologies de la cryptographie pour constituer une signature numérique qui garantit l'identité du créateur des données et fournit la preuve que celles-ci n'ont pas été modifiées.

Dans cet article qui s'adresse à un utilisateur

non expert en cryptologie, il ne sera pas question de rentrer dans le raffinement mathématique des algorithmes comme par exemple l'AES[1] pour le chiffrement symétrique ou le RSA[2] pour le chiffrement asymétrique. Si vous êtes intéressés par la cryptologie et que vous possédez des connaissances solides en mathématiques, vous verrez qu'on se rend compte, en comprenant le fonctionnement des algorithmes, que le génie humain n'a pas de limites. **Cependant, il n'est absolument pas nécessaire d'être un cryptologue pour chiffrer et déchiffrer des données quand on possède l'application et les clés.**

Il ne sera non plus traité le sujet des échanges de clés secrètes, privées ou publiques comme c'est fait par exemple dans le PGP[3], ni de la gestion des certificats numériques, mais il est intéressant si vous souhaitez progresser dans la connaissance des mécanismes qui assurent la transmission des clés de chiffrement de bien appréhender les techniques d'échange et de gestion des clés. Il sera peu question enfin du mécanisme de la signature électronique qui utilise les empreintes de fichiers signés et le chiffrement asymétrique pour garantir l'intégrité et l'appartenance d'un message.

Dans cet article nous expliquerons simplement pourquoi et **comment chiffrer et signer** des données, afin de faire ressortir que si les mécanismes mis en jeux sont très complexes l'utilisation du chiffrement est très simple, la difficulté étant reportée au niveau de l'outil et non pas à celui de l'humain. De plus, les outils de cryptologie, libres ou commerciaux, qui s'affirment sur le marché sont très conviviaux.

Mais pourquoi chiffrer ?

Par exemple, supposons que vous déteniez sur votre tablette, des données sensibles comme la liste des mots de passe de tous les sites Web que vous fréquentez, même ceux où vous n'êtes pas censés être allés, ou vos données médicales ou une liste de clients et prospects avec des informations particulièrement sensibles. Supposons que vous oubliez votre tablette dans un taxi, et que malgré vos efforts pour la récupérer, vous ne la retrouviez plus… Le mieux que vous puissiez espérer serait que votre tablette

(1) *Advanced Encryption Standard* ou AES (litt. « norme de chiffrement avancé »), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. (NDLR : Origine Wikipédia).

(2) **Le chiffrement RSA** (nommé par les initiales de ses trois inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman) un algorithme de cryptographie asymétrique utilisé dans le commerce électronique. Breveté1 par le Massachusetts Institute of Technology (MIT) en 1983, il a expiré le 21 septembre 2000. (NDLR : Origine Wikipédia).

(3) Pretty Good Privacy (qu'on pourrait traduire en français bon niveau de confidentialité), plus connu sous le sigle PGP, est un logiciel de chiffrement cryptographique, développé et diffusé aux États-Unis par Philip Zimmermann en 1991. PGP garantit la confidentialité et l'authentification pour la communication des données. Il est souvent utilisé pour la signature de données, le chiffrement et le déchiffrement des textes, des courriels, fichiers, répertoires et partitions de disque entier pour accroître la sécurité des communications par courriel. (NDLR : Origine Wikipédia).

soit désintégrée par un coup de foudre ou une explosion de sa batterie… N'y comptez pas trop ! Tant pis pour la tablette, mais quid de vos données sensibles qui sont importantes et qui ne doivent pas être récupérées par un « attaquant ». Vous l'avez compris, si vos données sont en clair, celui qui a récupéré votre tablette en prendra connaissance. Si vos données sont chiffrées, vous pouvez dormir plus tranquille. Ce sera sans conséquences fâcheuses pour votre vie privée ou professionnelle.

On parle beaucoup du RGPD (règlement général pour la protection des données personnelles) et des sanctions de la CNIL qui commencent à frapper les organisations qui ne protègent pas leurs données à caractère personnel dans les règles de l'art. Si vos données sont exfiltrées frauduleusement, c'est fréquent, mieux vaut qu'elles aient été chiffrées pour ne pas avoir d'ennuis avec la CNIL et les personnes dont vous détenez des données personnelles.

Bob chiffre et déchiffre un fichier sur son disque

Nous introduisons deux personnages qu'on retrouve très souvent dans la littérature de la cryptologie, Bob et Alice. L'un chiffre, l'autre déchiffre.

Pour chiffrer/déchiffrer, il vous faut posséder une application **et une paire de clés asymétriques**. Une des deux clés (**votre clé publique**) est contenue dans un **certificat numérique** et l'autre (**votre clé privée**), dans l'idéal, est sur un token USB[4] ou une carte électronique, protégée par un code PIN ou encore par un dispositif de biométrie. Vous pouvez générer vous-même, grâce à une application de chiffrement, cette paire de clés mathématiquement liées, ou plus sûrement, vous pouvez l'acheter à un prestataire qui vous fournira une clé privée et un certificat numérique. Ce dernier contient la clé publique correspondante, signée par une autorité à laquelle vous, ainsi que tous ceux avec qui vous souhaitez échanger des données chiffrées, faites confiance. Quand on chiffre avec l'une des clés, on déchiffre avec l'autre.

(4) C'est une clé USB standard qui possède les mêmes fonctions d'authentification, de chiffrement et de signature qu'une carte à puce. Elle est évolutive grâce à l'hébergement de nombreux certificats SSO, qui permet de déployer des applications sans remettre en cause l'existant. La clé Token est compatible avec la plupart des applications. Elle possède aussi un niveau de sécurité élevée, avec la protection par code PIN et l'utilisation de paramètres propres à l'entreprise.

Précisons ici que ce n'est pas avec ces clés qu'on chiffre ou déchiffre les données. Ces clés ne servent qu'à transporter, de manière sûre, une clé de chiffrement symétrique, la **clé secrète**, produite par l'application de chiffrement, qui elle est utilisée pour chiffrer et déchiffrer.

Pour chiffrer ou déchiffrer, vous rentrez votre token USB ou votre carte dans votre PC, l'application de chiffrement vous demande votre code PIN ou votre mot de passe. Vous êtes prêts à chiffrer ou déchiffrer.

Rien de plus facile donc pour l'utilisateur !

*Pour chiffrer un fichier sur votre disque, vous sélectionnez ce fichier en cliquant sur le bouton gauche de la souris. Le fichier étant sélectionné, vous cliquez sur le bouton droit. L'application vous propose un menu, souvent un pop-up menu, qui vous demande ce que vous voulez faire. Sur le menu, vous cliquez sur l'option « **chiffrer** ». C'est tout. Votre fichier est chiffré et son extension est modifiée.*

Parfois, surtout quand le produit vient de l'étranger avec une interface mal traduite, on rencontre le mot « *crypter* », mais oubliez ce mot qui ne veut rien dire et qui ne devrait pas exister. Bien entendu, il se passe des choses très complexes durant le chiffrement, mais la difficulté est résolue au niveau de l'application. Pour vous, rien à faire de plus que de sélectionner le fichier et dire que vous voulez le chiffrer.

La principale réticence que l'on rencontre chez un utilisateur, les premières fois qu'il chiffre un fichier, est « *bon, j'ai chiffré mon fichier, mais suis-je bien sûr de pouvoir le déchiffrer quand j'aurai besoin de le récupérer en clair ?* » Sous-entendu : si je ne suis pas sûr de pouvoir le déchiffrer, mieux vaut ne pas prendre le risque de le chiffrer. *Rassurez-vous, déchiffrer un fichier sur votre disque est aussi simple que le chiffrer : vous sélectionnez le fichier chiffré (clic gauche), vous cliquez sur le bouton droit de votre souris, l'application vous propose un menu pour savoir ce que vous voulez faire.*

*Vous choisissez l'option « **déchiffrer** », et le déchiffrement se produit ! Votre fichier est maintenant revenu en clair avec son extension d'origine, parce que vous avez bien sûr les clés pour le déchiffrement.*

On trouve sur la toile beaucoup de logiciels libres, comme le GPG version libre du PGP, ou commerciaux. Pour une utilisation plus sûre, choisissez de préférence des logiciels de chiffrement certifiés Critères Communs ou CSPN (Certification de Sécurité de Premier Niveau) décernés par l'ANSSI. Un logiciel de cryptologie français est un premier pas vers la souveraineté des données sur notre territoire et on ne plaisante pas avec des données sensibles qui peuvent être convoitées par des puissances étrangères.

Bob chiffre, Alice déchiffre

Échanger un fichier chiffré, pour un déchiffrement par un autre utilisateur est à peine plus compliqué.

Bob chiffre un message sensible à l'intention d'Alice qui a besoin du certificat numérique de Bob pour le déchiffrer. Ce certificat numérique n'est pas un secret et il est destiné à tous ceux à qui Bob souhaite envoyer des messages ou des fichiers chiffrés. Si, par exemple dans le cas de la messagerie, Bob envoie à Alice un message chiffré ou un fichier chiffré attaché à son courriel, quand Alice veut en prendre connaissance, l'application lui demande le certificat numérique de Bob. Elle peut le demander à Bob directement ou le trouver elle-même dans un

annuaire que Bob lui a indiqué. Ou encore Bob peut attacher son certificat numérique, en clair, à son message. Un certificat numérique et son contenu n'ont rien de secret.

C'est tout et c'est facile : Alice clique sur le message chiffré ou sur le fichier chiffré attaché et le déchiffrement se produit.

À quoi sert au juste le certificat numérique de Bob, dont Alice a besoin ? Il contient les coordonnées de Bob (nom, prénom, organisation…) et ses dates de validité. Il contient aussi la clé publique de Bob, mathématiquement liée à sa clé privée. Le certificat est signé numériquement par une autorité de confiance. Toute modification du certificat sera décelée par l'application, grâce aux mécanismes de signature numérique. Il est conseillé qu'Alice lise le contenu du certificat de Bob, pour savoir en particulier qui est l'autorité qui l'a signé, et ne poursuivre la transaction que si elle a confiance en cette autorité mais ce n'est pas indispensable pour qu'elle déchiffre le message de Bob.

L'intégrité par la signature numérique

Sans entrer dans les détails, le chiffrement assure la confidentialité d'un fichier mais n'est pas suffisant pour assurer son intégrité, c'est-à-dire assurer que le fichier n'a pas été modifié et qu'il vient bien de celui qui l'a produit. **L'intégrité est assurée par la signature numérique**. Bob signe son fichier ; son application de signature électronique calcule une empreinte du fichier et chiffre cette empreinte par la clé privée asymétrique de Bob. Il envoie à Alice son fichier accompagné de son empreinte chiffrée.

(5) SHA-2 (Secure Hash Algorithm) est une famille de fonctions de hachage qui ont été conçues par la National Security Agency des États-Unis (NSA).

L'application de signature électronique d'Alice recalcule l'empreinte du fichier reçu, par la même fonction irréversible (souvent aujourd'hui le SHA2) [5], que Bob. L'application de signature électronique d'Alice déchiffre, à l'aide de la clé publique de Bob trouvée dans son certificat, l'empreinte qui a été chiffrée par la clé privée de Bob. L'autorité qui a signé le certificat de Bob est la garante de la validité de la signature numérique.

Si les deux empreintes, **empreinte recalculée** et **empreinte déchiffrée** correspondent, le fichier n'a pas été altéré et se trouve être vraiment le fichier envoyé par Bob. Petite précision linguistique : on parle ici d'*empreinte*. On dit « *hash* » en anglais et « *condensat* » en bon français.

Compliqué de signer un message ou un fichier ? Non, car les difficultés sont reportées au niveau de l'application. Pour l'utilisateur, signer est très simple. Ainsi, avec la messagerie **Thunderbird** à laquelle on ajoute l'extension **Enigmail**, on clique sur une icône représentant une clé pour chiffrer le message et/ou sur une icône représentant un stylo pour le signer. C'est très simple.

Transferts sécurisés à travers des Réseaux Privés Virtuels (VPN)

Si Bob depuis son Intranet à Paris veut transférer un fichier sensible à Alice qui se trouve sur son Intranet à Lille, Bob envoie le fichier en clair par l'Internet, depuis Paris, et Alice le reçoit en clair à Lille. Rien de plus simple encore, pour Bob et Alice, il n'y a rien de plus à faire que d'envoyer ou recevoir le message. Mais le fichier, s'il est sensible, ne doit pas passer en clair sur l'Internet. Un relais, un « *Gateway* », à la sortie de l'Intranet de Bob à Paris, se met en rapport avec un relais à l'entrée de l'Intranet d'Alice à Lille. Après authentification mutuelle, **le relais de Bob chiffre et celui d'Alice déchiffre**. Le mécanisme est totalement transparent pour Bob et Alice. On peut prendre l'image d'un tunnel sur l'Internet où tout ce qui passe est chiffré. Le transfert est donc **privé** car nul ne peut savoir ce qui passe dans le tunnel s'il ne possède la clé pour déchiffrer. Le tunnel est **virtuel** car dans la réalité il est fictif. L'information, découpée en datagrammes chiffrés, passe sur l'Internet par les mêmes mécanismes que si l'information passait en clair.

(6) Pour assurer la sécurité d'un réseau d'entreprise, il faut habituellement empiler un ensemble d'équipements et de logiciels tels que firewall, passerelles de VPN et d'antivirus, filtrage d'URL ou encore outils de prévention et de détection d'intrusions. Pour répondre à cette problématique il existe des équipements réunissant toutes ces fonctions en un seul boîtier (appliances de sécurité multifonctions ou solutions d'UTM (Universal Threat Management)).

Rien de plus simple, Bob et Alice n'ont qu'à envoyer le fichier et le recevoir en clair. Ce sont les relais à la séparation entre l'Internet et les Intranets, souvent sur les boîtiers *appliances*[6], qui ont aussi une fonction de « *firewalls* » qui chiffrent et déchiffrent.

En conclusion pour la cryptologie à l'usage du grand public

La cryptologie propose des outils indispensables, pour qui travaille sur des données sensibles. C'est une discipline passionnante pour les cryptologues et pour les cryptanalystes (ceux qui décryptent les données chiffrées sans avoir les clés pour les déchiffrer). Pour l'utilisateur, les outils sont très faciles à utiliser avec des interfaces conviviales, que ces outils soient des logiciels libres ou commerciaux.

Chiffrer les données apporte un gage de confiance en diminuant le risque que les données sensibles soient lues, ou modifiées, par des personnes non autorisées, dans notre cyberespace, lieu de tous les dangers pour l'humain qui évolue dans un monde qui devient de plus en plus numérique, donc de plus en plus menacé.

L'AUTEUR

Gérard Peliks travaille depuis plus de vingt ans dans le domaine de la sécurité de l'information. Ingénieur diplômé, son dernier employeur a été Airbus Defence & Space Cybersecurity. Il est lieutenant-colonel de la Réserve Citoyenne de Cyberdéfense (DGGN) et membre du Conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI). Il préside l'atelier sécurité de l'association Forum Atena, et il est chargé de cours sur différentes facettes de la sécurité à l'Institut Mines-Télécom et au pôle Léonard de Vinci.

Il est président de l'association CyberEdu, initiative de l'ANSSI pour que la sécurité du numérique soit évoquée dans les cours d'Informatique de l'enseignement supérieur.

Comment faire
durablement évoluer les comportements pour améliorer la cybersécurité ?

Par Olivier Pommeret

L'Homme, souvent présenté comme un maillon faible en matière de sécurité, en est en fait un fort sur lequel il faut agir à condition d'adopter les bons comportements. Le domaine de la cybersécurité ne fait pas exception, bien au contraire, mais comment faut-il agir pour faire adopter les bonnes attitudes et les conserver dans la durée : problème de management, besoin de « carottes » ou de « bâtons », de conseils ou de pédagogie ? « La vérité est (peut-être) ailleurs » …

OLIVIER POMMERET

Chercheur associé au Laboratoire de droit international et européen LADIE EA 7414) Université côte d'Azur

La cybersécurité est une affaire d'humains et concerne tout le monde !

La présence du numérique dans nos activités professionnelles et personnelles est telle que la cybersécurité est devenue un sujet de préoccupation pour tous. Que les problèmes soient causés, directement ou indirectement, par l'outil informatique (failles de sécurité, « bugs », pannes, ...) ou de mauvais usages volontaires (attaques, arnaques, atteintes à la réputation, ...) voire involontaires (méconnaissance, fausse manipulation, ...), ils impactent en effet au quotidien non seulement les citoyens mais également les entreprises, les collectivités territoriales ainsi que les institutions de l'État de manière générale (Ministère de la Défense, 2017 ; Ministère de l'Intérieur, 2018).

S'il fallait estimer la part de responsabilité directe dans les dommages observés entre les outils logiciels et les matériels informatiques défaillants, bien qu'ils soient pensés et conçus par l'homme, et la mauvaise utilisation de ces derniers, celle-ci irait jusqu'à 80 % en « faveur » du facteur humain (Crossler et al., 2013). Des études récentes sur le sujet, confirment les résultats mesu-

rés depuis plusieurs années (Kaspersky Lab, 2017 ; KPMG, 2018 ; Prince, 2015 ; Proofpoint, 2018).

Les limites de la pédagogie en matière de cybersécurité

Les actes malveillants volontaires, finalement minoritaires même si les médias leur donnent plus de visibilité, sont à distinguer des actes involontaires liés à des problèmes de comportement des usagers et à l'origine de la plupart des dommages subis (Proofpoint, 2018).

C'est sur ce sujet du comportement que sont réalisés les formations et les messages pédagogiques préventifs destinés à diminuer le risque « cyber ». À condition d'être répétées régulièrement, ces mesures sont efficaces et généralement mises en application. Cependant, elles sont souvent déployées uniquement à court terme du fait d'une pédagogie (au sens large) qui n'est pas toujours adaptée, ni efficace (Bada et al., 2015 ; Bones, 2017) et parce qu'elles visent de mauvaises habitudes fortement enracinées et des biais cognitifs. Si ces derniers nous aident dans certaines situations (rapidité de réaction, tri dans ce qu'il est important de mémoriser, recherche de sens, …), c'est d'ailleurs pour cela qu'ils ont été conservés lors de l'évolution de notre espèce, ils nous poussent aussi à prendre des décisions pouvant paraître irrationnelles ou inappropriées à un contexte. Ceci les rend comparables, pour rester dans le domaine informatique, à des « bugs » du cerveau, des failles de fonctionnement.

Certains de ces biais, apparaissant lors de raisonnements en « système 1 », lors de pensées « réflexes » prenant des raccourcis (Kahneman, 2011 ; Kahneman and Tversky, 1974), peuvent être corrigés via une posture plus réfléchie, dite en « système 2 ». Ce mécanisme demande plus de temps et d'attention. Il consomme beaucoup d'énergie et il est donc non spontané. D'autres biais peuvent être contournés ou mieux utilisés pour faire agir dans l'intérêt de l'individu et de son environnement (entreprise, famille, etc.), à condition bien évidemment que cela se réalise dans le cadre d'une éthique sans faille, respectant une liberté de choix, sans manipulation et en toute transparence ; des critères encadrant ce qui a pris le nom il y a une dizaine d'années de « *nudge* » (Bruns et al., 2018 ; Hansen and Jespersen, 2013 ; Thaler et al., 2009).

Connaitre et utiliser les biais cognitifs pour améliorer la cybersécurité via les « nudges »

Dans le domaine de la sécurité, les recherches en « économie comportementale » ont déjà mis en avant des biais cognitifs pouvant être à l'origine d'erreurs aux conséquences parfois très graves (accidents d'avions, mauvais choix étant la cause d'incidents dans le domaine

du nucléaire, de l'aérospatiale, *etc.* - Dejours, 2018 ; Morel, 2014 ; Reason, 2013). Les solutions apportées pour les contrer font souvent figure de pansements plus ou moins efficaces (« check-lists », normalisation des procédures, …) car elles ne peuvent couvrir l'ensemble des situations, notamment en cas d'imprévus (Taleb, 2007) nécessitant une rapidité de décision.

Cependant, si l'on prend en exemple la sécurité routière, la création de nudge a bel et bien permis de diminuer de manière significative et durable des accidents. Un des cas les plus connus, cité dans de nombreux ouvrages, dont celui du Prix Nobel d'Economie 2017 (Thaler et al., 2009), concerne la réduction des accidents au niveau d'une série de virages dangereux de « Lake Shore Drive » à Chicago. La solution la plus efficace identifiée (- 40 % d'accidents) a consisté à peindre sur le sol une série de bandes parallèles de plus en plus proches, donnant l'impression au conducteur que sa voiture accélère et l'incitant par réflexe « à lever le pied ». D'autres expérimentations, certaines réalisées en 2017 en France (La Voix du Nord, 2017) et mises notamment en application dans le XIV[e] arrondissement de Paris dès 2018, ont consisté à peindre des passages piétons en 3D « trompe l'œil » comme si ces derniers étaient en suspension.

© Site demain la ville – Blog / Bouygues immobilier

Le conducteur perçoit très bien qu'il s'agit d'une peinture et non de blocs de béton qui sortiraient du sol mais il est fortement incité à ralentir au niveau du prétendu obstacle. Dans d'autres domaines, c'est le biais de comparaison sociale qui a pu montrer son efficacité : pour augmenter le nombre de donneurs d'organes au Royaume-Uni, via un message sur la page d'accueil du site web dédié : « *Chaque jour, des milliers de gens qui voient cette page décident de s'enregistrer* », ou encore pour diminuer la consommation d'électricité chez un producteur aux États-Unis en faisant apparaître sur la facture des utilisateurs un smiley coloré, facilement compréhensible, indiquant sa position par rapport à ses « voisins ». Des *nudges* basés sur les mêmes mécanismes ont été utilisés dans le métro pour inciter les personnes à prendre les escaliers au lieu des escalators. Des visuels indiquent sur le premier une personne svelte, sur le deuxième une personne avec de l'embonpoint. Seul, l'individu sera peut-être

toujours tenté par l'escalator mais sous le regard des autres, il préférera emprunter les escaliers…

Tout cela pourrait-il fonctionner pour la cybersécurité ? Si, pour le moment, très peu de publications mettent en évidence l'efficacité des *nudges* dans ce domaine (Briggs et al., 2017 ; Choe et al., 2013 ; Coventry et al., 2014b ; Pfleeger and Caputo, 2012 ; Renaud and Zimmermann, 2018 ; Tsai et al., 2010), ce n'est pas par manque de résultats positifs mais surtout par l'absence de recherches actives sur le sujet (Briggs et al., 2017 ; Coventry et al., 2014b).

La « *Behavioural Insight Team* » (BIT), dite « *Nudge Unit* », département créé par le Premier ministre britannique afin d'étudier l'usage des *nudges* dans le domaine des politiques publiques, a publié un premier rapport en 2014 (Coventry et al., 2014a) listant, en effet, le fort potentiel des *nudges* dans l'amélioration de la cybersécurité. Un autre rapport plus récent de la BIT insiste sur l'importance de l'étude des comportements, en particulier l'attention, vis-à-vis du web afin notamment de promouvoir les bonnes attitudes (Halpern and Costa, 2019). En France, la « Revue stratégique de cyberdéfense » du 12 février 2018, produite par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), indique dans ses recommandations qu'il serait nécessaire d'étudier « *l'apport des nudges pour le développement de l'autonomie des citoyens en matière de cybersécurité* » avec pour finalité de diffuser la culture de la sécurité numérique dans toute la société (SGDSN, 2018).

Malgré l'identification de cette forte potentialité des *nudges* en matière de cybersécurité, nous tardons pourtant, en France, à lancer des programmes de recherche dédiés, probablement en partie du fait de la difficulté de travailler de manière transdisciplinaire entre sciences sociales et sciences « de l'ingénieur »… un autre biais, culturel cette fois-ci ! Notons tout de même quelques initiatives visant à identifier de tels *nudges* comme le projet « *Cyber-Nudge* » que j'ai eu le plaisir d'initier récemment au Laboratoire de Droit International et Européen de l'Institut du Droit de la Paix à l'Université de Nice Côte d'Azur.

Si l'humain est au cœur de la cybersécurité, travaillons sur l'humain !

Une nouvelle tendance en matière de gestion de la cybersécurité, certes non applicable à tous les domaines, consiste à éliminer le problème « à la racine » en réduisant voire en supprimant totalement la présence de l'outil informatique dans les processus industriels notamment (gestion et production d'énergie, *etc.*) au profit donc de l'humain et d'outils plus analogiques (Bochman, 2018). Cette approche recentrée sur l'humain rend l'identification et l'utilisation de *nudges* d'autant plus pertinentes, mais pas seu-

lement. En replaçant l'humain au centre de la démarche de cybersécurité, ce sont tous les enseignements liés à l'optimisation de nos comportements et à l'amélioration de la qualité de nos décisions qui doivent être mobilisés : Intelligence Émotionnelle, Intelligence Interpersonnelle, Psychologie sociale et cognitive, etc. L'objectif étant d'apprendre à mieux nous connaître et connaître les autres, à améliorer notre attention et notre concentration par la pratique de la méditation en pleine conscience, par exemple, à comprendre ce qui nous motive, à valoriser et mieux utiliser nos « soft-skills » (confiance, empathie, créativité, gestion du stress, *etc.*)… en bref, à mieux maîtriser toutes les formes de l'information quant à son identification, sa sécurité et son utilisation, ce que j'ai regroupé sous le terme d' « Intelligence Personnelle » par analogie avec l'Intelligence Économique et la bonne gestion des informations dans les entreprises.

Le champ paraît vaste, mais il a un double avantage. Il suscite, actuellement et très sûrement pour les années qui arrivent, un fort intérêt des scientifiques en tant qu'expression d'un nécessaire équilibre face aux progrès et à l'engouement pour l'Intelligence Artificielle. Il bénéficie déjà de très nombreuses et solides publications dans les domaines de la psychologie, des sciences sociales ou des neurosciences notamment. En effet, s'il y a une machine surpuissante qui évolue pourtant très lentement au regard des avancées technologiques, c'est bien le cerveau humain. Osons l'interdisciplinarité et focalisons-nous sur toutes ces études en lien avec les comportements et les biais cognitifs pour améliorer efficacement notre cybersécurité.

L'AUTEUR

Docteur en Biologie & Pharmacologie et titulaire d'un Mastère Spécialisé en Intelligence Économique et Management des Connaissances, Olivier Pommeret est expert dans les domaines de la veille et de la recherche d'information sur sources ouvertes (OSINT). Consultant dans ces domaines depuis 2006, il enseigne également dans différentes écoles (EOGN, École de Guerre, SKEMA,...), Universités et Établissements publics sous tutelle du Premier ministre (INHESJ, IHEDN). Passionné par l'étude des comportements humains, il effectue des recherches au sein du LADIE (EA 7414 - Université Côte d'Azur) sur l'utilisation positive des biais cognitifs (nudge) pour améliorer la cybersécurité.

En parallèle de ses activités professionnelles, Olivier Pommeret est réserviste citoyen au grade de Chef d'Escadron pour la région de Gendarmerie PACA.

Bibliographie sélective

- Alemanno, A., Sibony, A.-L., 2015. Nudge and the Law. Hart Publishing.
- Bada, M., Sasse, A., Nurse, J., 2015. Cybersecurity Awareness Campaigns. Why Do They Fail to Change Behaviour? https://www.sbs.ox.ac.uk/cybersecuritycapacity/content/cybersecurity-awareness-campaigns-why-do-they-fail-change-behaviour

- Bochman, A., 2018. Internet Insecurity : No amount of spending on defenses will shield you completely from hackers. It's time for another approach. Harv. Bus. Rev.
- Bones, J., 2017. Cognitive Hack: The New Battleground in Cybersecurity ... the Human Mind (Internal Audit and IT Audit). CRC Press.
- Briggs, P., Jeske, D., Coventry, L., 2017. Behavior Change Interventions for Cybersecurity, in: Little, L., Sillence, E., Joinson, A. (Eds.), Behavior Change Research and Theory. Academic Press, San Diego, pp. 115–136. https://doi.org/10.1016/B978-0-12-802690-8.00004-9
- Bruns, H., Kantorowicz-Reznichenko, E., Klement, K., Luistro Jonsson, M., Rahali, B., 2018. Can nudges be transparent and yet effective? J. Econ. Psychol. 65, 41–59. https://doi.org/10.1016/j.joep.2018.02.002

- Choe, E.K., Jung, J., Lee, B., Fisher, K., 2013. Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing, in: Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., Winckler, M. (Eds.), Human-Computer Interaction – INTERACT 2013, Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 74–91.
- Coventry, L., Briggs, P., Blythe, J., Tran, M., 2014a. Using behavioural insights to improve the public's use of cyber security best practices. Behavioural Insight Team.
- Coventry, L., Briggs, P., Jeske, D., van Moorsel, A., 2014b. A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment, in: Marcus, A. (Ed.), Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience, Lecture Notes in Computer Science. Springer International Publishing, pp. 229–239.
- Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010
- Dejours, C., 2018. Le facteur humain, 7e édition. ed. Presses Universitaires de France - PUF.
- Halpern, D., Costa, E., 2019. The behavioural science of online harm and manipulation, and what to do about it https://www.bi.team/publications/the-behavioural-science-of-online-harmand-manipulation-and-what-to-do-about-it/

- Hansen, P., Jespersen, A., 2013. Nudge and the Manipulation of Choice. A Framework for the Responsible Use of Nudge Approach to Behaviour Change in Public Policy (SSRN Scholarly Paper No. ID 2555337). Social Science Research Network, Rochester, NY.
- Kahneman, D., 2011. Thinking, Fast and Slow.
- Kahneman, D., Tversky, A., 1974. Judgment under Uncertainty: Heuristics and Biases. Science 185, 1124–1131.
- Kaspersky Lab, 2017. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky Lab official blog https://www.kaspersky.com/blog/the-human-factor-in-it-security/
- KPMG, 2018. Cybersecurity and the CFO | KPMG | BE KPMG. URL https://home.kpmg.com/be/en/home/insights/2017/08/cybersecurity-and-the-cfo.html.

- La Voix du Nord, 2017. Sécurité routière - Le premier passage piétons en 3D est à Cysoing Voix Nord. URL http://www.lavoixdunord.fr/253682/article/2017-10-27/le-premier-passagepietons-en-3d-est-cysoing.

- Ministère de la Défense, 2017. Cybersécurité : au cœur des menaces informatiques, le facteur humain https://www.defense.gouv.fr/terre/actu-terre/cybersecurite-au-coeur-des-menacesinformatiques-le-facteur-humain.

- Ministère de l'Intérieur, 2018. État de la menace liée au numérique en 2018. http://www.interieur.gouv.fr/Le-ministre/Communiques/Etat-de-la-menace-liee-aunumerique-en-2018.

- Morel, C., 2014. Les décisions absurdes: Sociologie des erreurs radicales et persistantes.

- Pfleeger, S.L., Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. 31, 597–611. https://doi.org/10.1016/j.cose.2011.12.010
- Prince, B., 2015. Employees Not Following Policy is the Biggest Threat to Endpoint Security, IT Pros Say | SecurityWeek.Com https://www.securityweek.com/employees-not-followingpolicy-biggest-threat-endpoint-security-it-pros-say.

- Proofpoint, 2018. The Human Factor 2018 Report https://www.proofpoint.com/us/human-factor2018.
- Reason, J., 2013. L'erreur humaine: 2e édition., 1st ed. Transvalor - Presses des mines, Paris. Renaud, K., Zimmermann, V., 2018. Guidelines for ethical nudging in password authentication. SAIEE Afr. Res. J. 109, 102–118.
- SGDSN, 2018. Revue stratégique de cyberdéfense | Secrétariat général de la défense et de la sécurité nationale http://www.sgdsn.gouv.fr/evenement/revue-strategique-decyberdefense/

- Sunstein, C.R., 2016. The Ethics of Influence: Government in the Age of Behavioral Science. Cambridge University Press, New York, NY.

- Taleb, N.N., 2007. Le Cygne noir : La puissance de l'imprévisible.

- Thaler, R., Sunstein, C., Midal, F., Pavillet, M.-F., 2009. Nudge : La méthode douce pour inspirer la bonne décision. Pocket, Paris.

- Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A., 2010. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Inf. Syst. Res. 22, 254–268. https://doi.org/10.1287/isre.1090.0260 Wikipedia, 2018a. Apprentissage profond. Wikipédia. Wikipedia, 2018b. AlphaGo. Wikipédia.

© Businessman holding tablet and showing holographic - par Lunatictm

UNE MESURE STATISTIQUE DE LA CYBERCRIMINALITÉ FRAGMENTÉE

Le Service statistique ministériel de la sécurité intérieure (SSMSI) a été créé en 2014 pour que les décideurs puissent bénéficier d'une approche en conformité avec les normes de la statistique publique. Celles-ci s'appuient sur le code des bonnes pratiques de la statistique européenne et le règlement 223/2009 révisé du Parlement européen et du Conseil du 11 mars 2009 relatif à la statistique européenne. En effet, les statistiques liées à la cybercriminalité répertorient les infractions pénales tentées ou commises à l'encontre ou principalement au moyen d'un système d'information et de communication (SIC). Elles doivent pouvoir être distinguées parmi des codes de natures d'infractions existants (NATINF) ou enrichis pour accompagner l'évolution de cette délinquance spécifique. Pour mieux appréhender son périmètre, on pourrait s'appuyer sur des sources administratives mais également sur des structures qui fournissent des études sur la cybercriminalité : les sociétés offrant des services de sécurité informatique, éditeurs de logiciels antivirus, sociétés d'assurance ou les cabinets de conseil, tout en tenant compte du contexte de recueil et d'analyse de ces données externes. On peut estimer raisonnablement que la mise en œuvre de méthodes innovantes d'analyse permettront à moyen terme d'améliorer la connaissance statistique de la cybercriminalité.

Les défis de la mesure
statistique de la cybercriminalité

Par Tiaray Razafindranovona et André Moreau

La mesure de la cybercriminalité n'échappe pas aux difficultés classiques de celle de la délinquance. Pour demeurer pertinents, les outils de la statistique administrative doivent non seulement s'adapter à l'émergence de nouveaux phénomènes délinquants, comme c'est le cas avec la cybercriminalité, mais aussi se conformer aux récentes normes internationales qui permettent une production de statistiques comparables avec les pays étrangers, à l'appui notamment des actions de coopération internationale policière. Inexistante au début des années soixante-dix, la cybercriminalité constitue une adaptation de la délinquance aux récentes évolutions technologiques. La statistique de la cyberdélinquance est aujourd'hui essentiellement produite à partir des données administratives de la Police et de la Gendarmerie nationales et quelques enquêtes de victimation permettent de compléter la vision du phénomène. La mobilisation d'autres sources administratives, comme les informations saisies sur des plateformes de signalement en ligne, ainsi que la mise en œuvre de méthodes innovantes d'analyse permettront d'améliorer la connaissance statistique de la cybercriminalité.

TIARAY RAZAFINDRANOVONA

Administrateur de l'Insee. Responsable des méthodes statistiques Service statistique ministériel de la sécurité intérieure SSMSI / BPDS

ANDRÉ MOREAU

Lieutenant-colonel de gendarmerie. Adjoint au chef du Bureau de la méthodologie et des études statistiques Service statistique ministériel de la sécurité intérieure. Chargé d'études.

Mesurer la délinquance[1]

(1) Estival A., Filatriau O., La mesure statistique de la délinquance, AJ Pénal 2019.224.

Le Service central d'étude de la délinquance (SCED) de la Direction centrale de la police judiciaire (DCPJ) a mis en place en 1972 un outil de suivi statistique des seuls crimes et délits constatés par les forces de sécurité : l'état 4001, du nom du formulaire papier utilisé lors de sa création.
Les infractions y étaient classées en 107 catégories nommées index, très hétérogènes par la nature et la gravité des faits. Pour pouvoir appliquer une métrique unique, à savoir le « fait constaté », à l'ensemble des index, il est fait usage d'unités de compte spécifiques par index correspondant à la façon la plus pertinente de mesurer chaque type d'infraction (victimes, infractions, auteurs, procédure, objets). Depuis 2015 pour la Police nationale et 2016 pour la Gendarmerie nationale, les systèmes d'information centralisent toutes les infractions enregistrées par les forces de sécurité avec nettement plus de détails que ce qui figurait dans l'état 4001.

Toutefois, les remontées via les logiciels de rédaction des procédures ne sont pas suffisantes pour appréhender la délinquance dans son ensemble. En effet, il est admis que l'enregistrement d'un événement dépend de la propension de la victime à porter plainte, de la priorité des forces de sécurité à la découverte de tel ou tel type d'infraction et enfin de la disposition et de la capacité des services à consigner cet événement. Pour y remédier, des enquêtes de victimation ont été mises en place : en France, l'enquête « Cadre de vie et sécurité » (CVS) est réalisée annuellement, depuis 2007, par l'Insee auprès d'environ 23 000 ménages en partenariat avec l'Observatoire national de la délinquance et des réponses pénales (ONDRP) et le service statistique ministériel de la sécurité intérieure (SSMSI créé en 2014).
Cette enquête vise à connaître les actes de délinquance dont les ménages et leurs membres ont pu être victimes.

Une décennie de polémique sur les statistiques administratives…

L'hétérogénéité des modes de mesure rend donc inappropriée l'addition des chiffres mesurés dans les différentes catégories. Pourtant un chiffre unique de la délinquance a longtemps été utilisé par les services de police et de gendarmerie pour piloter l'action publique et les politiques l'ont également mis en avant à des fins de communication[2], en particulier à partir de 2002.

(2) Mucchielli L., Robert P., Crime et sécurité. L'état des savoirs, Paris, La Découverte, 2002.

Au même moment, la mise en œuvre du management par objectifs de la délinquance, connu sous la dénomination de « politique du chiffre », a également contribué à brouiller, voire décrédibiliser les statistiques de la délinquance enregistrées par les forces de sécurité. En septembre 2012, un groupe de travail interne au ministère de l'Intérieur a été mandaté pour « rompre avec une présentation des statistiques reposant sur des indicateurs trop globaux, imprécis et hétérogènes »

et « redonner aux statistiques leur véritable vocation : être un outil au service de l'efficacité de l'action des policiers et des gendarmes ». En 2014, il a été créé le Service statistique ministériel de la sécurité intérieure (SSMSI) qui produit les statistiques sur la délinquance en toute indépendance et en s'assurant de leur fiabilité.

LE SERVICE STATISTIQUE MINISTÉRIEL DE LA SÉCURITÉ INTÉRIEURE SSMSI

Afin de produire des statistiques en conformité avec les normes de la statistique publique qui s'appuient sur le code des bonnes pratiques de la statistique européenne et le règlement 223/2009 révisé du Parlement européen et du Conseil du 11 mars 2009 relatif à la statistique européenne, la France a créé en 2014 un service statistique ministériel au sein du ministère de l'Intérieur (SSMSI). Conformément au décret n° 2014-1161 du 8 octobre 2014, il est placé sous l'autorité fonctionnelle conjointe des directeurs généraux de la police nationale (DGPN) et de la gendarmerie nationale (DGGN). Il est officiellement reconnu comme membre du service statistique public national, au sens de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, par un arrêté du 9 décembre 2014, au côté de l'Insee et des 15 autres services statistiques ministériels. La cheffe actuelle du service est la seule responsable, technique et éditoriale des informations et des données publiées par le service[3], dans le respect des règles techniques et déontologiques de fiabilité et de neutralité de la statistique publique.

(3) Le principal vecteur de diffusion de ces informations est le site internet https://www.interieur.gouv.fr/Interstats

Mesurer la cybercriminalité est encore plus complexe

Les limites évoquées sur la délinquance globale enregistrée sont encore plus marquées

Mesurer la cybercriminalité à partir des seuls évènements enregistrés dans les données du ministère de l'Intérieur conduit à une sous-estimation du phénomène.

En effet, certaines victimes d'infractions « cyber » peuvent considérer que le préjudice subi ne justifie pas la démarche de déposer une plainte (banalisation des faits, anonymat des auteurs) ou, du moins, que cette démarche n'est pas indispensable : par exemple, le remboursement par la banque d'un débit frauduleux sur compte bancaire peut s'effectuer sans dépôt préalable de plainte. De plus, les victimes, en particulier les personnes morales (entreprises, administrations, …), peuvent choisir de ne pas déposer de plainte pour des questions d'image ou de réputation[4].

(4) Protéger les internautes – Rapport sur la cybercriminalité (Groupe de travail interministériel sur la cybercriminalité).

Plus en amont encore du dépôt de plainte, une spécificité de la cybercriminalité est la transparence de certaines infractions : les victimes ne sont pas forcément conscientes qu'elles subissent une atteinte. Par exemple, il est difficile pour une per-

sonne non avertie de repérer une utilisation clandestine, par un tiers, de son ordinateur transformé en « machine zombie » pour par exemple miner de la cryptomonnaie (*cryptojacking*) ou encore lancer des attaques par déni de service.

Une absence de définition juridique unique

La mesure de la cybercriminalité se heurte à l'absence de définition juridique unique : ses contours peuvent alors apparaître comme flous. La cybercriminalité ne renvoie pas ainsi à une liste de natures d'infractions (Natinf[5]) bien déterminées ni à un index spécifique puisqu'elle couvre une bonne partie de l'ensemble du champ infractionnel.

(5) Il s'agit d'une nomenclature du ministère de la Justice qui repose sur les différents textes de loi s'appliquant en France.

En 2014, un groupe de travail « Cybercriminalité », piloté par le SSMSI, a été mis en place avec des représentants du ministère de la Justice, du ministère de l'Intérieur, du ministère de l'Économie et des Finances et du ministère de l'Économie Numérique pour établir une définition de ce concept : la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou principalement au moyen d'un système d'information et de communication (SIC), à savoir : les infractions spécifiques à l'encontre des SIC et de leurs données, les infractions relatives à la diffusion de contenus illicites via les SIC et les autres infractions tentées ou commises principalement au moyen des SIC.

Par ailleurs, une autre spécificité de la cybercriminalité, compliquant sa mesure ou sa connaissance statistique dans un cadre national standard, est son caractère largement transnational : les atteintes subies par la victime sur le territoire national peuvent provenir d'attaques opérées depuis l'étranger, des fonds peuvent être détournés vers l'étranger et les données techniques nécessaires à l'enquête peuvent être hébergées à l'étranger.

Une production fragmentée de données statistiques sur la cybercriminalité

Une multitude d'acteurs fournit des chiffres sur la cybercriminalité. La plupart d'entre eux ne sont pas labellisés au sens de la statistique publique mais peuvent néanmoins être abondamment commentés dans le débat public.

Ainsi, un grand nombre de sociétés privées fournissent des statistiques ou des études sur la cybercriminalité : les sociétés offrant des services de sécurité informatique (comme les éditeurs de logiciels antivirus), les sociétés d'assurance ou encore les cabinets de conseil. Ces données peuvent être d'un grand intérêt pour appréhender les nouvelles formes de cyberdélinquance. Cependant, ces acteurs privés ont des intérêts propres et la méthodologie utilisée n'est pas forcément transparente :

les chiffres doivent être pris avec un certain recul et l'interprétation en termes statistiques doit être prudente.

La fragmentation[6] de la production de données renvoie dans une certaine mesure à l'hétérogénéité conceptuelle de la cybercriminalité. Le rôle de la statistique publique et du SSMSI est de diffuser des résultats à la fois garants d'une qualité statistique certaine et dont l'homogénéité facilite l'interprétation.

(6) Côté A.-M., Bérubé M., Dupont B., *Statistiques et menaces numériques* – Comment les organisations de sécurité quantifient la cybercriminalité, Réseaux 2016/3.

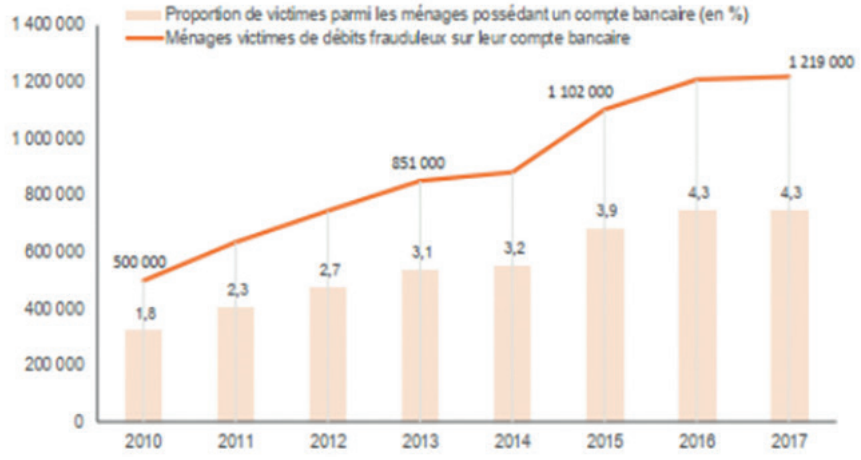
Sources et résultats de la statistique publique sur la mesure de la cybercriminalité

Appréhender la cybercriminalité par les enquêtes sur échantillons représentatifs

Les données d'enquêtes sur échantillons représentatifs de ménages ou d'entreprises peuvent être mobilisées pour appréhender et quantifier certains aspects de la cybercriminalité par le prisme des victimes.

Depuis 2011, le questionnaire de l'enquête « Cadre de Vie et Sécurité » comprend

Nombre annuel de ménages victimes de débit frauduleux sur leur compte bancaire et proportion de ménages victimes entre 2010 et 2017



Champ • Ménages ordinaires de France métropolitaine.
Source • Enquêtes Cadre de vie et sécurité 2011 - 2018, Insee-ONDRP-SSMSI.

un module spécifique sur les escroqueries bancaires qui sont en forte progression : la proportion de ménages qui déclarent avoir été victimes de débit frauduleux sur leur compte bancaire a plus que doublé entre 2010 et 2017[7], passant de 1,8 % à 4,3 %.

(7) Rapport d'enquête « cadre de vie et sécurité » 2018 (SSMSI).

Ces atteintes ont une large composante « cyber » : en moyenne entre 2015 et 2017, 56 % des ménages victimes indiquent que le débit frauduleux a été effectué sous la forme d'un achat en ligne réglé par carte bancaire. En 2018, le questionnaire s'est également enrichi d'un module spécifique sur les arnaques. Là aussi, la composante « cyber » de ces infractions est très marquée : en 2017, pour un ménage victime d'une arnaque sur deux, le contact se réalise via Internet, que ce soit par un site en ligne ou par un courriel.

L'enquête sur l'utilisation des technologies de l'information et de la communication (TIC) et le commerce électronique dans les entreprises, réalisée annuellement par l'Insee auprès d'environ 13 000 sociétés, comporte en 2010 et 2015 un module spécifique de questions sur la sécurité des TIC. La part de sociétés victimes d'incidents liés aux TIC est en progression. En particulier, 7 % des sociétés déclarent avoir subi en 2015 une destruction ou une altération de données due à l'attaque d'un programme malveillant ou à un accès non autorisé, alors qu'elles étaient 4 % en 2010[8].

(8) Demoly E., Vacher T., Sécurité numérique et médias sociaux dans les entreprises en 2015, Insee Première n°1594.

Une quantification de la cybercriminalité par les données administratives de la délinquance enregistrée

La quantification de la cybercriminalité couvrant un spectre d'infractions plus large s'effectue à partir des données administratives de la délinquance enregistrée.

Cette mesure repose sur les logiciels de rédaction des procédures de la police (LRPPN) et de la gendarmerie (LRPGN), en s'appuyant sur une

Modalités de la prise de contact pour les arnaques

Modalité de la prise de contact	%
Internet, contact en ligne, site, courriel	51
Par téléphone	23
À domicile	7
En magasin, sur un marché, salon ou foire	7
Par courrier papier	ND
Autres	10

ND : non diffusable, l'effectif de victimes ayant répondu étant inférieur à 30.
Champ : France métropolitaine, individus âgés de 14 ans et plus victimes d'arnaque en 2017. Arnaque la plus récente.
Source : Enquête Cadre de vie et sécurité 2018, Insee-ONDRP-SSMSI ; traitements SSMSI.

liste, définie par le groupe de travail mentionné supra, de Natinf, dites « spécifiques », relevant explicitement de la cybercriminalité. Elles sont au nombre de 97 et 59 d'entre elles décrivent des atteintes aux systèmes de traitement automatisé des données.

Les systèmes d'information permettent aussi le comptage d'infractions « cyber » au sein d'autres Natinf, dites « génériques », qui n'identifient pas explicitement des actes de cybercriminalité mais qui peuvent relever de la cybercriminalité dès lors qu'elles ont été commises sur internet ou dans le cadre d'un SIC. Le repérage de ces infractions s'effectue sur le mode opératoire, le contexte de la procédure et la nature de lieu de l'infraction pour la police (LRPPN) ou par une coche « cyber » déclenchée au moment de la rédaction du message d'information statistique pour la gendarmerie (LRPGN).

Après expertise de la qualité des données recueillies, le SSMSI estime qu'il ne peut diffuser pour l'instant, auprès du grand public, que les évolutions des atteintes aux systèmes de traitement automatisé des données[9]. En effet, il considère que les autres NATINF spécifiques ne sont pas toujours suffisamment utilisées lors de l'enregistrement et que les variables annexes servant au repérage des infractions « cyber » ne sont pas toujours bien renseignées.

(9) État de la menace liée au numérique en 2019 (Ministère de l'Intérieur).

Une mesure de la cybercriminalité enregistrée permettant de mieux apprécier son ampleur et son évolution temporelle est néanmoins envisageable dans un futur proche. À cette fin, des travaux sont en cours au SSMSI en collaboration avec le SSP Lab de l'Insee, pour mieux identifier, à partir de la description sur la manière d'opérer, les infractions qui relèvent de la cybercriminalité en combinant l'utilisation de techniques innovantes d'analyse textuelle et de machine learning. De plus, l'analyse des données issues des plateformes de signalement en ligne (Percev@l pour les fraudes à la carte bancaire, Pharos pour les contenus illicites sur Internet) viendra compléter le panorama sur la cybercriminalité au-delà de la seule délinquance enregistrée.

L'AUTEUR

Diplômé de l'Ensae et du master APE de l'École d'Économie de Paris, Tiaray Razafindranovona est responsable des méthodes statistiques au Service statistique ministériel de la sécurité intérieure.

Sa dernière contribution aux publications Interstats du SSMSI porte sur l'analyse conjoncturelle de la délinquance enregistrée : Interstats Conjoncture n° 49 – octobre 2019. [https://www.interieur.gouv.fr/Interstats/Actualites].

L'AUTEUR

Docteur en sciences de gestion, André Moreau étudie les statistiques de la délinquance. Officier de liaison pour la Gendarmerie nationale auprès du Service statistique ministériel de la sécurité intérieure, ses travaux portent sur les phénomènes émergeants comme la cybercriminalité.

Sa dernière contribution aux publications Interstats du SSMSI traite des arnaques : Plus de la moitié des arnaques passent par internet - Interstats analyse n° 21 – juillet 2019. [https://www.interieur.gouv.fr/Interstats/Actualites].

UNE ASSISE SCIENTIFIQUE DE L'ÉTUDE DU CYBERHARCELEMENT

L'absence de perception de la différence entre le monde virtuel et la réalité conduit à une désinhibition qui génère une exposition d'un quotidien sur les réseaux sociaux détournée par les cyberharceleurs. Si une réponse législative sanctionne ces actes, il reste à explorer ce champ délictuel en associant une démarche scientifique et théorique avec le retour d'expérience lié à une pratique professionnelle. Le projet de recherche CyberNeTic étudie les comportements spécifiques attachés au cyberharcèlement et travaille à l'identification des stratégies d'influence et de manipulation enclenchées par les prédateurs. Le phénomène de cyberharcèlement se trouvant à la croisée de plusieurs champs disciplinaires : communication, psychosociologie, linguistique et informatique. Il s'agit donc d'inventer une méthodologie et de créer un protocole de recherche inédit qui rende intelligible l'écosystème du délinquant en repensant le rapport de la victime à son prédateur. La finalité de cette démarche est de dégager des profils de cyberharceleurs, d'identifier des phénomènes d'engrenage et de distinguer des logiques d'influence. Cette maîtrise permettra à la Gendarmerie nationale de consolider l'assise scientifique de ses missions sur le terrain en conceptualisant les actions de cyberharcèlement et en appréhendant leur probabilité de survenance.

De la victime au prédateur :
les sciences humaines et sociales pour repenser le phénomène du cyberharcèlement

Par Marlène Dulaurans et Jean Christophe Fedherbe

Une photo intime qui nous échappe, un mot de passe trop fragile, un ordinateur laissé sans surveillance, une négligence sur les réseaux sociaux… Quelques minutes d'inattention pour qu'un monde jusque-là préservé bascule dans l'impensable : le cyberharcèlement. Pour mieux appréhender ce phénomène, il faut visiter son périmètre pour cerner les stratégies de cyberharcèlement et situer les rapports entre le prédateur et sa victime.

MARLÈNE DULAURANS

Maître de conférences en Sciences de l'information et de la communication

ANDRÉ MOREAU

Enquêteur spécialisé en technologies numériques (NTECH) Cellule d'Identification Criminelle et Numérique Bordeaux

Repenser le rapport à la criminalité en ligne : les phénomènes de harcèlement

(1) Nouvelles Technologies de l'Information et de la Communication.

Si Internet a été porteur de certains idéaux, comme le partage de connaissances et l'essor des compétences, qui ont permis l'avènement des NTIC[1], il faut reconnaître que le rêve utopique a été quelque peu écorné et a ancré tout un imaginaire dans une réalité beaucoup plus cruelle où la société de l'information est devenue « *plus violente et plus inégalitaire que ne l'a été la société industrielle* » (Piatti, 2001).

En effet, la multiplication des canaux de diffusion, la viralité, la fragmentation des identités numériques sont autant de paramètres qui ont généré des vulné-

rabilités propices aux risques et menaces pour les individus, multipliant les occasions de vengeances, de diffamations, d'usurpation d'identité, *etc.* Certains auteurs y voient la résurgence d'une « *nouvelle criminalité* », d'une « *délinquance astucieuse* », d'autres identifient des « *infractions dites intelligentes* ». Il est indéniable, comme le postule Jean Carbonnier, que « *l'évolution des mœurs et des techniques [a donné] naissance à de nouvelles formes de délinquance* ». Les jeunes sont d'autant plus exposés à ces cyberviolences qu'ils ne connaissent pas les modes de défense auxquels ils peuvent avoir recours et qu'ils peuvent être amenés à se retrouver dans des situations dédaléennes. En effet, si pour le monde des adultes la séparation est bien distincte, le monde virtuel dans lequel évolue quotidiennement la jeune génération apparaît au contraire comme une extension de la vie réelle (Kerr, Lucock, Steeves, 2009). Les écrits numériques qu'ils partagent sont les illustrations de ce que Dumesnil nomme le « *copinage dématérialisé* », où des liens forts se tissent, accentués par le temps passé ensemble en ligne, l'intimité qu'ils y créent, les émotions qu'ils ressentent, *etc.*

Si cette frontière entre le monde virtuel et le monde réel apparaît de plus en plus poreuse, l'avènement du numérique et d'Internet a également enclenché une autre mutation sociale importante chez les jeunes. En effet, des « *espaces extimes* » (Flichy, 2010) ont éclos sur les réseaux sociaux encourageant les mineurs à rendre publics des éléments de leur vie qui relèveraient théoriquement de la sphère intime. Ce nouveau mode de communication, où la parole publique et la parole privée se mêlent étroitement, participe d'un phénomène général de désinhibition, dans lequel importe peu la qualité des relations entretenues en ligne puisqu'il se joue dans l'exposition de leur quotidien sur les réseaux sociaux, le besoin d'être vu, reconnu et de gagner en popularité. Dans ce contexte, l'augmentation du nombre d'informations personnelles émises sur les réseaux sociaux est corrélée avec celle d'éléments étalés, par conséquent appropriables et détournables lors de pratiques de harcèlement virtuel.

Repenser le travail collaboratif et les partenariats avec la société civile

Même si le cyberharcèlement se retrouve au cœur de nouveaux enjeux organisationnels, juridiques, sociaux, *etc.*, ses contours en sont encore peu délimités. En effet, la loi du 4 août 2014 a créé un article (222 - 33 - 2 - 2 du Code pénal), qui réprime toute sorte de harcèlement et fait figurer dans une liste de circonstances aggravantes (au 4°) celle de l'infraction commise sur Internet « par l'utilisation d'un service de communication au public en ligne. Quelques outils de lutte existent mais ils sont rapidement confrontés à la difficulté d'une réponse pénale pertinente par rapport à une infraction encore très récente pour les tribunaux. De fait, cette relativité historique a influen-

cé les recherches scientifiques qui n'ont consacré jusqu'alors que très peu de travaux à ces cyberviolences malgré une médiatisation accrue du phénomène.

À l'initiative de la Gendarmerie nationale, une collaboration inédite s'est opérée avec l'université « Bordeaux Montaigne » et le laboratoire du MICA en sciences de l'information et de la communication[2] pour permettre à la démarche théorique du scientifique, de se centrer et de s'allier à la pratique professionnelle gendarmique. Ainsi est né le projet de recherche CyberNeTic[3] qui vise à étudier les comportements spécifiques attachés au cyberharcèlement et à identifier les stratégies d'influence et de manipulation enclenchées par les prédateurs lorsqu'ils commettent leurs exactions. En instaurant une démarche de recherche-action, il s'est agi pour la Cellule d'Identification Criminelle et Numérique de Bordeaux de s'appuyer sur l'analyse conceptuelle propre à la recherche pour améliorer la connaissance de sa propre pratique et pour favoriser une meilleure compréhension de l'impact de ses interventions. Dans le même temps, grâce à l'expérience éclairée du terrain, les savoirs théoriques ont été également enrichis pour offrir une nouvelle lecture des cyberviolences et accompagner le cas échéant la conduite de changements. Le retour d'expérience nous a démontré que trois conditions doivent être réunies pour que ces visions croisées soient parfaitement complémentaires. En effet, la collaboration se doit d'être co-constructive, flexible et compréhensive.

(2) https://mica.u-bordeaux-montaigne.fr/

(3) « CyberNeTic. Du virtuel au réel : se prémunir des mécanismes du cyberharcèlement »

La co-construction est essentielle dans un premier temps parce qu'elle permet d'instaurer une relation dialogique constante où les modes empiriques et théoriques de fonctionnement trouvent une articulation propre. Le fondement même de cette collaboration est celui de la réactivité, chacune des parties prenantes s'impliquant sur toutes les phases méthodologiques, de l'analyse des données, de l'interprétation des résultats, de l'implémentation des actions, *etc.*

Cette co-construction est indissociable dans un deuxième temps d'une démarche qui s'appuie sur la flexibilité. En effet, le projet de recherche est inédit et nécessite d'inventer une méthodologie et de créer un protocole de recherche qui au fur et à mesure de la mise en place d'actions sur le terrain, opère des itérations constantes vers les préceptes théoriques adéquats.

Enfin le travail collaboratif doit s'inscrire dans une démarche compréhensive car il permet de mettre en correspondance des réalités professionnelles aidant à l'intelligibilité de la connaissance de l'écosystème du délinquant et de son comportement en ligne. Pour cela, les données qualita-

tives sont privilégiées donnant aux acteurs sociaux la possibilité de devenir les sujets conduisant à la recherche.

© Gendarmerie nationale

La dimension scientifique de l'étude doit se nourrir de la transversalité des approches mêlant les retours d'expérience issus de la pratique et une théorisation des stratégies des prédateurs.

Repenser le rapport à la victime et au prédateur

L'analyse des phénomènes de cyberharcèlement nécessite également de repenser le rapport aux victimes en reconsidérant le rapport même au prédateur. En effet, ce sujet émergent s'invite de plus en plus régulièrement au débat public et la question sociétale divise ouvertement. Les affaires médiatiques de la ligue du LOL, de Marie Laguerre, de Marion Seclin, d'Isabelle Saporta, de Linda Kebbab, de Nadia Daam, etc., sont les témoignages de délits qui incitent à réexaminer les délais de prescription des faits et les niveaux de responsabilités pour répondre au mieux aux infractions commises et accompagner les victimes dans leur dépôt de plainte.

La science peut être amenée à jouer un rôle constructif dans cette réflexion. En effet, le phénomène de cyberharcèlement se retrouve à la croisée de plusieurs champs disciplinaires (sciences de l'information et de la communication, de la psychosociologie, de la linguistique, de l'informatique, etc.) en imposant que le traitement de l'objet d'étude s'observe au regard de la transversalité pour une pratique d'intervention « gendarmique » véritablement adaptée aux réalités du terrain.

Par ailleurs, les données qui constituent le cœur d'observation des phénomènes de cyberharcèlement revêtent une sensibilité particulière pour les victimes : échanges discursifs relevant de l'intime, photo ou vidéo compromettante, etc. Autant d'éléments qui touchent à l'intégrité des personnes et qui impliquent une dimension réputationnelle à haute valeur sociale. Aussi faut-il envisager d'élaborer des modes de traitement de ces données dites « sensibles » en garantissant une protection absolue avant toute utilisation. Il faut pouvoir assurer l'anonymisation et la sécurisation de certains documents ou procédures détenus sur le territoire national par différentes unités, procéder à leur collecte et à leur extraction, à leur transfert, à un accompagnement éclairé du traitement quantitatif et qualitatif pour que l'interprétation soit la plus pertinente possible.

S'il est pris soin à chaque étape de préserver les victimes, nous souhaitons recentrer notre projet de recherche sur

l'étude du phénomène de cyberharcèlement par une approche compréhensive du discours des prédateurs et des mécanismes manipulatoires qu'ils mobilisent pour contraindre, forcer, violenter, *etc.* L'un des traits majeurs de notre travail consiste à s'appliquer à faire émerger des figures « idéales-typiques » de cyberharceleurs afin de proposer une interprétation étayée de l'émergence du phénomène social dans différents contextes d'origine (pornodivulgation, arnaque aux sentiments, usurpation d'identité, commentaires haineux, *etc.*), d'appréhender la complexité du champs infractionnel (extraterritorialité, temporalité, *etc.*). Cette approche permettra d'identifier des phénomènes d'engrenage enclenchés, de distinguer des logiques d'influence, de construire des catégories de comportement, de comprendre la signification des écarts observés dans des actes singuliers, etc. Il s'agit pour la Gendarmerie nationale de consolider l'assise scientifique de ses missions sur le terrain soit en conceptualisant le sens subjectivement possible des actions de cyberharcèlement, soit en appréhendant au plus juste la probabilité pour qu'elles interviennent.

Bibliographie :

- CARBONNIER, Jean. Sociologie juridique. PUF, 1978. ISBN 2130461824, 9782130461821.
- FLICHY Patrice, Le sacre de l'amateur. Sociologie des passions ordinaires à l'ère numérique, La République des idées, 2010, 112 pages.
- KERR Ian, LUCOCK Carole, STEEVES Valerie, Lessons from the identity trail. Anonymity, privacy and identity in a networked society, Oxford University Press, 2009, 592 pages.
- PIATTI, Marie-Christine. Les libertés individuelles à l'épreuve des nouvelles technologies de l'information. PUL, 2001. ISBN 2729706747, 9782729706746.

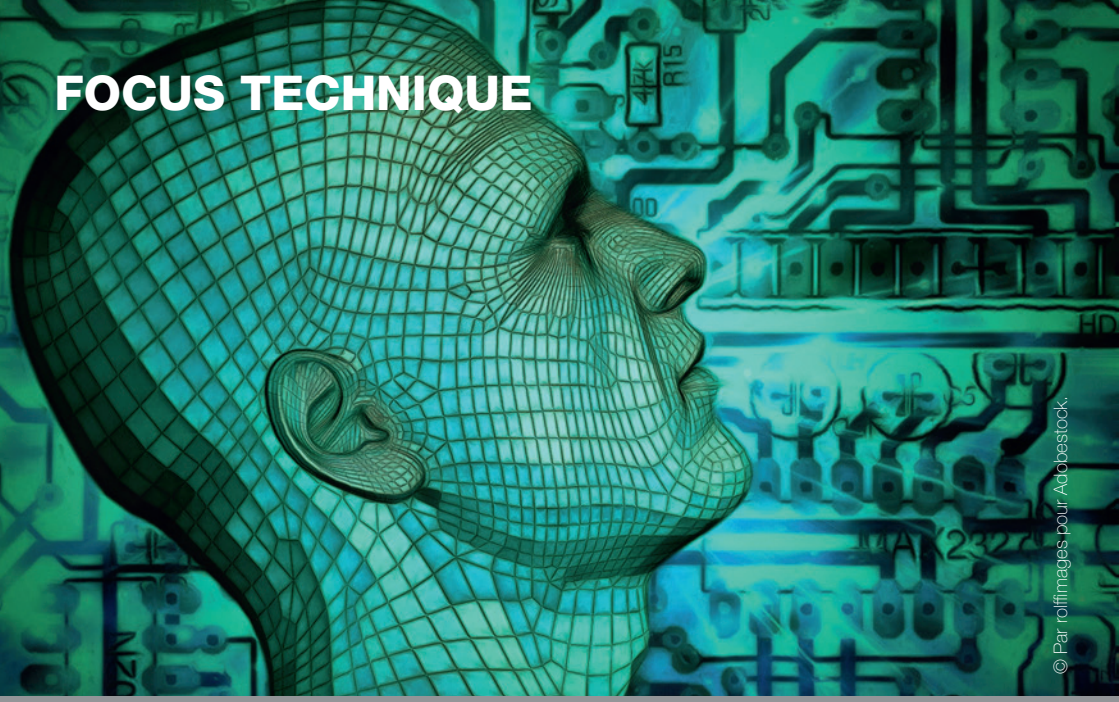
L'AUTEURE

Marlène Dulaurans est maître de conférences en Sciences de l'Information et de la Communication, auprès de l'université Bordeaux Montaigne. Rattachée au laboratoire du MICA (Médiation, Information, Communication, Art - EA 4426) dans l'axe Communication, Organisations & Sociétés, ses travaux se concentrent principalement sur les médias et réseaux sociaux, les pratiques émergentes et les nouvelles formes d'expression sur le net, ainsi que le cyberharcèlement.

L'AUTEUR

Officier de police judiciaire depuis mai 1990, Jean-Christophe Fedherbe sert en tant qu'enquêteur spécialisé nouvelle technologie (Ntech) dès 2006 en unité de recherche à PAU. Il rejoint une unité similaire à Bordeaux, puis devant l'émergence des nouvelles technologies dans le domaine judiciaire, il est affecté en 2011 à la Brigade Départementale de Renseignements et d'Investigations Judiciaires (BDRIJ) pour occuper le poste dédié à la criminalistique informatique puis il rejoint la Section Opérationnelle de Lutte contre les Cybermenaces (SOLC) - Cellule d'Identification Criminelle et Numérique. Ses champs d'expertise portent principalement sur le recueil de la preuve numérique.

Il est titulaire depuis 2012 d'un master 2 en Sécurité des Systèmes d'Information (SSI).



LA MODÉLISATION 3D EST UNE MODALITÉ D'AUTHENTIFICATION

La certitude de l'identité d'une personne et de sa présence sur une scène peut être appuyée, dans une logique probatoire, par une reconnaissance biométrique qui passe par une authentification qui peuvent emprunter une technique de modélisation 3D.

La méthodologie mêle la capacité et la puissance de calcul de logiciels, capables d'établir un modèle 3D d'un visage à partir de plans photographiques différents et de vidéos. L'expertise technique d'un opérateur, qui tempère par des traitements spécifiques le caractère dégradé d'images, permet d'affiner la reconnaissance d'une personne.

Ces méthodologies sont déjà utilisées avec succès par l'IRCGN pour la modélisation des scènes de crime. Pour rendre la modélisation 3D accessible, les protocoles pourront, dans le cadre de ce nouveau projet, être mis à la disposition des enquêteurs de terrain via les smartphones « Neogend » et généralisés à tous types de traces et d'indices.

Projet de modernisation de la biométrie : l'authentification d'identité grâce aux visages 3D

Questions à Marie-Charlotte Poilpré

L'examen du visage est l'une des principales modalités biométriques utilisées. Facile d'accès, non intrusive, innée, c'est la méthode que nous utilisons tous pour nous reconnaître. Il subsiste un questionnement sur la fiabilité de la méthode et la confiance que l'on peut accorder aux machines. Il reste également à évaluer comment les experts de la gendarmerie envisagent d'améliorer leurs compétences en termes d'authentification d'identité par le visage.

MARIE-CHARLOTTE POILPRÉ

Officier criminalistique
Institut de Recherche Criminelle de la Gendarmerie Nationale

Qu'est-ce que l'authentification d'identité ?

La biométrie peut être définie comme la reconnaissance d'individus, sur la base de leurs caractéristiques biologiques ou comportementales[1].Aujourd'hui, avec les avancées technologiques de ces dernières années, elle s'est popularisée et nous entoure : contrôle d'accès, déverrouillage de smartphone, vote électronique, passage aux frontières, ouverture de compte,… Nos empreintes digitales et nos photos remplacent désormais les obsolètes mots de passe.

(1) Jain A. K., Roos A., « Bridging the gap between biometrics and forensic science », Handbook of biometrics, 2015

La biométrie est employée selon deux finalités : l'identification et l'authentification. L'identification vise à répondre à la question « Qui êtes-vous ? » ; cela consiste à confronter une donnée biométrique d'une personne (photographie, voix, empreinte digitale, prélèvement ADN, à une série d'identités connues, enregistrées dans une base de données, afin de déterminer une liste de candidats

probables. En général, des scores sont calculés par les algorithmes et les candidats sont classés par ordre de pertinence. Dans le domaine des visages, c'est ce qu'on appelle la **reconnaissance faciale**.

L'authentification, quant à elle, vise à répondre à la question « Êtes-vous bien Monsieur X ? » ; cela consiste à juger de la ressemblance entre une donnée biométrique d'une personne se disant « Monsieur X » avec le modèle de référence enregistré de « Monsieur X », afin de confirmer l'identité. Avec les visages, on parle de **comparaison faciale**.

Dans le système judiciaire français, la reconnaissance faciale se fait au moyen d'un système automatisé. Ce dernier confronte l'image d'un auteur d'infraction inconnu aux photographies présentes dans la base de données des délinquants. Il en ressort une liste de suspects potentiels qui oriente les investigations des enquêteurs.

Lorsqu'un suspect sérieux est identifié, les enquêteurs demandent confirmation de son identité aux experts de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (I.R.C.G.N.), qui procèdent à une comparaison faciale. Cette analyse est réalisée manuellement, par comparaison des caractéristiques morphologiques.

Avec les technologies actuelles de traitement des images et de biométrie, comment expliquez-vous que les experts réalisent encore la comparaison faciale manuellement ?

Les systèmes automatisés, tels que celui qui est utilisé par les forces de l'ordre ou encore ceux qui autorisent le déverrouillage des smartphones, sont dits « contraints » : le visage doit être présenté de face, yeux ouverts, l'image doit être de bonne résolution et l'illumination contrôlée. Les algorithmes de reconnaissance faciale sont assez peu robustes aux variations de pose trop importantes ; seuls quelques degrés de rotation sont tolérés par rapport à la prise de vue de face. Ainsi, il ne sera pas possible, pour un système automatisé, de comparer un visage de profil avec un visage de face.

Or, en criminalistique, les experts sont souvent (si ce n'est tout le temps) confrontés à des images dont les conditions de prise de vue ne sont pas maîtrisées. Les visages sont généralement capturés par des caméras de vidéo protection, placées en hauteur et pas nécessairement dans l'axe du déplacement. Les images peuvent être prises de nuit et les systèmes vidéo présentent rarement une résolution propice à la comparaison faciale (c'est-à-dire permettant de voir les détails fins du visage). Ainsi, les experts n'ont à

leur disposition que des images où l'auteur est visible de profil et en plongée, rendant impossible l'utilisation des algorithmes.

Quant aux images de la personne suspectée, nous travaillons principalement avec les photographies anthropométriques issues du fichier des délinquants. Il s'agit d'un jeu de trois images montrant la personne de face, sur son profil droit et sur son trois-quarts gauche.

Avoir des images montrant l'auteur et le suspect dans la même position est donc extrêmement rare et ceci explique que les experts travaillent sur les images manuellement.

La méthode préconisée par les communautés de laboratoires de criminalistique (l'ENFSI[2] pour l'Europe et le FISWG[3] pour les pays anglo-saxons) est celle dite de l'analyse morphologique. Elle consiste en la comparaison de 19 composantes faciales, sur la base de leur forme, leur position et leurs détails discriminants (yeux, nez, bouche, oreilles, ligne d'implantation des cheveux, sourcils, rides, imperfections dermatologiques,...). L'expert observe et juge de la ressemblance de chacune de ces composantes puis prend une décision pour répondre à la question « s'agit-il de la même personne ? ».

La littérature et de récentes expérimentations démontrent que, dans des conditions idéales, grâce à leur formation et la méthodologie employée, les experts obtiennent de très bons résultats en la matière[4,5,6]. Mais tout le problème de la discipline est là : nous ne sommes jamais dans des conditions idéales !

Si la méthode et les experts sont bons, comment pourrions-nous nous placer dans les conditions idéales et ainsi rendre la comparaison de visages meilleure, voire infaillible ?

Vous l'aurez compris, la principale difficulté réside dans la qualité des images issues de vidéo-surveillance et la concordance de position entre les images de l'auteur et celles du suspect.

S'agissant du premier point, il faudrait pouvoir agir sur la qualité des systèmes de vidéoprotection déployés.

En 2007, un arrêté technique[7] a été rédigé afin de contraindre les installations de

(2) European Network of Forensic Science Institutes.

(3) Facial Identification Scientific Working Group.

(4) White D., Phillips P. J., et al., « Perceptual expertise in forensic facial image comparison », *Proceedings of the Royal Society : Biological Sciences*, 2015.

(5) Towler A., White D., Kemp R. I., « Evaluatinf the feature comparison strategy for forensic face identification », Journal of Experimental Psychology : Applied, 2017.

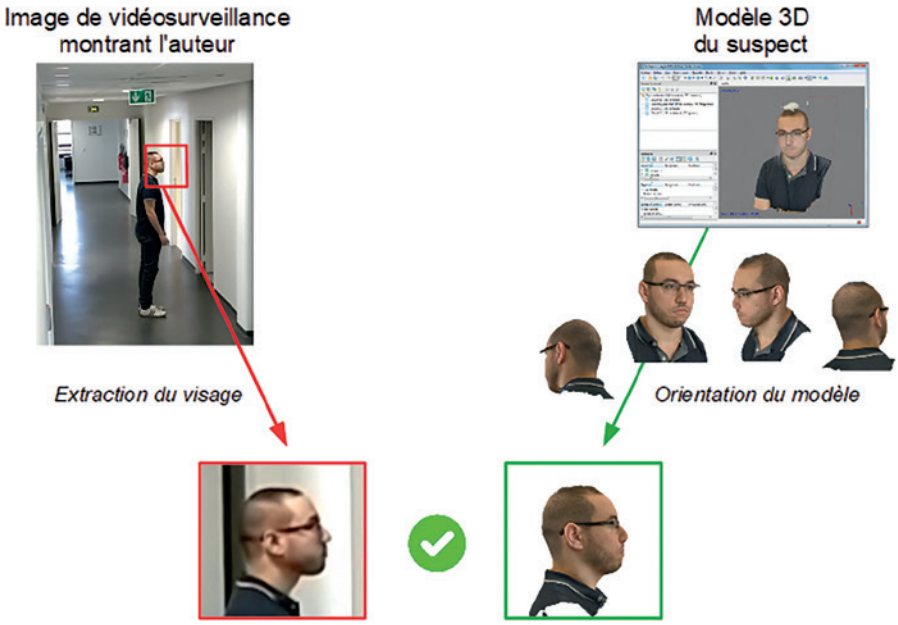
(6) Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

(7) Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

systèmes vidéo, notamment en imposant une résolution minimale et un cadencement d'images minimal. Lorsque ceci s'avère insuffisant (par exemple : sujet trop loin de la caméra ou conditions d'illumination défavorables), l'expert peut procéder à des traitements numériques des images afin de mieux faire ressortir les composantes faciales. Il faut néanmoins être conscient du fait que la marge d'amélioration des images est assez faible. Plus la qualité sera dégradée, moins les détails fins du visage seront visibles et moins l'expert pourra se prononcer de manière appuyée.

En ce qui concerne la concordance de pose, il n'est évidemment pas possible d'agir sur les images de l'auteur. En revanche, l'idée du projet lancé dans notre laboratoire à l'I.R.C.G.N. est d'agir sur les images du suspect. Ce dernier étant connu, il s'agit de ne plus capturer uniquement les trois photographies face/profil/trois-quarts, mais de générer un modèle 3D du visage afin de pouvoir le placer dans l'exacte position de l'auteur.

Depuis 2 ans maintenant, nous testons des modalités de modélisation 3D. Le département Signal-Image-Parole de l'I.R.C.G.N. réalise des modélisations 3D de scènes de crime depuis plus de 10 ans et jouit ainsi d'une expertise en la matière. Parmi les moyens connus de modélisation, certains ont dû être mis de côté du fait de leur incompatibilité avec le vivant (scanner laser notamment). Après plusieurs phases de tests, notre choix s'est porté sur la photogrammétrie. Il s'agit d'un procédé qui vise à combiner plusieurs photographies d'un objet prises sous des angles différents pour en générer une représentation 3D. S'agissant du visage, qui est un « objet » complexe par ses courbes, ses jeux d'ombres, ses différents tissus, nous avons établi un nombre minimal de 150 clichés. Ci-dessous, un exemple de modèle 3D de visage :



Maintenant que nous avons un modèle 3D du visage, il est possible de le repositionner dans la même position que l'auteur, permettant ainsi à l'expert de procéder à une comparaison par analyse morphologique pertinente.

Ce projet n'est-il pas un peu trop teinté « science-fiction » ? Les gendarmes du terrain pourront-ils y avoir accès ?

Bien évidemment, le but de ce projet est de rendre la technologie accessible à tous les gendarmes, et en particulier aux enquêteurs, sur le terrain, qui réalisent les auditions des suspects. C'est pourquoi ce projet s'inscrit dans une démarche réaliste qui nous a orientés vers les seules technologies que nous savons matures, simples d'utilisation et mobiles.

De manière concrète, chaque gendarme dispose aujourd'hui d'un smartphone, le « Neogend ». Il s'agira, pour eux, de prendre une vidéo du suspect, selon un protocole défini, qui maximise les chances d'obtenir un modèle 3D viable. La vidéo sera ensuite transmise à l'I.R.C.G.N. via notre réseau de télécommunication sécurisé. Elle sera traitée de manière automatique sur un serveur dédié, au moyen d'une licence logicielle de photogrammétrie. Le modèle du visage sera renvoyé à l'enquêteur sous forme de pdf3D et nous conserverons à l'I.R.C.G.N., dans le temps de l'enquête, le modèle « riche » afin d'être en mesure de l'utiliser à des fins de comparaison faciale.

Ce process sera également généralisé à tous types de traces et indices (c'est l'objet du projet Phidias) : semelles de chaussure pour comparaison avec des empreintes de pas, carrosserie de véhicule à la suite d'un choc pour analyse en accidentologie,… L'objectif est, à terme, de rendre la modélisation 3D accessible à tous et pour tous types d'analyses criminalistiques.

Avec ce projet, nous confirmons l'utilité et la puissance des modèles 3D, notamment pour la numérisation des scellés.

L'AUTEURE

Marie-Charlotte Poilpre, capitaine de gendarmerie, est ingénieur en traitement des images médicales de formation. Officier criminalistique à l'Institut de Recherche Criminelle de la Gendarmerie Nationale depuis 2016, elle est responsable de l'unité d'expertise Vidéo-Imagerie du département Signal-Image-Parole et membre du comité d'éthique.

En parallèle de ses activités d'expert judiciaire, elle prépare depuis deux ans un doctorat avec l'Université Paris-Est Créteil ayant pour sujet la modélisation 3D des visages aux fins d'expertises judiciaires de comparaison faciale.

JUSTICE : UNE RÉPONSE FONDÉE SUR UN RÉSEAU NATIONAL ET UNE COOPÉRATION INTERNATIONALE

La cybercriminalité a pour caractéristique principale d'être polymorphe et très évolutive. Elle bénéficie du dynamisme de l'écosystème numérique. La classification des infractions, hormis celle qui est issue de la classique sphère du traitement automatisé des données, reste délicate du fait du foisonnement des pratiques délictuelles qui épousent les évolutions technologiques. La difficulté d'établir un régime probatoire ne peut se régler que dans un cadre de coopération internationale incluant les GAFAM, avec l'aide d'EUROPOL, EUROJUST et INTERPOL. Sur un plan national, on ne peut que se féliciter du rôle primordial du tribunal de grande instance de Paris qui bénéficie depuis la loi du 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et de crimes de sabotage informatique. Au travers d'un réseau de magistrats « cyber-référents », les juridictions interrégionales spécialisées (JIRS) accroissent le traitement du contentieux de la cybercriminalité. La densification des relations entre les acteurs judiciaires et de la cybersécurité est également une priorité. La DACG contribue aux travaux stratégiques du centre de coordination des crises cyber (C4) et aux réunions du Groupe de Contact Permanent (GCP) qui a pour objectif d'améliorer le dialogue avec les acteurs privés.

Lutte contre la cybercriminalité
en 2019 : défis et voies d'amélioration

Par Jacques Martinon

Le cybercriminel a pour caractéristique singulière de s'adapter rapidement aux évolutions de l'environnement numérique, afin d'en exploiter les failles techniques ainsi que de détourner les nouveaux usages légitimes en opportunité d'obfuscation[1] voire d'ingénierie sociale au détriment des victimes. Symétriquement, les acteurs de lutte contre la cybercriminalité doivent adapter leurs stratégies, méthodes et organisations afin d'améliorer leur efficacité.

JACQUES MARTINON

Chef de la Mission de lutte contre la Cybercriminalité (MLC)

Direction des Affaires Criminelles et des Grâces (DACG)

Toutes les juridictions peuvent certes connaître des faits de cyberdélinquance[2], mais il convient de relever que le tribunal de grande instance de Paris bénéficie d'une compétence concurrente nationale en matière de cyberattaques[3]. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation en priorisant les tendances les plus préoccupantes touchant la population française ainsi que son tissu économique.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité (**partie I**), avant d'aborder les adaptations de l'organisation judiciaire actuelle et les nouvelles relations des acteurs judiciaires avec ceux de la cybersécurité (**partie II**).

(1) NDLR : L'offuscation, assombrissement, obscurcissement ou brouillage est une stratégie de gestion de l'information qui vise à obscurcir le sens qui peut être tiré d'un message. Cette stratégie peut être intentionnelle ou involontaire. Cette stratégie peut par exemple servir en matière de protection de la vie privée (par exemple, pour la protection des données personnelles ou la gestion de la réputation numérique), mais peut servir de base à un choix dans le contenu du message, à des tactiques de guerre ou à la sauvegarde de la confidentialité des informations. L'usage utilise aussi le terme d'obfuscation, néologisme d'emprunt lexical tiré de l'anglais obfuscation venant du latin obfuscare (construit avec ob : devant, fuscus : sombre).

Partie I - Une cybercriminalité polymorphe et occulte

La typologie de la cybercriminalité demeure un défi intellectuel puisque l'angle traditionnel des qualifications pénales est imparfait. Les « cyberattaques » recouvrent en réalité de nombreux « phénomènes cyber » distincts dans leurs modes opératoires et leurs motivations, tels le cyberespionnage, le cybersabotage, le rançongiciel…

Aujourd'hui, la cybercriminalité reste largement occulte, notamment du fait que les outils statistiques traditionnels sont de facto inopérants pour apprécier finement les évolutions des phénomènes. À cela s'ajoutent les problématiques classiques du chiffre noir et d'une preuve numérique parfois chimérique.

I. Une cybercriminalité polymorphe et évolutive

La cybercriminalité a pour caractéristiques principales d'être polymorphe et naturellement très évolutive, bénéficiant du dynamisme de l'écosystème numérique.

A/ Une classification délicate

La cyberdélinquance, au sens strict, couvre les phénomènes pénaux dont l'objet est l'atteinte à un système de traitement automatisé de données (STAD) réprimée par les articles 323-1 à 323-4 du Code pénal. Dans la pratique, cette catégorie est divisée entre les phénomènes de haute intensité (atteinte aux intérêts fondamentaux de la Nation, dimension internationale, haute technicité, nombre important de victimes avérées ou supposées) et de basse intensité.

La seconde catégorie regroupe les phénomènes qui ont pour vecteur principal un STAD ou ont été facilités par son utilisation ; il s'agit de la cyberdélinquance au sens large, incluant de nombreuses escroqueries. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'internet sombre (*darknet*).

B/ Les nouveaux métiers de la cybercriminalité

La cybercriminalité prospère et de nouveaux « métiers » fleurissent régulièrement, faisant naître le concept de « *Crime as a Service* » (analogie avec les services informatiques traditionnels), telles les locations/ventes d'infrastructures de type

(2) Nous utiliserons indifféremment les expressions « cybercriminalité » et « cyberdélinquance », étant entendu que le terme « cybercriminalité » est le plus usité du fait de son pendant anglo-saxon « cybercrime », alors même que la quasi intégralité des infractions « cyber » sont bien des délits, et non des crimes au sens du droit pénal français.

(3) Article 706-72-1 du code de procédure pénale (créé par la loi n°2016-731 du 3 juin 2016) : « *Pour la poursuite, l'instruction et le jugement des infractions entrant dans le champ d'application de l'article 706-72, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles 43, 52 et 382.*»

(4) Un cas célèbre étant, en 2016, le Botnet issu du maliciel Mirai qui a servi à des attaques DDos (Distributed Denial of Service) touchant notamment OVH et Dyn, cette dernière affectant une partie critique d'Internet au niveau de la gestion des services DNS (Domaine Name System). En août 2019, le C3N (gendarmerie nationale) a démantelé avec succès le Botnet Retadup composé de plus 500 000 machines infectées.

botnets (réseau d'ordinateurs ou d'objets connectés[4] « zombies », sous le contrôle d'un serveur dit *Command & Control*), de maliciels divers (comme certains rançongiciels qui connaissent un regain dévastateur auprès des entreprises et des collectivités territoriales), des services de *Crypter/Packer* (augmentant la furtivité des maliciels), de *Money mules* (personne qui transfère de l'argent acquis illégalement pour le compte de tiers) ou encore de *Mixer/Blender*[6] (facilitant le blanchiment des cryptomonnaies).

(5) Le site Bestmixer.io a toutefois été mis sur la touche par une action conjointe d'EUROPOL et des enquêteurs financiers néerlandais.

Les cryptomonnaies sont sources de nombreuses opportunités, en les dérobant aux plateformes d'échanges ou aux particuliers, mais également en détournant la puissance de calcul de terminaux afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (*Cryptojacking*).

Plus original, il existe des campagnes de recrutement via des annonces d'emploi pour des administrateurs de *Darknets*, comme ci-dessous pour Liberty Market :

« **Nous cherchons à recruter un membre**, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction des posts du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »

Figure 1 Source : www.ladn.eu

Dans la même veine, on relèvera un service de type « Tag Telegram », où des personnes sont simplement rémunérées pour réaliser des tags, dans des zones urbaines prédéterminées, comprenant des indications techniques pour rejoindre une discussion Telegram d'un dealer. Ce nouveau job permet de matérialiser « l'uberisation » rampante des trafics de stupéfiants, où le consommateur commande directement sa drogue via son smartphone et une application de messagerie cryptée, et se fait livrer à domicile H24 7j/7.

© Source : Trustwave

Figure 2 : cas ukrainien (15$/jour – SMIC mensuel local 140$).

Une des conséquences probables sera l'éclatement des logiques des territoires de points de *deals*, avec un déplacement sur la visibilité, la furtivité et la popularité de leur vecteur numérique de communication. D'autres tendances inquiétantes semblent se dessiner avec des applications d'échange décentralisées, anonymes et basées sur les cryptomonnaies (Ex : Openbazaar, Haven).

II. Une cybercriminalité occulte

La lutte contre la cybercriminalité est handicapée par plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice (**A**) et une preuve numérique aléatoire (**B**).

A/ Le chiffre noir de la cybercriminalité

(6) La doctrine américaine est différente à cet égard, au vu de l'activisme récent du Department of Justice (DoJ) à l'encontre de ressortissants chinois ou russes.

(7) Voir le cas d'Airbus en janvier 2019.

Certains phénomènes cybercriminels de haute intensité, comme le cyber-espionnage ou le cyber-sabotage, sont peu judiciarisés du fait de leur nature sensible[6]. La publicité d'une cyber-attaque à l'encontre d'une entreprise peut nuire à son image. Le règlement européen pour la protection des données personnelles (RGPD) est un espoir, dès lors que les violations de données personnelles conduisent à une obligation de notification dans les 72 heures à la CNIL[7].

Concernant les particuliers, les raisons du chiffre noir sont diverses, du fait d'un caractère parfois imperceptible de l'infraction ou d'un sentiment erroné de l'inutilité de la plainte, souvent couplé à de faibles préjudices matériels.

Une meilleure sensibilisation semble nécessaire, d'où l'importance du dispositif national d'assistance aux victimes d'actes de cybermalveillance[8] et des mesures facilitant le dépôt de plainte. La future plate forme THESEE (projet porté par le Ministère de l'Intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La récente loi de Programmation pour la Justice (LPJ) insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne[9].

(8) https://www.cybermalveillance.gouv.fr/

(9) Nouvel article 15-3-1 du Code de procédure pénale.

(10) Cette expression d'origine militaire fait référence à la perte soudaine des communications de l'adversaire pouvant être analysées, au profit de moyens de communications indétectables.

B/ Une preuve numérique victime du « *going dark* » [10] et de l'extraterritorialité

La libéralisation du chiffrement a amélioré sensiblement le niveau de cybersécurité mais a provoqué de manière collatérale des difficultés propres aux investigations judiciaires. La banalisation des applications de messageries instantanées chiffrées avec des protocoles particulièrement robustes comme ceux dits End to end est un défi actuel. De même, la généralisation

du chiffrement de type full disk sur les terminaux informatiques, dont les smartphones, a rendu délicate l'exploitation forensique. Enfin, les architectures réseaux de type TOR (The Onion Router) participent à l'obfuscation des comportements criminels sur les Darknets. Demain, la fusion annoncée entre les applications de messageries et les cryptoactifs ne manquera pas d'inquiéter les professionnels[11].

(11) Voir le lancement du réseau TON et la cryptomonnaie GRAM par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliards de dollars.

À cela, s'ajoute la difficulté d'une preuve numérique désormais largement stockée en dehors de nos frontières. L'année 2019 est à ce titre charnière avec d'une part le futur règlement européen *E-Evidence*, doublé d'une directive dite « représentant », et d'autre part le dialogue que va mener la Commission européenne avec les USA afin de résoudre certains conflits de lois, sans compter les négociations entourant un second protocole additionnel à la Convention de Budapest contre la cybercriminalité (Conseil de l'Europe). Anticipant ces révolutions dans l'accès transfrontalier, la politique interne de certains GAFAM (Google par exemple) s'est modifiée en transférant la gestion de certaines réquisitions judiciaires françaises de leur maison mère basée aux USA à leur filiale de droit irlandais.

Partie II - Une organisation judiciaire de plus en plus étoffée et décloisonnée

Seront ici abordées l'organisation judiciaire actuelle (**I**) ainsi que les relations des acteurs judiciaires avec les acteurs de la cybersécurité (**II**).

I. Constats sur l'organisation judiciaire en 2019

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il sera rappelé le rôle primordial du tribunal de grande instance de Paris qui bénéficie, depuis la loi du 3 juin 2016, d'une compétence concurrente nationale en matière d'atteintes aux STAD et de crime de sabotage informatique[12].

(12) Nouvel art. 706-72-1 C. proc. pén.

Cette réforme a permis de consolider la création en 2015 d'une section, dite « F1 », du parquet de Paris, dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes. Les effectifs de cette section sont toutefois modestes[13] mais un renforcement est en cours. Le constat est plus inquiétant au siège avec notamment l'absence de juge d'instruction véritablement spécialisé. Des dépêches de centralisation du traitement de certains phénomènes de cybercriminalité sont à relever, produites par la mission de lutte contre la cybercriminalité de la direction des affaires criminelles

(13) Deux magistrats, ainsi qu'un assistant spécialisé et un greffier (données août 2019).

et des grâces (DACG) du ministère de la justice[14].

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée[15]. Enfin, un réseau de magistrats « cyber-référents » dans les tribunaux, cours d'appel et JIRS est en voie de consolidation, dans les suites de la première réunion nationale des magistrats cyberréférents, co-organisé le 14 juin dernier par le Parquet de Paris et la DACG.

(14) Dépêches des 10 mai 2017 et 22 juin 2018 concernant d'une part la mise en œuvre opérationnelle de la compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et de traitement judiciaire des «rançongiciels», et d'autre part la centralisation du traitement des «fraudes aux réparations informatiques».

(15) Ex : le démantèlement de la Main noire, une plateforme du Darknet, sous la supervision de la JIRS de LILLE.

(16) http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

II. Densification des liens entre acteurs judiciaires et acteurs de la Cybersécurité

L'administration centrale (DACG), via la mission précitée, contribue aux travaux stratégiques du centre de coordination des crises cyber (C4), instauré suite à la Revue stratégique de Cyberdéfense de février 2018[16], ainsi qu'aux réunions du Groupe de Contact Permanent (GCP). Ce GCP, piloté par la délégation ministérielle en charge des industries de sécurité et la lutte contre les cybermenaces (DMISC), a pour objectif d'améliorer le dialogue avec les acteurs privés comme Apple, Google, Twitter, Microsoft, Facebook et récemment Dropbox.

De plus, la DACG fait partie du conseil d'administration du GIP ACYMA (cybermalveillance.gouv.fr) et participe à la formation commune « *souveraineté numérique et cybersécurité* » de l'IHEDN (Institut des Hautes Etude de la Défense Nationale) et de l'INHESJ (Institut National des Hautes Etudes de Sécurité et de Justice).

Conclusion

Le levier judiciaire doit gagner en maturité mais des progrès sont en cours. La coopération internationale est un facteur clé de ce succès, avec l'aide d'EUROPOL, EUROJUST et INTERPOL. Les menaces issues du monde numérique ne doivent pas rester sans réponse et les politiques publiques doivent responsabiliser certains acteurs privés systémiques, tout en assurant une formation adaptée des magistrats et enquêteurs.

AUTEUR

Jacques Martinon est titulaire d'un DEA en droit privé (Panthéon Assas) et d'un DEA en droit européen (Panthéon-Assas). Magistrat de l'ordre judiciaire depuis 2008 (promotion ENM 2006), ses premiers postes ont été juge d'instruction au Tribunal de Grande Instance de Senlis, puis juge d'instruction au Tribunal de Grande Instance de Bobigny.

Il est actuellement le chef de la mission de lutte contre la Corruption et la Cybercriminalité de la direction des affaires criminelles et des grâces (DACG), au sein du ministère de la justice.

À ce titre, il est amené à suivre l'actualité nationale en lien avec la cybercriminalité ainsi que les négociations internationales (Conseil de l'Europe, Union européenne…).

Au-delà de la cybercriminalité au sens strict, ses attributions peuvent s'étendre aux problématiques engendrées par le recueil de la preuve numérique (chiffrement, extraterritorialité...).

Enfin, il est le Point de Contact France du nouveau Réseau Judiciaire Européen sur la cybercriminalité, sous l'égide d'EUROJUST.

EN SAVOIR PLUS

Liens utiles :

État de la menace cyber (rapport DMISC 2019) : https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019

Dispositif d'assistance aux victimes d'actes de malveillance : https://www.cybermalveillance.gouv.fr/

UNE ENQUÊTE QUI GARDE SA PERTINENCE PAR LE RENSEIGNEMENT CRIMINEL

Une économie internationalisée, caractérisée par des flux massifs et des intérêts hétérogènes, floute le périmètre de l'enquête sur la cybercriminalité. C'est pour l'enquêteur un univers particulier dont il faut pénétrer la culture, ses opérateurs, ses techniques et un mille-feuille de dispositions juridiques. Il lui faut emprunter une stratégie plus large et pro-active : le renseignement criminel. Ce dernier a pour objectif de comprendre la délinquance et de proposer des stratégies concrètes pour l'annihiler. C'est une approche ouverte et concrète pour comprendre des phénomènes souvent mieux perçus par d'autres interlocuteurs et de croiser les regards sur les risques cyber. La formalisation d'une méthode et le progrès des techniques de traitement de la donnée (mégadonnées, intelligence artificielle) offrant des perspectives nouvelles, le renseignement criminel fait appel à des techniques de collecte, d'analyse et de dissémination orientées sur l'opérationnel pour déboucher sur des recommandations réalistes et évaluables. Ces réponses, tant préventives que répressives, combinent des entraves administratives, partenariales ou pénales.

L'enquête judiciaire est-elle une réponse appropriée à la cybercriminalité ?

Par Jérôme Barlatier

Héritière de la rationalité des lumières et des codes napoléoniens, l'enquête judiciaire se fonde sur le postulat d'un traitement individualisé, où un lien doit être établi par la preuve entre les faits criminels et leur auteur. Particulièrement adaptée pour les faits d'atteintes aux personnes pour lesquels le taux d'élucidation se maintient à un niveau élevé, l'enquête a progressivement été remise en question avec le développement de trois contentieux de masse qui ont fait peser un soupçon sur sa pertinence en tant que mécanisme de régulation sociale.

LCL JÉRÔME BARLATIER

Pôle judiciaire de la Gendarmerie nationale
Service central de renseignement criminel

Trois soupçons sur l'enquête judiciaire

D'abord, l'enquête montre précocement ses limites dans le traitement des **atteintes aux biens** qui ont prospéré dès l'apparition de la société de consommation et de l'accroissement des valeurs disponibles. Profitant principalement du lien d'inter-connaissance entre l'auteur et la victime, l'élucidation des investigations devient bien plus délicate dans une société d'anonymat, de mobilité des individus et d'affaissement des modes traditionnels de contrôle social.

Ensuite, l'enquête judiciaire a montré ses limites en matière de **délinquance économique et financière**. Dans l'univers de l'entreprise et de la finance, l'action de l'enquêteur est tout au plus un *ultima ratio*, un moyen auxiliaire qui vient suppléer des modes de contrôle plus spécifiques, tels que la conformité et l'assurance. Ici, la notion de risque et de régulation vient se substituer à celle de vérité et de justice. On ne dépose plainte que lorsque cela sert ses intérêts personnels.

L'enquête, acte curatif du passé, cède le pas à des dispositifs de provisionnement des risques destinés à garantir l'avenir.

Enfin, l'expansion du trafic de stupéfiants, dans les années 1970, démontre que la mécanique judiciaire est impuissante à endiguer, de façon native, un phénomène fondé sur une économie internationalisée, caractérisée par des flux massifs et des intérêts puissants. Il en est aujourd'hui de même de la plupart des activités perpétrées par les groupes criminels organisés.

Délinquance d'appropriation, criminalité organisée, délinquance économique et financière impliquent une réponse immédiate et massive, alors que le processus pénal prévoit un traitement différé au cas par cas.

Face aux volumes de contentieux, dans une logique managériale mue par la rationalité budgétaire, police et justice orientent leurs activités de détection et d'investigation sur les phénomènes prioritaires. Le réalisme de l'efficacité procédurale les invite à préférer des contentieux courts et efficaces aux dossiers de longue haleine. Ainsi, à maints égards, la lutte contre la délinquance est conditionnée par les contraintes de la procédure et les capacités de traitement de la machine judiciaire. Elle se trouve ainsi souvent réduite à égratigner la surface de phénomènes plus complexes et profondément enracinés.

Depuis vingt ans, l'émergence de la cybercriminalité confirme et aggrave ces constats.

La cybercriminalité comme ultime sommation

L'apparition de l'Internet et la démocratisation de l'informatique personnelle créent un contexte d'autant plus délicat à appréhender pour l'enquête judiciaire. En quelques années, la délinquance du monde logique est venue concurrencer celle du monde physique. Ainsi, le volume et le préjudice des escroqueries sur Internet sont désormais supérieurs aux escroqueries traditionnelles (ONDRP, 2018).

Internet est tout à la fois objet et vecteur de criminalité. Il crée une délinquance spécifique tout en offrant des opportunités de méfaits nouvelles, telles que les atteintes à la réputation, les arnaques ou le trafic de stupéfiants. Garantissant un relatif anonymat, abolissant les barrières géographiques, donnant un accès illimité aux victimes dans l'intimité de leur domicile ou de leur téléphone, cet environnement est favorable aux activités criminelles. Pour l'enquêteur, il est un univers délicat à appréhender, disposant d'une culture, d'interlocuteurs, de techniques et de dispositions juridiques spécifiques.

Confirmant les soupçons portés sur l'enquête, la cyberdélinquance est caractérisée par un taux d'élucidation et de mise

en cause particulièrement faibles. Toutefois, sa remise en cause est bien plus profonde : la faible reportabilité des infractions par les victimes révèle que celles-ci se détournent désormais des forces de l'ordre au profit d'autres modes de remédiation. De récentes études attestent, en effet, que seulement un fait sur 200 ferait l'objet d'un dépôt de plainte. En matière de rançongiciel, la volonté des entreprises de protéger leur réputation et de garder l'espoir de récupérer leurs données les incite à ne pas révéler les faits. En matière de fraude en ligne à la carte bancaire, avec un préjudice moyen inférieur à cinquante euros et une indemnisation quasi-systématique par les banques ou les E-commerçants, les préjudices sont rendus indolores pour les consommateurs. Sécurisées dans leurs transactions par une politique favorisant la confiance en l'économie numérique, les victimes ont appris à se passer de l'enquête. Les délinquants, quant à eux, génèrent d'importants bénéfices dans une relative impunité.

L'érosion progressive de la performance de l'enquête constatée depuis 150 ans devrait inviter les forces de l'ordre à réviser leur approche des phénomènes criminels en intégrant les investigations judiciaires dans une stratégie plus large et pro-active où le savoir précède l'action : le **renseignement criminel**. Certes, la préoccupation de mieux connaître les populations vivant quasi exclusivement de la délinquance n'est pas nouvelle, toutefois, la formalisation d'une méthode (Rattcliffe, 2016) et le progrès des techniques de traitement de la donnée (mégadonnées, intelligence artificielle) offrent des perspectives nouvelles en la matière.

© Gendarmerie nationale

Le renseignement criminel par ses techniques transversales génère des solutions d'ordre administratif ou pénal dans une démarche partenariale.

Le renseignement criminel a pour objectif de comprendre la délinquance et de proposer des stratégies concrètes pour l'annihiler, la réduire, la détourner ou en limiter les effets. Orienté sur les phénomènes, les bandes criminelles ou les bassins de délinquance, il propose une approche ouverte et concrète.

Ouverte, car les forces de l'ordre ne sont pas toujours le point de vérité pour la compréhension de phénomènes souvent mieux perçus par d'autres interlocuteurs publics, privés ou académiques. Un séminaire de l'observatoire national

des sciences et technologies de la sécurité (ONSTS), organisé le 3 juin 2019 à Pontoise, a ainsi illustré l'intérêt de croiser les regards sur les risques cyber.

Concrète, car le renseignement criminel fait appel à des techniques de collecte, de traitement, d'analyse et de dissémination orientées sur l'opérationnel. Les recommandations qu'il formule doivent être réalistes, précises, acceptables et évaluables. Ses réponses sont tant préventives que répressives. Elles combinent des solutions d'entrave administrative, partenariale ou pénale. La création par la Gendarmerie nationale de la plateforme PERCEVAL relative aux fraudes en ligne à la carte bancaire est une démonstration de cette volonté de trouver des solutions à ce phénomène.

Dans cette perspective nouvelle, l'enquête et la réponse pénale ne sont pas vouées à l'obsolescence. Bien au contraire, éclairées par une meilleure compréhension de la délinquance, elles peuvent être remises en situation d'efficacité.

Références

Observatoire national de la délinquance et des réponses pénales, Rapport d'enquête « Cadre vie et sécurité 2018 », disponible en ligne : https://inhesj.fr/sites/default/files/ondrp_files/publications/pdf/rapport_CVS_2018.pdf.

Ratcliffe, J. H. (2016). Intelligence-led policing. Second edition. New York : Routledge. 222 p.

AUTEUR

Le lieutenant-colonel Jérôme Barlatier est responsable de l'analyse stratégique au sein du service central de renseignement criminel (SCRC). Il est l'auteur d'une thèse de doctorat en criminologie relative à la performance des processus d'enquête (https://www.researchgate.net/publication/321485215_Management_de_l'enquete_et_ingenierie_judiciaire_recherche_relative_a_l'evaluation_des_processus_d'investigation_criminelle).

DIRECTEUR DE LA PUBLICATION

Général de brigade **Laurent BITOUZET**

RÉDACTION

Directeur de la rédaction :
Général d'armée (2S) **Marc WATIN-AUGOUARD,**
directeur du centre de recherche de l'EOGN

RÉDACTEUR EN CHEF

Colonel (ER) **Philippe DURAND**

MAQUETTISTE PAO

Maréchal des logis-chef **Anne PELLETIER**
SDG

DÉPOT LÉGAL

Raison sociale de l'éditeur :
CREOGN, avenue du 13e Dragons,
77010 Melun cedex
Général (2S) Watin-Augouard
Imprimerie : SDG - 11 rue Paul Claudel
87000 Limoges
Décembre 2019

Session nationale
SOUVERAINETE NUMERIQUE & CYBERSECURITE
SEPTEMBRE À JUIN

Avec les *Livres blancs sur la défense et la sécurité nationale* de 2008 et de 2013, le cyberespace est entré dans le champ de la sécurité nationale. Conscients des enjeux pour la défense, la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN proposent, avec l'ensemble de leurs partenaires, une formation inédite de haut niveau qui doit permettre à une quarantaine d'auditeurs, hauts cadres des secteurs public et privé

- ✓ **d'acquérir une culture des enjeux de cybersécurité et de souveraineté induits par les transformations numériques**
- ✓ **de développer une vision stratégique "cyber", au profit de l'entreprise, de l'administration et des armées**

CONTACTS

IHEDN
Secrétariat
01 44 42 46 27
securite-economique@ihedn.fr
www.ihedn.fr

INHESJ
Secrétariat
01 76 64 89 93
recrutement.auditeurs@inhesj.fr
www.inhesj.fr