LA FACE CACHÉE D'INTERNET

RAYNA STAMBOLIYSKA

LAROUSSE

LA FACE CACHÉE D'INTERNET

Avertissement de l’éditeur :

Les appels de notes en italique renvoient aux sources, en fin d’ouvrage.

LA FACE CACHÉE D'INTERNET

RAYNA STAMBOLIYSKA

LAROUSSE

AVANT-PROPOS

par Stéphane Bortzmeyer

Je pense qu'il y aura deux sortes de gens qui liront cette préface, ceux à qui mon nom dit quelque chose et les autres, de loin les plus nombreux. Je vais donc m'adresser d'abord à la seconde catégorie de lecteurs et ne pas vous plonger tout de suite dans les détails techniques que les abonnés de mon blog adorent.

Ce livre parle d'une « *face cachée d'Internet* ». Elle est lointaine, l'époque où on faisait des études se demandant « combien d'heures par jour sont passées en ligne ». Aujourd'hui, il n'y a plus de distinction claire entre temps en ligne et temps hors ligne, on est connecté plus ou moins en permanence et on a toujours sur soi ou devant soi un équipement connecté.

On ne peut pas trouver une activité humaine qui n'ait pas migré vers l'Internet, que ce soit le business, la politique, la recherche scientifique, la drague ou, comme on le verra dans ce livre, la délinquance. Comme pour toutes les évolutions importantes de l'humanité, aucun parti politique n'avait explicitement mis cela à son programme, et aucun penseur médiatique ne l'avait prévu. Est-ce une bonne ou une mauvaise chose, cette connexion

permanente ? Disons que, quelle que soit la réponse à cette question, c'est la réalité du présent ; il est donc justifié de l'étudier, en attendant de voir ce qu'offrira le futur.

Donc, aujourd'hui, tout est sur Internet. Des affirmations qu'on lit trop souvent dans les médias comme « le terroriste communiquait avec ses complices *via* Internet » sont ridicules, non pas parce qu'elles sont fausses mais parce qu'elles sont de l'ordre de l'évidence. Elles nous en apprennent autant que si on lisait en gros titres « Le terroriste conduisait une voiture sur une route » ou « Le terroriste buvait de l'eau ». Dire qu'il y a du terrorisme, de la délinquance, de la criminalité et de la guerre sur Internet, c'est simplement énoncer une conséquence du fait cité plus haut : quand toutes les activités humaines sont sur Internet, les activités négatives et/ou illégales le sont aussi. Il est donc tout à fait scandaleux que des lois citent l'utilisation d'Internet comme circonstance aggravante.

Alors, y a-t-il une « face cachée » d'Internet ? Oui, si on veut dire qu'il y a des activités qui ne se font pas au grand jour. Nous avons tous des activités non publiques (*a priori,* les relations intimes d'un couple ne sont pas censées être en place publique). Non, si on veut dire que ces activités sont forcément illégales. Nous avons tous des activités cachées qui ne sont pas illégales (et quand quelqu'un me dit le contraire, je lui demande une copie de ses bulletins de paie, de sa déclaration de revenus, le code de sa carte de crédit et la liste de ses dix derniers partenaires sexuels).

Il n'y a pas non plus de « face cachée » si on essaie de la réduire à un lieu. De même que dans le monde extérieur à Internet, la délinquance ne se limite pas au « 9-3 », mais se pratique aussi dans les beaux quartiers (sous une forme évidemment différente : un emploi fictif à la mairie ou au parlement est plus glamour qu'un vol à l'arraché), de même les activités illégales ou franchement abominables sur l'Internet ne se limitent pas à un *dark net* fantasmatique. Xavier de la Porte, dans son excellente chronique sur France Culture[1],

avait bien indiqué que le vocabulaire habituel pour parler du dark web avait de nombreuses analogies avec le vocabulaire utilisé pour parler de la banlieue, présentée comme un espace à part.

Et c'est là tout le mérite du livre de Rayna Stamboliyska. Elle explique en détail ce qui se passe loin du regard de l'utilisateur ordinaire de Facebook, ce que ne voit pas (ou pas tout de suite) l'utilisateur d'Internet ordinaire. C'est moins sensationnel mais c'est plus utile. Dans ce livre, vous apprendrez ce qu'il en est du piratage informatique, de la propagande sur Internet, des activités illégales comme la vente de drogue et tout ce qui est habituellement regroupé sous le vocable flou de « darknet ». Et vous apprendrez aussi que la plupart des activités cachées sont parfaitement honorables, voire admirables, mais doivent rester cachées pour préserver leur auteur (un dissident dans une dictature par exemple). Vous verrez aussi qu'une partie des activités cachées et moralement contestables sont effectuées, non pas par des gangsters, mais par des États, y compris des États qualifiés de « démocratiques ». Les révélations en mars 2017 de l'encyclopédie secrète du logiciel malveillant que tient la CIA (qui inclut des logiciels développés en interne) en sont un bon exemple.

La tâche était difficile, car le sujet se prête aux fantasmes et aux approximations. Les experts ont eu ainsi la stupeur de lire dans le n° 256, daté de décembre 2016, de la revue de la Gendarmerie nationale, qu'il existait un « Marianas Web », plus profond que le dark web et accessible uniquement à partir d'un « ordinateur quantique ». Il s'agissait à l'origine d'une farce d'étudiant, qui avait réalisé un article sur ce Marianas Web imaginaire. La farce, échappant à son créateur, avait été reprise dans certains médias, pour finir par apparaître dans la revue d'une organisation d'habitude plutôt sérieuse.

Comme la délinquance dans le monde extérieur à Internet, qui a une réalité (la délinquance existe) et une représentation (les films de gangsters...), les activités cachées sur l'Internet sont

difficiles à décrire. D'où l'abus de représentations graphiques pathétiques, où le hacker (russe, forcément russe) porte cagoule, capuche, gants et lunettes noires.

C'est pour cela qu'il fallait que ce livre soit rédigé par une experte, qui suit la « face cachée » depuis longtemps, en connaît les acteurs, peut faire la différence entre le fantasme et la réalité, et expliquer à tous de quoi il retourne. C'est ce que réussit très bien Rayna Stamboliyska.

Maintenant, un mot pour les gens qui me connaissent et qui lisent mon blog. Le plus amusant dans les abus du terme « darknet » est qu'il existait un darknet longtemps avant que les médias s'en emparent pour désigner quelque chose de sale et de dangereux. En fait, un darknet est un réseau qui n'émet rien, qui ne fait que recevoir, tout comme un télescope n'émet pas de lumière mais collecte celle émise par les étoiles. Ce terme est donc souvent cité dans la littérature scientifique. Un intense trafic (l'IBR, *Internet Background Radiation*) circule en permanence vers les darknets : logiciels à la recherche de victimes à pirater, erreurs de configuration, réponse à des messages dont l'adresse IP source était usurpée, abus de l'adresse 1.2.3.4 (le réseau 1.2.3.0/24 est le darknet qui reçoit le plus de trafic) lors de tests…

Un détail ? Oui, mais cela faisait longtemps que j'avais envie de rectifier cette erreur.

LES MYTHES D'INTERNET

POURQUOI CE LIVRE ?

Commencer un livre est difficile, bien plus que le terminer. Alors, plutôt que de nous perdre en généralités maladroites et verbeuses, je vous propose de plonger immédiatement dans le grand bain numérique.

Tout d'abord, merci à vous qui lisez d'avoir eu la curiosité d'ouvrir ce livre ! Celui-ci a pour but de démystifier des choses parfois terrifiantes, mais le plus souvent purement abstraites et qui, pense-t-on souvent, n'arrivent qu'aux autres. Internet a un rôle extrêmement important dans nos vies, mais sait-on ce qui se passe derrière ? De quoi parle-t-on lorsqu'on dit « piratage », « diffusion de logiciels vérolés », « attribution des attaques informatiques », « surveillance » ou encore « collecte de données personnelles » ? Est-ce que tous les criminels sont des hackers – et inversement, – et se cachent-ils tous aux tréfonds du « Darknet » ? Ce sont certaines des questions auxquelles nous tenterons de répondre ensemble.

Ce livre rejoint ainsi une série toujours plus riche d'ouvrages[1] que l'on peut définir comme étant d'intérêt général. Plus précisément, notre but sera d'explorer, de cartographier et de clarifier les actions et les acteurs de cet espace virtuel, mais si réel, qu'est

1 : Une sélection d'ouvrages sera tenue à jour sur le site web face-cachee-internet.fr

Internet. Comme chaque entreprise de cette envergure, nous avons fait de notre mieux pour avoir l'art et la manière. Nous espérons avoir tenu le pari de l'écriture honnête, riche et accessible. En parlant d'art et de manière, rappelons que la vulgarisation est un art difficile : il ne s'agit pas seulement de réduire la complexité de concepts et mécanismes d'action, mais aussi de ne pas prendre le lecteur pour un idiot en simplifiant à outrance.

Le but, disons sous-jacent, est de vous donner des outils critiques et des connaissances grâce auxquels vous serez capable d'améliorer votre hygiène numérique et de mieux appréhender les enjeux qui s'y rattachent. Pour y parvenir, nous sommes bien entourés : les 350 pages de ce livre contiennent ainsi des entretiens et éclairages d'experts, en France et au-delà. Le chapitre 03 est le seul où les entretiens sont absents : comme vous le verrez, sa nature est un peu particulière et de nombreux interlocuteurs approchés, qu'ils soient du côté obscur ou clair de la loi, ont refusé que leurs dires soient imprimés. Ce souhait a été respecté et les éclaircissements les plus pertinents ont été distillés dans le corps du texte. Enfin, ces entretiens vous changeront de la prose et de l'autodérision qui ne tardera pas à pointer ici et là : on peut très bien écrire des choses sérieuses, chez un éditeur tout à fait sérieux, sans pour autant se prendre (trop) au sérieux.

Faisons rapidement le tour de la structure du livre. Le sujet de *La Face cachée d'Internet* est très large, trop large, même pour 350 pages. Le cadrage final divise ainsi le présent ouvrage en trois grands axes thématiques. L'introduction (que vous êtes en train de lire) pose les jalons et déconstruit quelques mythes, tentant au passage de donner des éléments de réflexion utiles pour appréhender ces activités de l'ombre. Il est important de saisir que les variations de tonalité que l'on pourra découvrir dans les prochaines pages reflètent leurs développements : ainsi, si le ton est plutôt équilibré lorsque nous parlons des « hackers » russes qui auraient fait élire Donald Trump, il s'agit d'introduire la mesure et le recul nécessaires pour apprécier les incidences d'un tel évènement. De même, si vous

sentez un changement perceptible de ton entre les chapitres 02 et 03, c'est également logique : parler de l'effervescence qu'était Anonymous n'a rien de comparable à la cartographie tout en retenue du darkweb, pourtant sujet à toutes sortes de fantasmes plus ou moins ragoûtants. Si nous avons insisté sur ces variations, c'est également pour rendre la lecture plus vivante et moins intense que s'il s'agissait d'un document plus traditionnel.

Nous allons le voir tout au long de cet ouvrage, les choses ont changé, et ont énormément changé. Ce n'est pas surprenant : ces évolutions reflètent nos usages et notre rapport mouvant à la technologie. La manière unique dont nous hybridons notre cognition à nos machines et autres terminaux connectés appelle un traitement plus subtil de cette interaction que le simpliste « Internet, c'est plein de méchants ». Ainsi, la complexité des sujets dont nous parlons ne cesse d'augmenter et en faire un récit simplet serait non seulement irrespectueux mais probablement dangereux. En effet, à vouloir de plus en plus faire tenir des idées complexes en 140 caractères, on en vient à perdre de vue les détails, les subtilités et les implications de ce qui est dit. Plus encore, ne perdons pas de vue l'autonomie de réflexion et de (ré)action que nous perdons face à ces machines connectées : nous avons sous-traité nos doutes et questions à Google ; confié les photos de nos nouveau-nés et de nos chers défunts à Facebook, Twitter et Instagram ; le secret de nos échanges privés et professionnels sont à la merci d'un mot de passe. Si cette symbiose avec le numérique que nous avons développée est difficile, voire impossible, à endiguer, il convient justement de commencer à la considérer comme une interaction quotidienne et de la traiter comme telle. Pour beaucoup, encore aujourd'hui, le rapport au numérique et son impact sur nos lois et nos vies relèvent de l'extraordinaire, entraînant une négligence qui peut coûter cher. Le propos de ce livre est donc de faire de notre mieux pour expliciter les enjeux et les risques, dans une approche moins techniciste et plus globale, sans céder à l'anxiété souvent générée par le traitement maladroit de ce genre de sujets.

Le chapitre 01, intitulé *Le côté obscur de la force : piratages et malveillance connectée*, a pour objectif de clarifier le « quoi ». Il cherche ainsi à expliquer le pourquoi et le comment du « piratage ». Je plaide coupable : c'est parfois un peu technique et il n'y a pas d'images. Cependant, prenez-le comme une introduction générale ; il pose les bases des défis et questions qui nous occupent, rappelant toujours cette idée fixe de confiance à l'heure du numérique.

Ce chapitre a beaucoup évolué entre octobre 2016 et mars 2017, pour refléter non seulement les cas les plus récents et les plus pertinents mais également pour réduire l'ampleur de sujets assez moches (et éprouvants à aborder). Ainsi, plutôt que d'en faire un catalogue à la Prévert de la grosse majorité des types de logiciels malveillants, nous avons surtout tenté d'aborder ceux qui paraissent les plus parlants, les plus insidieux et les plus complexes à appréhender. Amis geeks, ne venez pas pinailler sur les détails ! Il y a eu un compromis à faire et la préférence a été donnée à un niveau de complexité moyen avec des entorses à la doxa technique au profit de la clarification des enjeux. Pour aller plus loin, n'hésitez pas à venir faire la chiffrofête.[2]

Le chapitre 02, intitulé *La figure du hacker : les bons, les brutes et les Anonymous*, porte sur le « qui ». En effet, il aborde, à travers une brève histoire du collectif Anonymous, les profils de certains de ceux et celles que l'on présente sous le visage sempiternel du personnage en capuche et gants de chantier sur fond de chiffres défilant comme dans le film *Matrix* (les gants de chantier ou de déménagement ne sont vraiment pas confortables pour taper sur le clavier…). Anonymous correspond à une époque particulière et il peut surprendre de les retrouver autant mis en exergue ici. Ce choix est fait justement parce que leurs agissements correspondent à une époque et à une évolution du rapport à la technologie

2 : « Cafés vie privée » où on apprend à sécuriser ses outils ; les références en format numérique sont accessibles sur le site web dédié : face-cachee-internet.fr

qui fait office, à nos yeux, de période charnière. Les usages techniques et les valeurs défendues ont commencé à fondamentalement changer et les acteurs ont commencé à complexifier leurs rapports. C'est également dans ce chapitre que nous aborderons le rôle de WikiLeaks, comme une sorte de chimère qui a traversé les différentes époques numériques oscillant entre hacking, activisme et influence politique.

Le chapitre 03, *Le darkweb, des mots et des maux*, se veut surtout une déconstruction du « où » que certains ont tendance à utiliser pour en parler. Au-delà de l'histoire de Bernard Debré qui, à l'été 2016, a découvert le « DARK NET !!! » et autres fantasmagories, ce dernier chapitre semble cristalliser les oppositions et tensions actuelles. La fuite en avant – vers toujours plus de contrôle, de surveillance et de restrictions – se retrouve bien illustrée dans cet écosystème où des communautés de passionnés côtoient des délinquants. Comme dans le cas d'Anonymous et WikiLeaks, nous avons essayé de décrire d'une manière accessible et plutôt complète des évolutions dont les tenants et aboutissants ne semblent pas exister en français. C'est également dans ce chapitre que nous parlerons de chiffrement, de respect de la loi et d'une pratique de la sécurité qui dépasse le seul élément technique pour toucher au quotidien. Cette discussion, qui prend pour illustration différentes manières de se faire prendre le doigt dans le pot de confiture numérique, conclut les recommandations distillées tout au long du livre. Ces conseils peuvent parfois paraître irréalistes, mais réfléchissez-y et ne les rejetez pas d'entrée comme « trop compliqués » : contactez des associations, l'auteure de ce livre, etc. si vous avez des questions.

La boucle est bouclée : ce livre n'a pas pour but de vous faire peur, mais il fera de vous un internaute plus autonome dans les usages, moins infantilisé dans les rapports avec les différents acteurs et plus éduqué quant aux enjeux du numérique. Plus libre, en somme.

Commençons par le commencement…

LA FIN DES MYTHES

Peu après le début de l'écriture de ce livre a eu lieu l'une des pannes les plus spectaculaire du web : l'attaque de la société américaine Dyn qui a mis à genoux pendant plusieurs heures des services tels que PayPal, Netflix et Twitter. On y reviendra. Si nous en parlons ici, c'est parce que cette attaque permet d'expliquer en quelques paragraphes ce qu'est Internet, comment ce bidule est apparu, comment il est structuré (techniquement).

Mythe n° 1

On sait avec précision qui a inventé l'Internet et quand.

Parfois, ce fameux inventeur est Al Gore[1]. D'autres fois, c'est un Français. Ou bien, c'est une innovation américaine. Et bon, on mélange « internet » et « web »,… Or, ce n'est pas la même chose.

Internet est un « réseau des réseaux », un tissu de connexions permettant à différentes machines d'échanger des informations entre elles et (souvent) à de grandes distances. La transmission de ces informations repose sur un ensemble de protocoles réseaux aux noms sibyllins tels que IP, TCP, UDP, FTP, etc. Le développement d'Internet a débuté dans les années cinquante. Le web (ou ce que l'on connaît sous le sigle www pour World Wide Web) est une application d'Internet, développée pendant les années quatre-vingt-dix. Si l'on poussait la définition d'Internet un peu plus loin, on peut même dire que l'idée en a été décrite dès les années trente. Paul Otlet[2], un Belge souhaitant créer un réseau international des bibliothèques pour faciliter l'échange de connaissances, publie un essai prémonitoire intitulé *Traité de documentation : le livre sur le livre, théorie et pratique*[3]. Il y décrit le réseau ainsi :

« Ici, la table de travail ne serait plus chargée d'aucun livre. À leur place se dresse un écran et à portée, un téléphone. Là-bas, au loin, dans un édifice immense, sont tous les livres et tous les renseignements.….De là, on fait apparaître sur l'écran la page à lire pour connaître la réponse aux questions posées par téléphone,

avec ou sans fil. […] Utopie aujourd'hui, parce qu'elle n'existe encore nulle part, mais elle pourrait bien devenir la réalité pourvu que se perfectionnent encore nos méthodes et notre instrumentation. »

Familier, n'est-ce pas ? Il faut bien sûr attendre les années soixante pour que naissent les premiers réseaux, développés par des agences de défense et des universités américaines. Le cœur du problème était un mécanisme appelé *packet switching,* que l'on peut traduire par « aiguillage » ou « commutation de paquets ». Les paquets, un peu comme des colis, transportent de l'information entre différentes machines. Un paquet a un en-tête, une adresse de destination et une adresse d'expédition, et l'information à transmettre. La question à plusieurs millions de dollars à l'époque était de trouver un moyen pour que les paquets issus de différents réseaux puissent être échangés et former ainsi un seul réseau de réseaux. Si on filait la métaphore postale, on chercherait comment faire pour aiguiller des colis qui proviennent de réseaux de distribution parallèles à la Poste.

En 1971 et de façon indépendante, un Français, Louis Pouzin[4], est responsable du projet Cyclades, au sein de ce que l'on connaît aujourd'hui sous le nom d'INRIA. C'est à Cyclades que l'on doit la notion de « datagramme », une transmission de paquets sans ordre particulier pendant la transmission, mais dont l'ordre est reconstruit à l'arrivée. Cette approche est très dynamique et flexible, mais également coûteuse. Même si Cyclades est arrêté en 1978, ses productions et réflexions ont inspiré des protocoles utilisés aujourd'hui, dans l'Internet que l'on connaît[3]. Bon, on parle de la France des années soixante-dix : le monopole de la Poste (anciennement PTT) et son pendant communications électroniques, France Télécom, y est incontestable. Parallèlement à Cyclades se développe Transpac, dont la stratégie est différente : transfert des

3 : Dans un article de 1998, *Libération* revient sur l'histoire de « la France [qui] ne créa pas Internet » : http://www.liberation.fr/ecrans/1998/03/27/et-la-france-ne-crea-pas-l-internet-cyclades-est-le-projet-francais-qui-aurait-pu-avoir-le-meme-succ_231404

paquets par lot, moins dynamique certes, mais également moins coûteux. Transpac est aussi le nom d'une filiale de France Télécom, laquelle développe le protocole X.25[4] largement exploité dans le… Minitel. Internet aurait donc pu être américain, français, même belge… ou encore, soviétique. L'idée de développer l'économie à travers des réseaux connectant des machines date des années soixante et plus précisément, d'octobre 1961 quand s'est tenu le XXII[e] Congrès du parti communiste. C'est lors de cet évènement que le livre *Cybernetics in the Service of Communism* est rendu public : on y explique comment les sciences cybernétiques contribueront à l'essor de l'URSS. En pleine guerre froide, ça n'a pas beaucoup rassuré les Américains[5]. Le scientifique soviétique principal, Viktor Glouchkov, a bénéficié du soutien de Krouchtchev… jusqu'à ce que ce dernier soit démis de ses fonctions au profit de Brejnev. Le projet de Glouchkov, appelé OGAS, rencontre de moins en moins de soutien. Dans un ouvrage récent, *How not to Network a Nation : The Uneasy History of the Soviet Internet,* l'auteur revient sur la difficile histoire de la (non) création d'un Internet par des chercheurs soviétiques. Alors que l'idée initiale de Glouchkov semble à l'abandon, les nouvelles des avancées américaines des années soixante-dix inquiètent l'establishment soviétique. Glouchkov est de retour, avec un projet encore plus ambitieux : la gestion économique et productiviste ; pour faire face à la menace américaine, il faut créer un système universel qui contient toute l'information disponible et permet de prendre des décisions rapidement. Pour Glouchkov, l'information est le pouvoir.

Alors que l'on peut avoir un peu froid dans le dos à l'idée d'un système national à la Big Brother, le design des interactions était tel que l'OGAS aurait été le premier internet décentralisé doté de capacité d'autorégulation. Mais l'« Internyet » l'a emporté :

4 : La personne responsable de son développement en parle probablement le mieux : http://remi.despres.free.fr/Home/X25-TPC.html .

Glouchkov n'a pas eu accès au portefeuille du Politburo pour réaliser ce projet comme il le proposait. Victime des machinations politiciennes de dignitaires soviétiques lorgnant tous le même portefeuille, l'OGAS a été adopté mais dénaturé ; ainsi, au lieu d'un système englobant les institutions et fonctions de l'État couvrant tout le territoire de l'URSS, le résultat fut un patchwork de systèmes. Autrement dit, chaque administration a adopté un réseau dédié, ses propres centres informatiques et ses systèmes automatisés de gestion. Des incompatibilités flagrantes de matériel et de logiciel entre les agences aidant, ce morcellement a posé les fondations techniques à un renforcement du contrôle institutionnel sur les entreprises subordonnées et a implémenté le fonctionnement en silos des administrations.

Donc, contrairement au mythe répandu sur l'inventeur d'Internet, cette technologie s'est en fait créée au fil des années, par le travail de longue haleine de chercheurs et scientifiques de différents pays.

La situation est similaire en ce qui concerne le web, cette application parmi d'autres d'Internet. Tout comme dans le cas de l'Internet, le mythe de l'inventeur génial qui s'est réveillé un jour avec l'idée de connecter plein d'ordinateurs fait insulte à notre intelligence. Sir Tim Berners-Lee, souvent cité comme l'inventeur du web, fait certes partie de l'équipe qui a travaillé à ce qui nous permet aujourd'hui d'avoir des sites web. Cependant, l'idée d'hypertexte comme un ensemble de documents contenant des unités d'information liées entre elles par des hyperliens est développée à la fin des années soixante. Ainsi, lorsque Berners-Lee commence à s'intéresser à cet aspect technologique en 1980, il existe déjà plusieurs programmes développant l'hypertexte et les langages à balises. Ces derniers sont les précurseurs de HTML, cocréé par Berners-Lee et Robert Cailliau lors de leur séjour au CERN, un langage que l'on utilise toujours et qui sert à formater des documents texte. Les technologies web ont énormément évolué depuis la publication du premier site web en 1990, mais vous avez compris où je veux en venir.

Mythe n° 2

L'Internet résiste à une attaque nucléaire.

Ce mythe a la peau dure, fait vraiment étonnant étant donné la dimension rocambolesque de cette idée. Ce genre de propos est tenu[6] par des personnes intelligentes en plus, tel le directeur sécurité des systèmes informatiques chez Salesforce, le géant des logiciels de suivi client. Les histoires, fleurant souvent le complotisme, y vont bon train : oui, c'est l'agence américaine de recherche sur la défense (la DARPA) qui a créé Internet, alors forcément il résiste à des attaques nucléaires ; Internet a été fait dans le but de résister à une attaque nucléaire ; etc. D'aucuns l'ont même donné en exemple d'infrastructure solide après les attaques terroristes du 11 septembre[7].

Le mythe prend naissance dans un rapport de prospective rédigé par l'informaticien Paul Baran, travaillant à l'époque pour le *think tank* RAND Corporation, et participant au développement de ce qui est devenu par la suite Internet. La RAND, comme on l'appelle familièrement, a été fondée par le département de la Défense américain et est depuis 1948 une institution indépendante mais gardant des liens très étroits avec le secteur public américain. Dans le cadre d'un contrat avec l'armée américaine pour la période 1962-1965, Paul Baran étudie la transmission par paquets et la résilience de systèmes de communication informatiques. La conclusion est qu'un réseau décentralisé de communication par paquets pourrait résister à une attaque (guerre froide oblige). Cette étude n'a rien à voir avec les recherches et expérimentations sur l'Internet[5]. Mais le mythe est né.

Mythe n° 3

L'Internet est contrôlé par sept clés.

Si vous avez lu *Le Seigneur des Anneaux*, écrit par J.R.R. Tolkien, ou vu le film qui en est tiré, vous savez qu'on doit à cette œuvre la phrase devenue mythique : « Un anneau pour les gouverner tous. »

5 : D'aucuns avancent également l'argument économique http://www.networkworld.com/article/2333635/lan-wan/-net-was-born-of-economic-necessity--not-fear.html

Visiblement, l'idée de vivre en une permanente fiction ne déplaît pas non plus : on a donc eu droit à un mythe qui perdure, à savoir que sept clés détenues par sept personnes contrôleraient Internet[8]. La manière dont ce contrôle serait détenu par quatorze personnes au sein de l'ICANN[9] (pour *Internet Corporation for Assigned Names and Numbers*, c'est-à-dire, la Société pour l'attribution des noms de domaine et des numéros sur Internet[10]) n'est pas très claire, mais l'idée est là. Ces gens auraient aussi leur fête secrète, « *un rituel ultrasécurisé baptisé "cérémonie de la clé"* » d'après Business Insider France[11], lors de laquelle les maîtres des clés « *du métaphorique verrou ultime d'Internet sont vérifiées et mises à jour* ». Pour peu, on s'imaginerait des gens en toges avec des masques vénitiens et des poulets sacrifiés tellement le champ sémantique décrivant ce « *rituel* » ressemble au fantasme de messe satanico-templiéro-francmaçonne.

Quelle vérité donc derrière cette cabale qui aurait le pouvoir absolu sur le réseau des réseaux ? Eh bien, autant pour un bouquin fantastique, c'est une bonne trame, autant pour la vraie vie, c'est du n'importe quoi. Comme précisé plus haut, il ne s'agit pas de faire un procès d'intention aux journalistes ayant commis ces énormités, mais d'expliquer ce qu'il en est vraiment. Et la réalité est finalement très prosaïque et aussi éloignée du film que l'on peut l'imaginer.

L'un des nombreux amalgames dans ce genre d'articles est la mauvaise compréhension de la gouvernance des infrastructures. Divers organismes existent. Citons notamment la célèbre ICANN et le moins célèbre IETF. L'ICANN a un rôle de coordination des acteurs techniques :

« L'ICANN est chargée de coordonner la gestion des éléments techniques du DNS pour assurer la "résolution universelle" ("universal resolvability"), de sorte que tous les internautes puissent trouver toutes les adresses valables. Pour ce faire, l'ICANN supervise la distribution des identificateurs techniques uniques utilisés

dans les opérations Internet et l'affectation des noms de domaine de premier niveau (tels que .com, .info, etc.).

Les autres questions concernant les internautes, telles que les règles relatives aux transactions financières, le contrôle du contenu sur Internet, les messages électroniques à caractère commercial non sollicités ("spam") et la protection des données n'entrent pas dans le cadre des responsabilités de coordination technique de l'ICANN. »

Assez loin de la cabale décrite plus tôt, quand même !

Quant à l'IETF (pour *Internet Engineering Task Force*, Groupe de travail d'ingénierie d'Internet[12]), il s'agit du collectif qui élabore les standards du réseau[6]. Encore moins cabalistique, l'IETF est ouvert à toute personne souhaitant se joindre au travail de standardisation (même si, étant donné la nature des activités, il vaut mieux avoir les tripes bien accrochées techniquement parlant).

Mais quel rapport avec les prétendus détenteurs des clés d'Internet ? Ces instances font tout simplement partie de l'ensemble assurant la gouvernance technique du réseau. Quant aux quatorze personnes de la cabale, la réalité plutôt austère du bidule appelé DNSSEC n'a rien d'un film hollywoodien. Pour comprendre, clarifions le DNS (Domain Name Server), une des bases d'Internet. Il s'agit d'un système de traduction de noms de domaines (exemple.com) en adresses IP[7] afin de les associer à une machine sur Internet. Ainsi, trouver l'adresse IP associée à un nom de domaine est ce que l'on appelle la « résolution DNS ». C'est elle qui permet à votre requête d'être orientée dans les tuyaux du réseau. On peut aussi

6 : Le plus souvent, les travaux de l'IETF sont rendus publics sous forme de RFC (Request for Comment). Il est impossible de laisser passer l'occasion : si vous vous demandez quel(s) livre(s) lire, ne cherchez pas plus, allez sur bortzmeyer.org où une quantité incroyable de RFC sont traduits et commentés en français, souvent de façon très accessible pour des gens non spécialistes.

7 : Les ordinateurs connectés à un réseau IP (Internet Protocole) possèdent une adresse IP. Ces dernières sont numériques afin d'être plus facilement traitées par une machine. En IPv4, elles sont représentées sous la forme « xxx.xxx.xxx.xxx », où « xxx » est un nombre variant entre 0 et 255 (en système décimal). En IPv6, les IP sont sous forme « xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx », où « x » représente un chiffre de la base hexadécimale.

y conserver des métadonnées, c'est-à-dire des données sur les données, concernant le domaine en question : le serveur e-mail, la lutte contre les spams, etc. Le système prévoit la délégation d'un nom de domaine à un autre serveur DNS et est hautement distribué pour assurer le fonctionnement du service[8]. Une façon de sécuriser les communications entre les tuyaux est apportée par le protocole DNSSEC[13]. Laissons la parole à Stéphane Bortzmeyer, l'une des personnes travaillant sur celui-ci et auteur de la préface :

« Résumé simplement, […] la technologie DNSSEC [est] un mécanisme technique et organisationnel qui permet de sécuriser une partie importante de l'infrastructure de l'internet, le système des noms de domaine. Sans DNSSEC, il est relativement facile à un craqueur de subvertir ce système en redirigeant un nom (mettons bortzmeyer.org qui sert au courrier que je reçois) ailleurs que ce que voulait le titulaire du nom. […] Une caractéristique importante de DNSSEC est qu'il est optionnel : aujourd'hui, seule une petite minorité des noms (bortzmeyer.org en fait partie) est protégée par DNSSEC et seule une minorité des utilisateurs se servent de serveurs de noms qui vérifient les signatures que DNSSEC appose. »[14]

Comme on le voit, parler d'Internet implique de bien distinguer différentes notions. Pas besoin de retenir tous les détails exposés ci-dessus, mais il est primordial de les avoir parcourus pour concevoir les fondements d'infrastructures, de protocoles, etc. inséparables d'exigences techniques et de leur gouvernance.

D'INTERNET À PEURNET ?

Nous connaissons maintenant mieux l'histoire d'Internet[9]. Nous savons comment il influence notre quotidien et notre horizon. Mais il ne fait pas que cela : il nourrit également nos peurs.

8 : On parle de serveurs racine, dont le nombre varie en fonction de la manière dont on les compte : http://www.bortzmeyer.org/combien-serveurs-racines.html
9 : Pour « une contre-histoire » d'Internet, voir le documentaire de Julien Goetz et Jean-Marc Manach pour ARTE : https://www.youtube.com/watch?v=FZaBj6xaLR0

Connaissez-vous Polybius ? Il s'agit d'un jeu d'arcade lancé avec de la petite monnaie, distribué dans l'État d'Oregon aux États-Unis vers 1980. On dit de ce jeu, psychédélique et abstrait, qu'il provoquerait des effets sur les perceptions, allant de l'insomnie à l'amnésie en passant par les hallucinations et les crises d'épilepsie. Des menus d'options cachées (mais pas introuvables) suggèrent que les successions de formes géométriques et les couleurs vives sont créées dans le but de générer ces effets psychoactifs chez les joueurs. Les données laissées par les joueurs sur les machines sont, dit-on, collectées chaque nuit par des agents du gouvernement américain (employés par la CIA) et envoyées pour analyses comportementales. La diffusion du jeu couvre en tout et pour tout deux semaines. Depuis sa disparition, les témoignages de joueurs affectés font persister l'ombre de la CIA et sa tentative de manipulation de l'esprit[15].

On en tremble, c'est horrible… sauf que le jeu Polybius n'a jamais existé. C'est juste une (bonne) histoire d'horreur et une légende urbaine à la longévité étonnante. On peut même trouver des captures d'écran montées en vidéos sur YouTube de gens ayant prétendument photographié de vraies séquences du jeu. Polybius est un tel phénomène de culture alternative que même un épisode des *Simpsons* daté de 2006 y fait allusion. Les histoires de jeux vidéo exerçant un contrôle sur la psyché des jeunes joueurs sont connues : outre Polybius, il y a l'histoire de la version « possédée » (un peu à l'instar de la jeune enfant du film *L'Exorciste*) de Mario 64 (1996) où des voix murmureraient en japonais par-dessus la musique.

On ignore qui a inventé ces mythes, et pourtant ils tournent et survivent à la logique et au bon sens. Ils ne touchent pas seulement les jeux mais aussi des programmes télé et autres créations audio-visuelles. Ce sont les *creepypasta,* une dérivation de l'argot *copy-pasta,* c'est-à-dire le fait de diffuser des bouts de textes en les copiant-collant (*copy-paste* en anglais) dans différents forums tels

que 4chan et Reddit (voir chapitres 02 et 03). Creepypasta est donc le nom collectif de ces bouts d'histoires d'horreur qu'on diffuse ainsi. C'est une création littéraire d'un genre un peu particulier[10], une sorte de fiction de la peur à la Stephen King mais réservée au monde numérique, où la réputation de l'auteur n'a pratiquement aucune valeur ; ce qui compte, c'est réussir la prouesse de faire peur et d'élever une histoire au rang de légende urbaine.

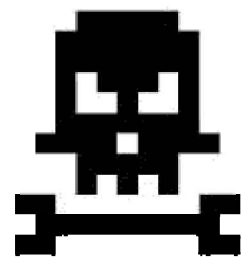
Vous vous demandez pourquoi aller de la technique à quelque chose *a priori* sans rapport ? Rappelons que ce livre explore la « face cachée ». Autant les tuyaux sont cachés par leur niveau de technicité, autant des actions qu'ils rendent (indirectement) possibles le sont également par leur motivation première. Les creepypastas sont un exemple éclatant de cette viralité de la peur à l'heure du numérique : c'est lorsque le moyen infecte le message qu'ils opèrent le mieux. Dans notre cas, on est plein dans la configuration où, si on pousse un peu, « Internet parle de lui-même ».

Et, si on y pense, l'horreur n'a pas besoin de sang ou de décomptes de cadavres pour faire effet. « *L'ambiance est primordiale car l'ultime critère d'authenticité n'est pas l'assemblage de l'intrigue mais la création d'un sentiment particulier* », écrivait l'un des maîtres de la science-fiction et du suspense, Howard Lovecraft. Le creepypasta est une sorte d'industrialisation de cette approche : l'effet du réseau amplifie d'une façon particulièrement intense une menace inconnue, l'obscurité pouvant surgir de n'importe où, y compris des agissements et outils les plus ordinaires.

Au-delà des histoires d'horreur (trop souvent vraiment nulles) copiées-collées sur des forums et autres « murs » Facebook, le cœur du creepypasta nous suivra tout au long de ce livre, des pièces

10 : Il y a un recueil de creepypastas, comptant plus de 10000 créations http://creepypasta.wikia.com/wiki/Creepypasta_Wiki Il y en a également une bonne collection sur Encyclopedia Dramatica.

jointes vérolées aux e-mails menteurs probablement envoyés par des Russes jusqu'aux inventions les plus modernes et les plus morbides, les Red Rooms du darkweb. Les menaces sont réelles : programmes informatiques capables d'infecter nos terminaux ; logiciel espion pouvant écouter nos enfants ou voler nos données privées ; attaquant pouvant passer outre notre pare-feu et compromettre notre site web professionnel, etc. J'aime à imaginer que vous, chers lecteurs, pardonnerez cette petite digression littéraire ; il faut dire qu'elle donne le fil rouge de ce livre : en comprenant ce qui nous fait peur, nous pouvons y faire face. En comprenant comment évolue un écosystème à la fois technique et nourri par une culture (parfois alternative) forte, on peut restaurer une confiance perdue.



01

LE CÔTÉ OBSCUR DE LA FORCE : PIRATAGES ET MALVEILLANCE CONNECTÉE

x x x

01

....

COMMENT SE FAIT-ON PIRATER ?

Le 21 octobre 2016, la société Dyn, gestionnaire d'infrastructures stratégiques d'Internet pour le compte de nombreuses entreprises, se retrouve sous le feu d'une attaque informatique. Parmi les entreprises clientes se trouvent Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, le *New York Times*. Les utilisateurs des services normalement fournis par ces sociétés rencontrent donc des interruptions sporadiques et de durées différentes desdits services. Petit à petit, il apparaît que l'attaque contre Dyn provenait de centaines de milliers de machines connectées à Internet de par le monde. Ces machines étaient aussi bien des ordinateurs que des caméras de surveillance, des grille-pains et des babyphones.

On se doute bien qu'un babyphone ne se lancera pas par magie à l'assaut d'infrastructures critiques. L'enquête préalable, qui a débuté alors que l'attaque battait son plein, a révélé que toutes ces machines[1] ont été infectées et détournées à l'insu de leurs propriétaires. Ainsi, les machines infectées ont été sous le contrôle d'attaquants *a priori* malveillants qui ont inondé Dyn avec des requêtes provoquant une des attaques DDoS les plus spectaculaires à ce jour.

DDoS est le sigle le plus connu de ce que l'on appelle un déni de service distribué (en anglais, *Distributed Denial of Service*).

.....

1 : Il s'agit du botnet Mirai, un réseau d'agents automatiques ou semi-automatiques connectés entre eux (les bots) exécutant certaines tâches.

En temps normal, un serveur reçoit une requête et y répond : si vous demandez à votre navigateur d'afficher la page d'accueil de twitter.com, la plupart du temps, il le fait sans problème. Les serveurs sont de plus en plus nombreux et puissants pour pouvoir répondre à un nombre important de requêtes. Dans le cas d'une attaque DDoS, il s'agit de saturer le serveur de requêtes qui semblent légitimes : il ne sait plus « où donner la tête ». Le service est alors interrompu ou répond de manière aléatoire. Du point de vue de l'utilisateur final, la page d'accueil de twitter.com ne se charge pas ou, au mieux, se charge très (très) lentement et/ou occasionnellement. C'est ce qu'il s'est passé dans le cas de l'attaque contre la société Dyn. Les infrastructures touchées servaient des entreprises tierces : le résultat visible par tous fut que de nombreux sites web ne répondaient plus.

Des médias ont relayé, parfois avec humour, que « quelqu'un avait cassé Internet ». Cependant, derrière cette plaisanterie, ce cas démontre l'importance de la sécurité informatique. Et celle-ci concerne autant les infrastructures techniques que leurs opérateurs et les informations transmises. Il est illusoire de vouloir vulgariser cette complexité en quelques pages. Néanmoins, examinons ensemble quelques cas récents qui ont défrayé la chronique.

DE PLUS EN PLUS CONNECTÉS, DE PLUS EN PLUS EN DANGER ?

Autrefois, dans les années 1960-1970, seuls les ordinateurs centraux étaient équipés de logiciels et seules quelques personnes interagissaient avec ces programmes. Avec l'invention et la démocratisation de l'ordinateur personnel, le logiciel s'est installé dans nos maisons. Peu après, Internet et le web se sont popularisés. Tous ces ordinateurs personnels se sont retrouvés connectés – ainsi que leurs logiciels respectifs. Aujourd'hui, il y a du logiciel littéralement partout.

Dans le passé, avant qu'Internet n'atteigne le grand public, attaquer le logiciel sur un ordinateur personnel non connecté était

difficile. En tout cas, dans le sens actuel de la notion d'attaque. Cela étant dit, le tout premier ver informatique, Creeper, date de 1971. Il s'agit du premier logiciel autoréplicatif : il se copiait lui-même. Le ver se propageait dans ARPANET, l'ancêtre d'Internet dont on a parlé dans l'introduction. Pour le contrer, les chercheurs ont créé Reaper. Creeper n'était pas ce que l'on a l'habitude de nommer un logiciel malveillant, son seul effet était d'afficher un message sur l'écran de l'ordinateur infecté : « *Je suis louche : attrape-moi si tu peux.* »[2] Par ailleurs, divers outils existaient permettant de copier et modifier des logiciels commerciaux. Ainsi, Discology[3] fut le premier logiciel contrefait pour ordinateurs Amstrad et permettait de copier des logiciels. Plus encore, Discology pouvait s'autocopier alors qu'il était protégé contre la copie… Bref, les gens n'ont pas attendu l'avènement d'Internet pour jouer avec les machines !

Une fois que tous les ordinateurs et leurs logiciels respectifs furent connectés, la tâche a été facilitée : on pouvait aussi avoir accès à la machine à distance. L'évolution des ordinateurs s'est poursuivie et, un jour, nous avons pu acheter des téléphones portables dont la puissance dépassait de plusieurs ordres de grandeur celle des ordinateurs ayant permis d'envoyer Apollo dans l'espace[4]. Enfin, nous avons eu des téléphones intelligents, véritables petits ordinateurs avec une connectivité sans fil. Aujourd'hui, même nos objets quotidiens sont parfois dotés d'une telle connectivité : frigos, podomètres, grille-pains, sous-bocks de cocktails, etc. Ceux-là, que l'on présente habituellement comme des objets « intelligents », sont eux aussi équipés de logiciels. La dénomination IoT (*Internet of Things* ou, en français, Internet des objets) résume ainsi la promesse de connecter tous les objets à Internet, caractéristique apparemment nécessaire et suffisante à l'amélioration de notre quotidien.

2 : *I am the creeper: catch me if you can.* https://www.theguardian.com/technology/2009/oct/23/internet-history et http://corewar.co.uk/creeper.htm
3 : http://www.cpcwiki.eu/index.php/Discology
4 : http://www.usinenouvelle.com/article/toute-la-puissance-informatique-de-la-mission-apollo-dans-une-seule-requete-google.N180825

On peut légitimement se demander si avoir nos télés, frigos et cadenas de vestiaire connectés à Internet est une bonne idée. Il y a quelques années, lorsque des start-ups cherchaient à commercialiser des objets connectés « impactant positivement notre quotidien », pour reprendre les éléments de langage utilisés, une création avait paru surprenante : la poubelle connectée. Cette poubelle devait, par son intelligence *(sic)*, pousser ses propriétaires à faire attention à leurs déchets. Dès qu'on jetait quelque chose dedans, la poubelle prenait une photo et la postait automatiquement sur votre profil Facebook. Ainsi, votre entourage pouvait-il vous gronder si vous étiez négligent quant au tri des déchets… Même si cette start-up ne semble pas avoir réussi, de nombreuses autres ont été créées depuis visant à mieux gérer les déchets en ville *via*, par exemple, des poubelles connectées dont le niveau de remplissage est connu à tout moment, épargnant ainsi des déplacements inutiles d'éboueurs. L'*Internet of Things* devient l'*Internet of Trash*[5]…

L'explosion du nombre de périphériques équipés de logiciels et dotés de connectivité sans fil semble certaine. Des estimations portent même le nombre de ces objets à 50 milliards en 2020. Les développeurs de logiciels sont sûrs d'avoir du boulot. Mais *quid* de la sécurité de ces logiciels et objets connectés ? De plus en plus souvent, les équipes de développement sont soumises à des calendriers irréalistes pour accélérer la mise en production de nouvelles fonctionnalités. En outre, on voit apparaître de plus en plus de langages de programmation et outils de développement, opérant le plus fréquemment dans un environnement en ligne et, qui plus est, souvent déployé sur le *cloud*. Ce dernier[6], appelé parfois en français « informatique dans les nuages », présente ses propres

5 : *Trash* : poubelle

6 : On entend souvent que le cloud, c'est l'ordinateur de quelqu'un d'autre. Les données qu'on y met, les nôtres ou celles d'une entreprise, sont de plus en plus dispersées et dépendantes de tiers. Ainsi, en plus des problèmes liés à la sécurisation d'une infrastructure toujours plus complexe, par le fournisseur du cloud, une question de gestion des données se pose : l'endroit où vous stockez ces données n'est pas à vous, il vous est loué. Et si le fournisseur de cet espace loué venait à disparaître ou être compromis ? Pensez-y, ce cas est plus fréquent qu'on ne le croit.

problématiques en matière de sécurité. Enfin, de nombreux programmes acceptent des plug-ins (greffons) et add-ons (modules supplémentaires), ce qui ajoute certainement des fonctionnalités mais présente autant de brèches en devenir. Nous sommes ainsi face à une situation où l'« à-peu-près » s'accumule et se propage plus vite que l'on peut le dire, et où les usages et les niveaux d'hygiène numérique varient grandement d'un individu et d'une entreprise à l'autre.

Donc, en combinant la connectivité des machines, leur complexité et l'extensibilité des logiciels qui les équipent, on obtient une vaste surface d'attaque. Le site web de la Base nationale des vulnérabilités (*National Vulnerability Database*), « nourri » et maintenu par un ensemble d'administrations américaines, présente d'ailleurs bien l'évolution des nombres et types de failles[1]. Il est évident que le problème est très complexe : un attaquant peut viser n'importe où tandis qu'un défenseur doit défendre partout. De nombreuses failles peuvent être détectées rapidement et relativement facilement, c'est pourquoi les analyses de sécurité doivent se faire souvent. Cela ne signifie pas que l'on est à l'abri et que le système est parfaitement sécurisé, mais il peut ainsi résister à de nombreuses attaques automatisées. Lorsque des failles sont détectées, elles ont (normalement) droit à un correctif (ou un *patch*) ; celui-ci peut être définitif, mettant ainsi fin à l'existence de la vulnérabilité, ou palliatif et la brèche est colmatée provisoirement le temps de créer un correctif définitif.

CHERCHER LA FAILLE

Théoriquement, aller à la chasse aux vulnérabilités est facile. En pratique, c'est une autre histoire. Il est d'ailleurs illusoire de s'imaginer que, puisqu'un logiciel ou un programme informatique est utilisé depuis longtemps, il est forcément sécurisé. Ces dernières années, nous avons eu de nombreuses mauvaises surprises émanant de programmes matures. Parlons brièvement de deux de ces (très

mauvaises) surprises pour tenter non seulement d'en apprendre davantage sur les dangers potentiels, mais également pour découvrir comment les acteurs concernés réagissent.

BEAST est une vulnérabilité côté client. En termes moins abscons, il s'agit d'une faille dans l'un des protocoles de communication web les plus répandus. Lorsque vous visitez des sites web et que la barre d'adresse affiche « Sécurisé » et/ou un petit cadenas, c'est que vous utilisez le HTTPS. Eh bien, le *S* de HTTPS indique la présence du protocole cryptographique dont on parle ici, nommé TLS/SSL[7]. En quelques mots, il permet de chiffrer l'envoi des identifiants et mot de passe ; si vous le faites en HTTP, ces informations sont envoyées en clair. Si quelqu'un « écoute » votre trafic, ces informations sont donc disponibles à l'interception comme sur un plateau. C'est ce que prévient le HTTPS. En outre, une navigation en HTTP est vulnérable à diverses interventions telles que l'injection de code malveillant. Vous conviendrez que le mieux quand on se connecte à sa banque, son profil de réseau social et son e-mail est d'utiliser HTTPS. Si votre banque ou fournisseur d'e-mail n'offre pas cette sécurité de base, mieux vaut en changer. Pour reprendre une métaphore plus quotidienne, « c'est comme un camion Brinks, ça permet de transporter des trucs qui sont dedans hors des yeux des gens ; c'est solide, mais sans être absolu et il faut donner sa confiance à ceux qui le conduisent. » Par opposition, utiliser HTTP reviendrait à utiliser un camion en verre, ou totalement découvert.

Revenons donc à BEAST (« bête », comme dans *La Belle et la Bête*, pas comme « stupide »). Découverte en 2011, cette brèche a causé des sueurs froides à bien des gens ; elle compromettait en effet la navigation de toute personne se servant d'un navigateur web (ça fait beaucoup !). En conséquence, on peut réaliser ce que

7 : TLS/SSL existe depuis 1994 et a été remanié plusieurs fois pour s'adapter à l'évolution des usages. La page Wikipédia en anglais est bien faite mais technique : https://en.wikipedia.org/wiki/Transport_Layer_Security

l'on appelle communément une attaque de l'homme du milieu (de l'anglais *man-in-the-middle attack* abrégé en MITM). Cette dernière décrit une situation où un attaquant se place entre le client et le serveur, en se faisant passer pour ce dernier[2]. La vulnérabilité BEAST permettait une attaque MITM en altérant l'étape d'initialisation du protocole cryptographique. Quels sont les conséquences d'une telle altération ? Sans entrer dans les détails techniques, l'attaquant peut ainsi deviner la façon dont est faite l'initialisation du chiffrement, comprendre à quoi ressemblent les données chiffrées et influencer la manière dont la suite de la sécurisation se déroule. Certes, si deviner n'est pas le plus efficace, il n'en reste pas moins vrai que les diverses informations de navigation que l'on génère sans le savoir peuvent être collectées ainsi. Cette faculté ajoutée à la capacité d'altérer le chiffrement faisait de BEAST un très gros problème.

Si la plupart des éditeurs de navigateurs ont rapidement colmaté la brèche, Apple a mis très longtemps pour appliquer et déployer les correctifs. En novembre 2013, soit deux ans après la découverte et la description de la faille, Apple a fini par corriger le problème sur le navigateur Safari qu'il édite[3], mais il a ainsi laissé ses utilisateurs vulnérables à de potentielles attaques[4] pendant deux ans…

L'autre brèche ayant certainement provoqué une dépression profonde chez de nombreux spécialistes est Heartbleed (littéralement, « saignement de cœur »). Annoncé en 2014 par la société Codenomicon[5], la faille était « *susceptible d'attaquer pas moins de 66 % de l'Internet* ». Encore une fois, il s'agit d'une vulnérabilité dans un protocole de sécurisation du trafic web. L'un des outils permettant le HTTPS est cette fois mis à mal. Heartbleed est encore plus dangereux que BEAST : il est possible, sans effort particulier, de récupérer non seulement des identifiants et mots de passe, mais aussi des e-mails, documents, archives de messagerie instantanée, etc.[6] Pire encore, cette faille ne nécessite pas la mise en place d'une attaque type MITM : l'attaquant peut accéder aux

informations directement. Celles-ci peuvent par ailleurs être utilisées par l'attaquant pour se faire passer pour un acteur légitime dans une attaque MITM ultérieure. Un véritable cauchemar.

Il est évident, d'après ces exemples, que parfois il ne faut pas avoir peur des seuls virus et autres logiciels vérolés… On ne le répétera jamais assez : veillez à toujours mettre à jour les logiciels que vous utilisez[8]. Outre les nouvelles fonctionnalités, ces mises à jour permettent également d'appliquer des correctifs de sécurité.

JOUR ZÉRO

La faille Heartbleed que nous venons d'évoquer est ce que l'on appelle une vulnérabilité 0day (*Zero Day* ou « Jour zéro »). Il s'agit d'une faille qui n'a fait l'objet d'aucune publication. Généralement, une telle vulnérabilité n'est connue ni par l'éditeur de la technologie concernée, ni par ses utilisateurs. Logiquement, étant inconnue avant le jour de sa mise en évidence ou son utilisation publique, une telle vulnérabilité n'a aucun correctif connu. Par conséquent, un produit présentant une telle faille ne bénéficie d'aucune protection, qu'elle soit palliative ou définitive.

Cette définition implique le champ sémantique de l'extrême gravité. Ce n'est pas toujours le cas. Une vulnérabilité 0day signifie juste que la faille n'a pas de correctif. Sa gravité dépend de l'importance des dégâts pouvant être occasionnés, et notamment de l'existence d'un *exploit*. Ce dernier désigne toute approche technique qui exploite cette faille, causant ainsi les effets néfastes sur le produit concerné et, *in fine*, sur ses utilisateurs. Ainsi, une vulnérabilité 0day n'a pas nécessairement des usages néfastes ou illicites : on citera l'exemple d'une telle faille utilisée par le FBI pour démanteler un énorme réseau pédopornographique qui opérait sur le darkweb[7].

8 : Il est également évident qu'il faut avoir des mots de passe forts contenant des caractères variés et changés fréquemment.

Heartbleed est une faille 0day liée au code d'une des composantes principales du protocole TLS/SSL. Comme mentionné, la vulnérabilité 0day se transforme en danger si un *exploit* est implementé. La finalité de ces *exploits* peut varier[8] : par exemple des virus 0day existent ; la composante « infection » de machines tierces de Mirai fonctionne comme un virus.

La gravité d'une faille 0day peut également être déterminée par le nombre potentiel de services en utilisation. Toucher à une caractéristique de la navigation web (*e.g.*, Heartbleed), ou au langage structurant une majorité de bases de données en opération[9] par exemple, peut avoir des conséquences très fâcheuses assez rapidement. *Bis repetita*, il ne faut pas perdre de vue qu'il peut se passer beaucoup de temps entre la publication d'une faille 0day et le déploiement des correctifs par les utilisateurs du produit concerné. Et la situation est encore plus critique quand on pense aux objets connectés : les mises à jour et correctifs de sécurité semblent appliqués de façon un peu aléatoire[10]…

On a mentionné la publication de 0day plusieurs fois : mais comment, au juste, se fait-elle ? Différents sites web[11] existent où l'on peut soumettre son analyse de vulnérabilité. Généralement, une équipe identifiée et considérée comme digne de confiance se charge d'examiner les informations. Les personnes qui trouvent des 0days sont souvent des chercheurs au sein d'universités ou d'entreprises de sécurité. Signaler le problème à l'éditeur de logiciel concerné ou à l'organisation qui supervise le protocole visé est donc un geste bienveillant.

Comme nous ne sommes pas au pays de Candy, les choses ne se passent pas toujours ainsi. En effet, il existe aussi des vendeurs de 0days : ceux-là vont soit vendre la description de la vulnérabilité au plus offrant, soit créer un *exploit* à vendre. Et c'est là où la situation se corse : le plus offrant peut être par exemple un gouvernement et pas l'éditeur du logiciel affecté par la vulnérabilité. Des cas sont

connus où une vulnérabilité 0day a été acquise à près d'un demi-million de dollars mais l'acheteur n'était pas l'éditeur du logiciel concerné[12]. Et l'acheteur ne communique pas nécessairement le descriptif de la faille à l'éditeur, lequel peut tout simplement ignorer que la 0day existe. L'acheteur peut donc être un gouvernement et effectuerait un tel achat pour créer un panel de vulnérabilités et empêcher d'autres de les exploiter. Le problème est que si l'on ne permet pas à l'éditeur du logiciel concerné de créer des correctifs, on ne colmate pas la brèche. Et il se peut tout à fait que cette dernière soit identifiée par quelqu'un d'autre. La situation est également problématique, même si des considérations quelque peu différentes s'appliquent, si l'acheteur est un acteur privé.

Que ce soit la faille elle-même ou son *exploit,* il s'agit donc d'une technologie qui peut être utilisée à des fins défensives, mais également militarisée ou, en tout cas, utilisée à des fins offensives. Un véritable marché existe pour ces failles, et ses tenants et aboutissants sont complexes.

Aussi, personne de réellement impliqué dans cette activité n'en parle vraiment. Les chercheurs ne les abordent pas tant que les vulnérabilités n'ont pas été vendues ou publiées ; les acheteurs potentiels ne les rendent pas publiques parce que cela les rendrait inopérantes. Il existe cependant des moyens d'en savoir davantage : des vendeurs repentis, des e-mails d'acheteurs fuités[13], des journalistes d'investigation spécialisés, etc. Regardons-y de plus près.

Les vulnérabilités 0day pouvant être à but défensif ou offensif, des acheteurs et intermédiaires très divers existent. Comme on le verra dans le chapitre 03, des vendeurs de 0days officient sur le darkweb. De nombreuses entreprises en achètent : celles qui éditent le logiciel en font partie et achètent ces failles pour corriger leur produit et ainsi maintenir la confiance de leurs utilisateurs. Mais des entreprises moins bienveillantes sont également à l'affût : on peut citer les 30 000 livres sterling payées pour la 0day dans Flash par Hacking Team[14], une société italienne qui vendait des

logiciels offensifs et de surveillance à divers gouvernements peu respectueux des principes démocratiques (on en reparlera plus bas) ; ou encore Zerodium qui offrait 1 million de dollars à l'équipe qui trouverait une 0day dans iOS, le système d'exploitation de l'iPhone[15]. N'oublions pas également la société française Vupen, et son contrat avec l'agence américaine de renseignement NSA pour l'identification et la vente de 0days[16].

LE JOUR D'APRÈS

On s'en doute, un déséquilibre existe dans cet écosystème, notamment parce que certains seront plus enclins à ajouter des zéros sur le chèque (façon de parler) que d'autres. En outre, vu la nature d'une vulnérabilité 0day, on doit ajouter à ce système déséquilibré et complexe la rareté de la faille. La chaîne logistique de ces failles implique donc des hiérarchies d'acteurs et des vendeurs divers dont le sérieux peut grandement varier[17]. Typiquement, les prix peuvent monter à un niveau tel que l'éditeur ne pourra pas se permettre d'acquérir la vulnérabilité de sa technologie[18]. D'autres encore peuvent adopter une approche différente : citons une récente faille 0day affectant les ordinateurs sous Linux et les téléphones sous Android. La société qui l'a identifiée avait également mis au point un *exploit*[19]. Il s'agit là d'une approche marketing assez curieuse consistant à se faire de la pub en communiquant sur des failles spectaculaires (alors que pendant ce temps les développeurs de la technologie concernée s'arrachent les cheveux pour corriger).

Le modèle d'affaires des 0days est donc assez atypique. Soulignons en outre que les États, clientèle particulière qui tient à une discrétion absolue pour ses transactions, peuvent contribuer malgré eux à faire monter les prix. Pire encore, en se réservant un usage exclusif à des fins non communiquées au public, les agences de renseignement ne contribuent pas à corriger les failles, ce qui laisse un grand nombre de gens vulnérables. La NSA est par exemple très critiquée pour avoir collecté et utilisé

des 0days[20] sans laisser la possibilité de les corriger[21]. Les entreprises qui font du *bug bounty*[9] peuvent, si on force le trait, être vues comme des intermédiaires de telles failles, souvent malgré elles. Cependant, comme la découverte de failles pour le compte de clients est le cœur du modèle d'affaires de telles entreprises, elles n'ont pas spécialement intérêt à ce que ce marché périclite. Bien sûr, il ne faut pas jeter le bébé avec l'hypothétique eau du bain : à l'heure actuelle, peu d'entreprises ont des canaux de remontée des failles, donc les entreprises de *bug bounty* peuvent être dans ce cas une bonne solution. La règle, qui tient du bon sens, est simple : n'ouvrez pas les portes à des gens qui fouilleront chaque recoin pour trouver des soucis sans être dans les starting-blocks pour les corriger[21].

On en arrive à la question, complexe, de la régulation légale de ces vulnérabilités et leur commerce. De nombreuses études scientifiques existent, portant notamment sur le statut légal de ces failles. Un problème est que la définition d'une 0day est vague ou tout simplement inopérante[23] : on ne peut définir l'usage d'un logiciel qu'après qu'il a été utilisé. Par ailleurs, une telle faille peut très bien être connue de personnes (physiques ou morales) autres que l'éditeur du logiciel qu'elle concerne. Du coup, on ne pourra pas facilement introduire de notion de responsabilité légale. Il y a aussi eu des débats proposant d'introduire des règles imposant la publication obligatoire de ces vulnérabilités. Une telle démarche poserait d'autres problèmes. Et encore faudrait-il que les gouvernements, des acheteurs potentiels de ces vulnérabilités, légifèrent sur la publication desdites failles dont ils sont souvent les usagers[10].

9 : Programme proposé par de nombreux sites web et développeurs de logiciels qui permet à des personnes de recevoir reconnaissance et compensation après avoir reporté des bugs (par exemple, ceux concernant des exploits et des vulnérabilités).
10 : En novembre 2016, le gouvernement néerlandais a officiellement autorisé ses forces de police à faire usage de 0days pour assurer *« la sécurité nationale »*. http://www.zdnet.com/article/dutch-police-get-ok-to-exploit-zero-days-so-will-that-just-mean-more-surveillance/

Un aspect complémentaire se cache dans les canaux de transfert des 0days : on peut en acheter sur certains marchés du darkweb, mais des intermédiaires plus nombreux existent sans se cacher et ce marché « gris » est beaucoup plus vaste. Enfin, comme peu d'informations vérifiées et sûres existent sur ces failles et leurs utilisations[11], il est difficile de trancher : doit-on réguler leur commerce ou le pénaliser ? Chercher des failles est ce que font les experts en sécurité pour le bien de tous. Pénaliser un pan de leur travail serait une énorme bourde[24]. Ainsi, tout accord ou texte législatif qui pointerait le bout de son nez devrait éventuellement s'orienter vers la responsabilité de l'acheteur et non pas chercher à pénaliser les vendeurs[12].

LES CYBERATTAQUES

La gestion des failles étant une affaire compliquée, comment qualifier alors une cyberattaque ? Ce mot, fourre-tout, s'il exagère largement la dangerosité de l'opération, renforce également l'effet « épée de Damoclès » des menaces. Comme nous l'évoquions, il faut être conscient des dangers mais tomber dans la psychose ne sert à rien. En (ab)usant du mot « cyberattaque », nous n'utilisons plus notre discernement et il devient très difficile d'appréhender la gravité réelle que le terme sous-tend[13].

11 : Oui, des collections d'*exploits* existent mais, par définition, elles contiennent les exploits que des gens ont voulu rendre publics. On ne peut pas se prononcer sur ce que l'on ne connaît pas (stocks de 0days par gouvernements, acteurs privés, etc.).

12 : En France, la loi pour une République numérique du 7 octobre 2016 instaure la possibilité de déclaration de « *faille ou vulnérabilité* » (qui ressemblent à des 0days, en tout cas les professionnels les perçoivent ainsi) à l'ANSSI. La formulation semble cependant un peu maladroite, et est perçue par certains comme contre-productive : déclarer la faille à l'ANSSI paraît ainsi prohiber le signalement de la même faille à la personne/l'organisation en charge du service impacté ; l'inverse semble vrai aussi. Un éclaircissement de la part de l'ANSSI serait bienvenu, mais au-delà de cette requête, on a là un exemple très concret de la difficulté de gérer ces cas. https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/

13 : Le problème majeur dans ces cas-là est précisément le manque d'information de confiance : le moins qu'on puisse dire c'est que les informations en français ne se bousculent pas dans les résultats de recherche sur Internet.

« Cyberattaque » est un terme générique pour parler de manœuvre offensive visant des systèmes informatiques. Alors que « cyber » fait référence à des systèmes ou moyens informatiques, c'est « attaque » qui donne le sens plus spécifique : il s'agit de tentative de détruire, modifier, rendre inopérant ou vulnérable le système. Une cyberattaque peut aussi faire référence à la prise de contrôle ou à l'usage non autorisé d'un système informatique. C'est effectivement vaste, alors que ce dont la sécurité se nourrit est la précision.

Ce que « cyberattaque » sous-entend un peu trop vaguement, c'est la tentative délibérée de détourner les protections déjà présentes. En revanche, la notion de « cyberattaque » n'évoque pas du tout le domaine de la sécurité physique. Or, comme on le verra à différents moments dans ce livre, et notamment dans le chapitre 03, la sécurité des opérations dépasse celle de l'outil. Et la négliger peut aboutir à l'apparition de faiblesses supplémentaires.

Les cyberattaques peuvent être motivées par de très nombreux facteurs. Ils vont de la tentative plus ou moins réussie de tester ses premiers scripts glanés sur le web jusqu'à la création d'outils complexes et puissants tels que Stuxnet[14]. Dans chaque cas, une valeur est associée à l'action – et une perte de valeur à celui qui la subit. Cela ne signifie pas pour autant que complexité et valeur soient proportionnelles : une attaque relativement facile à exécuter peut coûter très cher. Et le prix que l'on paie n'est pas nécessairement exprimé de façon sonnante et trébuchante. En effet, une entreprise peut se voir aussi bien compromise financièrement qu'aux yeux de la justice (voir par exemple le cas d'ACS:Law dans le chapitre 02), ou encore auprès de ses clients. Ce dernier cas est probablement le pire, car regagner la confiance perdue est probablement le plus

14 : Un puissant virus informatique créé par des agences du renseignement américaines et israéliennes ayant visé les installations nucléaires iraniennes. Il visait les systèmes de contrôle, entre autres, des éléments clés de centrifugeuses d'enrichissement d'uranium. Le virus aurait entraîné une dégradation de celles-ci et des explosions. Stuxnet est considéré comme la première cyberarme.

difficile. Ainsi, le prix d'une bonne sécurité n'est pas nécessairement celui d'un audit de sécurité des systèmes informatiques. Cette remarque vaut bien évidemment pour tous les acteurs concernés.

VULNÉRABLES ET CONSCIENTS DE L'ÊTRE

En 2017, à peu près tous les médias incluent des « actus » sur des problèmes de sécurité informatique dans leur couverture éditoriale. Il est appréciable de voir ces informations communiquées au plus grand nombre : la sécurité est affaire de tous. Même si, le plus souvent, le traitement médiatique de ces sujets est liminaire et flou (pour le dire poliment).

Cette réserve mise de côté, on observe que les intrusions et compromissions reflétées dans ces actus sont très nombreuses et de plus en plus complexes. L'élément monétaire y est de plus en plus présent également, mais surtout, le lien direct entre notre vie « hors ligne » et celle « en ligne » est tellement fort que les répercussions d'une cyberattaque peuvent être graves et réelles. Votre téléphone intelligent fait tout un tas de choses et permet accessoirement d'appeler ; il donne aussi votre emplacement même si vous avez désactivé la géolocalisation *via* un bouton dédié. Eh oui, vous pensez que la connexion au réseau téléphonique ou 4G se fait « automagiquement » ? Bien sûr que non : le téléphone se connecte aux antennes environnantes, transmettant ainsi des informations sur son emplacement, donc le vôtre. En outre, les applications que l'on y installe ont des listes de « permissions » que vous devez leur accorder en amont de l'installation. Ces « permissions » sont de plus en plus abusives. Par exemple, une application faisant de la photo vous demande l'accès en lecture et écriture à vos SMS ou à votre agenda : pour quoi faire ? On peut lui donner l'accès à la caméra et à un répertoire pour y stocker les photos effectuées, mais pas l'autorisation de faire le café à notre place. Ainsi, trop souvent, les demandes de beaucoup d'applications sont abusives. Cependant, on clique sur le petit bouton vert « Accepter », et on n'y pense plus.

On pourrait consacrer trois cents pages supplémentaires à la question des données personnelles et leur privatisation croissante par de nombreux et divers acteurs privés. Pour l'instant, concentrons-nous sur l'idée que nous sommes vulnérables et qu'au lieu de tomber dans la psychose ou de se détourner de ce fait, on ferait mieux d'y remédier du mieux qu'on peut. Le lien quasi intime entre le numérique et notre quotidien le requiert.

Se dire qu'on n'est pas concerné parce qu'on n'a pas de compte Facebook/comptejeuxvideos.com/rayer l'inutile revient à faire l'autruche : l'administration française souhaite collecter des données biométriques personnelles de tous ses citoyens pour « faciliter » la fabrication de pièces d'identité[25]. Or, des audits de la part d'institutions publiques sollicitées telles que l'ANSSI et la DINSIC concluent que le système envisagé pour la conservation de ces mêmes données ne donne pas les garanties nécessaires quant à la sécurité des systèmes en œuvre[26]. En moins verbeux et langue de bois : les 60 millions de citoyens français que l'on obligera à donner leurs données biométriques personnelles peuvent voir la base de données idoine compromise plutôt facilement[15]. Il en est de même avec les dossiers médicaux partagés à venir : il s'agit d'y stocker des données personnelles très sensibles, mais quelles seraient les conséquences d'un problème d'accès ou d'une compromission ?

ENTRE LA CHAISE ET LE CLAVIER

La sécurité informatique n'est pas seulement une question technique. La sécurité informatique exige surtout une approche multidisciplinaire où la compétence technique est requise mais où vous, l'utilisateur, n'avez pas besoin d'un diplôme d'ingénieur en la matière

15 : Comme le précise Marc Rees de NextInpact, le journaliste qui a le premier « levé le lapin » du fichier TES, des propositions de loi existent déjà pour élargir les usages dudit fichier. Par exemple, celle du député LR Éric Ciotti pouvant aboutir au croisement des fichiers avec « *les images de vidéosurveillance centralisées dans les centres de supervision urbaine* ». https://www.nextinpact.com/news/103670-des-deputes-lr-veulent-coupler-videoprotection-et-reconnaissance-faciale.htm Voir aussi https://www.slate.fr/story/138356/saga-generalisation-fichier-des-gens-honnetes

pour vous protéger d'une bonne partie des menaces. Ce qui nous ramène à la discussion fondamentale du modèle de menaces qui aide à savoir quels risques vous seriez plus susceptible de courir et quelles sont les approches les plus optimales pour les prévenir.

Tout cela a l'air un peu abstrait, alors soyons concrets :

- Vous êtes cadre sup' dans une équipe R&D (Recherche et développement). Vous prenez le TGV et travaillez sur un projet important. Pour être alerte, vous allez vous chercher un café au wagon-restaurant du train. Que faites-vous de votre ordinateur ? Faites-vous comme beaucoup de gens et laissez-vous votre ordinateur ouvert, voire avec une session ouverte et le document clairement visible aux autres voyageurs ? Situation à risques.

- Vous êtes du genre à ramener du boulot à la maison. Avez-vous une clé USB dédiée ? Si oui, est-elle chiffrée ? La gardez-vous bien rangée, loin des affaires semblables familiales (clés USB avec les photos de vacances, etc.) ? Si vous avez répondu « non » à au moins une de ces questions, on doit se parler sérieusement.

- Vous voyagez beaucoup et notamment avec l'ordinateur que votre entreprise vous fournit. Allez-vous dans des pays exigeant d'avoir accès aux informations stockées sur vos machines ? Avez-vous pensé à demander à votre service informatique de chiffrer l'ordinateur en question ? L'avez-vous déjà oublié quelque part (un café, un aéroport, une gare) ?

- Vous recevez beaucoup d'e-mails dans le cadre de votre travail ou de vos études. Cliquez-vous sur toutes les pièces jointes, même si elles ne viennent pas nécessairement de collaborateurs ou collègues que vous connaissez bien ?

- On peut évoquer la gestion du badge (notamment celui avec une puce RFID qui permet d'ouvrir les portes dans un bâtiment où l'accès au public n'est pas autorisé ou sur présentation d'une pièce d'identité seulement) ; la clé USB « perdue » que l'on ramasse et

met sur l'ordinateur pour voir à qui elle appartient ; les photos prises sur le lieu de travail et postées sur les médias sociaux où on peut voir vos collègues, des mots de passe sur post-it collés ici et là, etc.

On le voit bien : inutile de tomber dans des histoires angoissantes de grand complot mondial pour s'appercevoir que le facteur humain joue un rôle très important dans la sécurité informatique. Dans les pages suivantes, nous parlerons de plusieurs aspects significatifs incluant – mais pas seulement – la technique : *phishing* (ou hameçonnage), *ransomware* (ou rançongiciel) et ingénierie sociale. On prendra enfin le cas du prétendu « hacking » russe des élections américaines pour illustrer les difficultés se posant face à un enquêteur numérique. Avant de s'y attaquer cependant, parlons de ce qui est communément appelé un modèle de menaces.

MAX LA MENACE

Le facteur humain est donc important à prendre en compte. On ne le répétera jamais assez, la sécurité informatique est l'affaire de tous, aussi bien d'un point de vue professionnel que personnel. Si vous faites confiance à une plateforme ou un service et qu'il se retrouve compromis par une attaque, il est normal de lui retirer votre confiance. En outre, une plateforme ou un service qui n'a pas fait le nécessaire pour s'assurer que les données collectées sont protégées selon les règles de l'art porte une responsabilité légale. On ne va pas ici trop s'aventurer sur ce chemin, il est cependant important de se rappeler que de nombreuses plateformes et services web sont légalement domiciliés outre-Atlantique. Cette « délocalisation » de la responsabilité rend les choses d'autant plus difficiles et on peut parfois observer les forces de police françaises démunies devant le problème lorsque l'on va poser quelques questions au commissariat de quartier[16].

16 : Le cas de figure inversé est également à souligner : Google est actuellement aux prises avec la justice américaine. Un tribunal exige ainsi, suite à une demande du FBI, que l'entreprise récupère des données et messages Gmail stockés dans des serveurs situés dans un autre pays. https://www.nextinpact.com/news/103708-emails-stockes-a-etranger-geants-americains-cloud-se-liguent-autour-google.htm

Lorsque l'on évalue les risques encourus, on peut être plus ou moins paranoïaque. Mais plaçons-nous à un niveau relativement bas en termes de parano : si vous avez un compte Facebook, est-il lié à votre compte Gmail ou Yahoo! ou bien à un e-mail sur lequel vous avez entièrement la main ? Il est possible, d'expérience, de se faire enfermer hors de son projet. Reprendre le contrôle des comptes qu'on ne gère pas entièrement est mission impossible ; les « services de confiance » tels que Google et Twitter vous laissent démuni et dans l'incapacité de parler à un humain pour faire valoir la nature du problème. Le commissariat local vous explique qu'ils n'y peuvent rien, voire n'y comprennent rien[17]. On se retrouve ainsi enfermé dehors, à se heurter à des interfaces web plus ou moins interactives, tournant en boucle entre la FAQ (foire aux questions, littéralement « questions fréquemment posées ») et lesdites interfaces, sans que jamais une réponse ne soit donnée à notre requête ou demande de contact. Cette incapacité de l'utilisateur par la délégation de confiance à des acteurs sur lesquels on n'a aucune prise est dangereuse : elle infantilise et enferme. On parle ici d'une situation loin d'être anodine : lier ses comptes sur des plateformes sociales ou de services publics à des adresses e-mail sur lesquelles on n'a pas le contrôle total est un gros risque. Le niveau de criticité est également haut : on est laissé sans véritable recours si cela se produit. Diminuer autant que possible l'externalisation de services qui nous sont importants est donc une excellente approche pour contrecarrer ce danger. Félicitations, vous venez de faire une première évaluation de risques numériques !

ALLONS À LA PÊCHE

Si l'on regarde les attaques que l'on peut endurer, on peut les regrouper dans trois grandes catégories[18] :

17 : Il s'agit d'une classification un peu arbitraire Si vous rencontrez un problème, le mieux est de vous référer aux recours décrits par l'ANSSI https://www.ssi.gouv.fr/en-cas-dincident/

18 : Il s'agit d'une classification un peu arbitraire mais elle est plus accessible.

1. donner des informations sensibles à quelqu'un usurpant le rôle d'un service légitime (hameçonnage) ;

2. voir ses machines compromises par des logiciels vérolés ou perdre le contrôle sur ses données au profit d'un rançongiciel ;

3. souffrir une inaccessibilité ou interruption de service (*via* une attaque DDoS comme dans le cas Dyn par exemple). On parlera un peu de DDoS dans le chapitre 02, cette attaque ayant été une approche privilégiée de certains groupes de « hackers » se revendiquant des Anonymous.

Une fuite de données personnelles peut résulter d'attaques relevant de n'importe laquelle de ces catégories. Une attaque de *phishing* se déroule généralement comme suit : vous recevez un e-mail comme « nous avons constaté une activité inhabituelle sur votre compte, cliquez ici pour le sécuriser ». C'est ce que vous faites parce que rien de particulier dans la notification ne vous inquiète. Résultat des courses : vous avez transmis votre mot de passe actuel et opérant à celui qui est derrière le *phishing*. Il peut donc se connecter au service concerné avec vos identifiants et mots de passe. Si c'est un e-mail où arrivent les notifications des ventes privées de vêtements, ce n'est pas si grave ; si c'est un compte bancaire, le problème est significatif. D'ailleurs, profitons de cette discussion pour suggérer une reformulation dans les conseils de la Gendarmerie : de temps à autre, le compte Twitter officiel gazouille que nous devrions faire attention à des « *e-mails suspects* ». Le problème est qu'une telle formulation ne veut pas dire grand-chose, voire est trompeuse. En effet, les attaques de *phishing* sont de plus en plus sophistiquées et de moins en moins suspectes ! Il ne s'agit d'ailleurs pas seulement d'e-mails : faux services clients[27], faux concours Facebook, etc. sont pléthore et n'ont pas vraiment l'air suspect…[28]

Ici la faiblesse est clairement humaine. On se fait avoir parce qu'on estime qu'il est très compliqué pour un tiers de reproduire « la tête » d'une notification Gmail ou d'un compte

« Il ne faut pas se reposer sur les antivirus »

« Vxroot »

Consultant sécurité des systèmes dans un grand groupe français

RS : Peux-tu nous dire en quelques mots en quoi consiste ton travail d'expert en sécurité informatique ? C'est un peu abstrait pour toute personne qui ne connaît pas le métier.

V : Mon travail consiste à accompagner et conseiller tout type d'entreprise (privée, publique, etc.) afin d'identifier les vulnérabilités qui peuvent impacter leurs systèmes d'information et de les aider à les corriger en fournissant des recommandations.

RS : Souvent les gens estiment que le plus important à faire est avoir un bon mot de passe. Je crois cependant que les priorités diffèrent selon que l'on soit expert ou pas. Alors, du point de vue d'un expert infosec, quelles sont les précautions essentielles pour avoir une bonne hygiène numérique au quotidien ?

V : En plus d'avoir un mot de passe difficile à deviner, il faut veiller à changer ce mot de passe régulièrement. Généralement, chaque trimestre.

Mais cela ne suffit pas. Les hackers malveillants utilisent d'autres méthodes pour accéder aux systèmes informatiques sans avoir besoin de s'authentifier, et donc de connaître le mot de passe de leurs victimes. Ces méthodes peuvent reposer sur l'exploitation de certaines vulnérabilités présentes dans les versions non mises à jour des

logiciels qu'on utilise au quotidien (navigateurs web, clients messagerie, etc.). C'est pourquoi il faut penser à mettre à jour ses logiciels régulièrement.

Il existe également d'autres méthodes qui ont comme objectif de piéger les utilisateurs à travers des techniques plus complexes à mettre en œuvre mais qui reposent essentiellement sur leur naïveté. Les hackers malveillants envoient des e-mails aux victimes dans l'espoir que ces dernières réagiront soit en cliquant sur des liens intégrés dans ces e-mails, soit en téléchargeant les pièces jointes. Il s'agit en fait de liens vers des sites web malveillants qui vont permettre aux attaquants de récupérer ce qu'on appelle les cookies de sessions des utilisateurs. Ces cookies vont permettre aux attaquants de se connecter sur les sessions de leurs victimes et réaliser des actions à leur insu. Les fichiers envoyés par e-mail permettent, après exécution, de donner la main à un attaquant sur la machine de sa victime. Il pourra par la suite accéder au contenu du disque dur, activer la webcam, etc.

Il ne faut pas se reposer sur les antivirus, car généralement les attaquants développent des nouvelles méthodes pour les contourner. Il faut plutôt adopter les bons réflexes et ne pas faire confiance au contenu des e-mails inconnus ou même des e-mails qu'on reçoit de la part des personnes de confiance mais qui présentent un contenu anormal.

RS : Comment savoir si l'on peut faire confiance à un site marchand ? De très nombreuses arnaques existent, peut-on les prévenir ?

V : On ne peut pas. Idem, il faut avoir les bons réflexes et ne faire confiance qu'aux sites web des marques connues. Il faut surtout faire très attention aux offres qu'on reçoit par

e-mail par exemple. Il se peut qu'il s'agisse d'une arnaque envoyée par une personne malveillante qui vise à rediriger les victimes sur un faux site web marchand qui ressemble à celui de la marque affichée. L'objectif est d'avoir la confiance de l'utilisateur pour le piéger, le pousser à passer sa commande et surtout à fournir ses coordonnées bancaires qui seront utilisées par la suite par ces attaquants.

Il faut vérifier les adresses (les URL) des sites web qu'on visite avant de passer toute commande et surtout vérifier la présence du cadenas vert qui sert à nous « confirmer » que nous sommes sur le bon site web. Un dernier point par rapport à cela, je recommande d'éviter de passer des commandes quand on est connectés sur des points wifi publics. Des personnes malveillantes peuvent intercepter notre connexion et nous rediriger vers un faux site alors qu'on a tapé la bonne URL.

Twitter légitime, donc la communication que nous avons reçue ne peut qu'émaner du service légitime. C'est faux. Le *phishing* est l'un des services de compromission les moins chers et il peut rapporter gros. Copier l'habillage d'une marque (le *branding*) ? Élémentaire ![29] Il dépend donc de vous d'être vigilant. Le facteur humain, donc.

VENI VIDI (GROUPE) VINCI

C'est plus facile à dire qu'à faire : alors que dans le cas d'un e-mail frauduleux, on peut avoir le réflexe d'aller sur le site du service concerné et vérifier que la demande est légitime ou même remonter le message au service en question, des cas plus sophistiqués et élaborés existent. Prenons le récent canular à l'encontre de Vinci, le groupe de BTP, qui a fait chuter l'action Vinci de

18 % de manière fulgurante[30] (transformant au passage le canular en escroquerie). Déjà, précisons le vocabulaire : malgré les titres sensationnalistes et abondants, comme « Vinci victime d'un piratage », il s'agit bien d'un canular (ou hoax) visant l'entreprise et non pas d'une cyberattaque[19].

Le 22 novembre 2016, un message électronique est envoyé à quelques rédactions spécialisées en économie (Bloomberg, etc.)[31]. Le communiqué est très alarmant : le directeur financier du Groupe Vinci vient d'être licencié suite aux conclusions d'un audit interne ayant démontré des « *transferts irréguliers* ». Ces derniers sont censés s'être étalé sur la période fin 2015-début 2016. La perte associée, colossale, avoisine les 3,5 milliards d'euros. Le communiqué se clôt sur une déclaration du P.-D.G. du groupe Vinci, se disant « *très choqué* ». Aux alentours de 16 heures ce même 22 novembre, l'information est rendue publique. L'action Vinci perd 18 % en 7 minutes (!).

Sauf que… rien de tout cela n'était vrai. Les rédactions sont tombées dans le panneau, et ce dans le cadre d'une brillante attaque d'ingénierie sociale, appelée aussi « attaque par réflexion » : on vise Vinci *via* les journalistes qui sont les réflecteurs de l'attaque. Bien sûr, certains des journalistes ont appelé le numéro de téléphone indiqué en contact en fin d'e-mail et *quelqu'un* leur a répondu, confirmant la véracité des graves informations précédemment communiquées. Mieux encore : le nom de l'attaché de presse est correct. Il s'agissait vraiment du nom de l'employé qui s'occupe des relations presse du groupe. Comme cela a été révélé par la suite, le numéro était faux. Mais pire encore, l'adresse e-mail émettrice était fausse aussi. En effet, le message provient de l'adresse « contact.abonnement@vinci.group ». Or, une rapide recherche dans un moteur indique que le nom de domaine du groupe Vinci est « vincigroup.com », non pas « vinci.group ».

19 : Chercher « piratage vinci » dans un moteur de recherche vous en donnera un exemple…

Ainsi, si l'on ne peut pas facilement constater si un numéro appartient vraiment à la personne indiquée en contact, constater que l'adresse e-mail est louche est assez facile.

Pour aller un peu plus loin, on peut vérifier les informations d'enregistrement des noms de domaines (elles sont publiques[20]). Un service, whois, permet de le faire ; de nombreux sites web permettent d'obtenir les résultats d'une telle requête aussi simplement que si l'on interrogeait un moteur de recherche classique[21]. Reprenons notre exemple :

Caractéristiques	**vincigroup.com**	**vinci.group**
Date d'enregistrement	le 24 février 2000	le 7 novembre 2016
Responsable	Philippe Drevard (Rueil-Malmaison, France)	Thomas Moulaert (Anvers, Pays-Bas)
Gestion	Par une société spécialisée	Par le responsable

Déjà, la comparaison pointe une incohérence : une personne domiciliée au Pays-Bas s'occuperait du site du groupe Vinci ? Si l'on cherche des informations sur chacun de ces noms, Thomas Moulaert semble inconnu au bataillon tandis que Philippe Drevard est responsable des communications de Vinci et on trouve très vite des interviews dans le *Journal du Net* datant de 2001[22]. Entre un inconnu et une personne dont le passé professionnel est estampillé « groupe Vinci », il est plus raisonnable de croire le dernier.

20 : Il est possible de demander au gestionnaire du nom de domaine de masquer les informations nominatives. Même dans ce cas, la date d'enregistrement est visible. Ainsi, si le faux nom de domaine était enregistré sans que l'on puisse voir les informations nominatives, la comparaison aurait montré clairement les connexions de vincigroup.com avec le groupe Vinci et aurait suscité de la suspicion envers un nom de domaine géré par on ne sait qui.

21 : Et des gens le font. Voir par exemple ce petit article de Mashable sur l'actuel porte-parole de la Maison Blanche et tout ce que l'on peut apprendre à partir d'une simple requête whois http://mashable.com/2017/02/07/sean-spicer-who-is/

22 : http://www.journaldunet.com/0111/011128vinci.shtml

Enfin, le message envoyé aux rédactions contient un lien vers le prétendu communiqué en ligne. La page est un clone du site original de Vinci[23]. Voilà donc comment, en environ une minute et demie, on peut trouver un bon faisceau d'indices permettant d'émettre de sérieux doutes quant à la véracité des informations communiquées. Et il n'est même pas question des sommes censées être en jeu (3,5 milliards !), montants qui auraient dû mettre la puce à l'oreille et susciter un effort d'inquisition plus important.

FRAIS COMME DU POISSON POURRI

Parvenir à identifier des éléments douteux dans le cas que nous venons de voir ne requiert aucune compétence technique particulière, mais nécessite une culture générale : il est effectivement difficile d'utiliser des outils dont on ne soupçonne même pas l'existence. Si, dans le cas de Vinci, l'entreprise n'a perdu que peu d'argent, personne n'est à l'abri et les coûts peuvent être considérables. Ainsi par exemple, en 2011, le ministère des Finances a été victime d'une opération de *phishing* très sophistiquée qui a permis la fuite de très nombreux documents relatifs au G20 et la compromission de cent cinquante postes de travail[32] ; ou la PME BRM qui s'est retrouvée à transmettre 1,6 million d'euros à un cabinet juridique factice, escroquerie ayant entraîné le dépôt de bilan de la société et la perte de quarante et un emplois[24]. Dans tous ces cas, le facteur humain a joué un rôle prépondérant ; une approche de prévention purement technique n'y aurait probablement rien changé.

Ces escroqueries plus élaborées sont à différencier du *phishing* « simple », le plus souvent d'inspiration crapuleuse. On parle en effet de « *spearphishing* » (harponnage) dont la visée

23 : Le site n'est malheureusement plus disponible en ligne, ni dans le cache de Google, et n'a pas été archivé dans la Web Archive.
24 : http://www.courrierdelouest.fr/actualite/bressuire-brm-mobilier-plombee-par-une-importante-escroquerie-07-09-2015-234392

est plus inquiétante. Il s'agit d'une attaque ciblée[30] : eposant généralement sur une usurpation de l'identité de l'expéditeur ; l'utilisation d'ingénierie sociale en amont est donc nécessaire. L'attaque a usuellement pour objet l'accès à des informations confidentielles[25].

Le *phishing* coûte peu cher et peut toucher de très nombreuses personnes, sans notion préalable de cible. Prenons le cas assez classique de *phishing* : vous recevez un e-mail de la part du Trésor public vous disant que pour percevoir un remboursement de surplus d'impôts, vous devez fournir toutes les données de votre carte bancaire. Bon, déjà c'est original, n'est-ce pas, de devoir transmettre des données de paiement pour recevoir de l'argent… La cible n'est pas prédéfinie ici : parmi les centaines ou milliers de personnes ayant reçu un tel message, quelques-unes se feront avoir. Le *spearphishing* diffère de cette approche en ce qu'il cible une personne ou un groupe restreint sur qui des informations très précises sont collectées en amont de toute attaque. Si quelqu'un souhaite avoir accès aux systèmes informatiques d'une entreprise, il ne ciblera pas tous les employés. Or ceux qui sont potentiellement en possession des mots de passe administrateur sont très paranoïaques (au sens prudents, précautionneux). Il faut donc disposer d'informations très spécifiques pour vaincre une telle méfiance. Là où le *phishing* est une approche grossière de pêche au chalut, le *spearphishing* consiste à l'élaboration d'une stratégie ingénieuse. Les enjeux peuvent également différer : les 150 euros sur le compte courant de tout un chacun n'ont pas le même intérêt que les rapports internes d'une société commercialisant des drones.

25 : De manière abusive, les attaques sophistiquées d'espionnage industriel ou autre sont appelées du « *phishing* » alors qu'elles relèvent plutôt du *spearphishing* . Voir les descriptions plus détaillées de l'ANSSI: https://www.ssi.gouv.fr/particulier/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/ et https://www.ssi.gouv.fr/particulier/principales-menaces/espionnage/attaque-par-hameconnage-cible-spearfishing/

ENFERMÉS DEHORS

Le facteur humain joue également un rôle important dans les cas d'attaque par *ransomware* (parfois appelé « rançongiciel » en français). Ce dernier est un logiciel malveillant qui « ferme à clé » l'ordinateur sur lequel il s'est installé et chiffre les données qui s'y trouvent. Son opérateur demande généralement une rançon (d'où le nom) pour déverrouiller le tout. La demande peut par exemple jouer sur le stress causé par une course contre la montre : si vous êtes un peu trop lent, vous dépasserez la date butoir et donc, vous ne reverrez plus vos données. Le *ransomware* Jigsaw promet même de procéder à l'effacement d'une certaine quantité de données toutes les heures[34]. L'approche est logique, à vrai dire : plus vous êtes stressé, moins vous agissez de façon rationnelle, donc moins vous avez le réflexe de demander un coup de main ou d'évaluer la situation et de prendre une décision différente que « OK, je vais payer tout de suite ».

Dans d'autres cas, le *ransomware* peut prétendre être une intervention des forces de l'ordre et/ou de justice : par exemple, après avoir infecté la machine, le rançongiciel Reveton affiche une image avec plein de logos ressemblant à ceux du FBI. Le message est clair : payer immédiatement 250 dollars d'amende pour avoir fait un usage prétendument illicite de contenus sous droits d'auteur ou courir le risque de se voir infliger une amende beaucoup plus importante (aux États-Unis, celle-ci peut monter jusqu'à 250 000 dollars et se voir doublée d'une peine de prison maximale de cinq ans)[35]. Du coup, 250 dollars, ce n'est rien du tout et les gens paient. Une variante implique un message signifiant que des contenus pédopornographiques ont été identifiés sur votre machine[36] (plutôt qu'une copie de Harry Potter téléchargée *via* streaming.xyz).

D'autres techniques, plus sociales disons, sont également employées. Vous souvenez-vous des PowerPoint qui circulaient il y a quelques années contenant des messages sirupeux et pseudo-spirituels sur fond de musique niaise que vous deviez transmettre

à trois amis sous peine de souffrir trois ans d'amour malheureux ? Des *ransomwares* ont repris l'idée, comme l'illustre Popcorn Time[37]. Vous avez un choix cornélien à faire : infecter des personnes de votre entourage en leur transmettant une pièce jointe vérolée ou bien payer pour n'infecter personne. L'approche n'est pas bête, à vrai dire : quelle que soit l'option choisie, l'attaquant a de fortes chances d'être payé, ce qui est tout de même son but principal. Assez sympathiquement, il y en a qui s'intéressent à l'amélioration des connaissances d'un plus large public, c'est ainsi qu'on peut tomber sur le *ransomware* Koolova qui ne vous laisse pas déverrouiller votre machine tant que vous n'avez pas lu les articles sur la sécurité numérique que le rançongiciel vous propose…[38] Cependant, cette approche ne signifie pas pour autant qu'il n'efface pas vos données si vous traînassez.

D'autres *ransomwares* sont tout simplement faux : ils requièrent qu'on paie, mais n'ont pas pour autant verrouillé la machine. Si ceux-là ne sont pas si dangereux, il y en a d'autres qui représentent un danger de nature différente : leurs opérateurs menacent de rendre publiques les informations trouvées sur votre ordinateur. Le danger devient autrement plus grave dans ce cas. En effet, comme vous avez une sauvegarde de vos données (vous en avez une, n'est-ce pas ?), faire une restauration si l'attaquant efface vos données est assez trivial. Déplaisant certes, mais facile. Si vos données sensibles et personnelles sont rendues publiques, c'est un autre problème...

INGÉNIERIE SOCIALE ET RANÇONS : QUEL RAPPORT ?

Nous avons beaucoup parlé de *phishing*. Ce n'est pas un hasard : la première source d'infection avec un rançongiciel est l'e-mail et notamment les e-mails de *phishing*. Ces derniers ont un taux d'ouverture de 30 %, donc environ trois personnes sur dix ouvriront un e-mail mensonger et potentiellement dangereux[39].

Au moins 90 % des e-mails de *phishing* envoyés en 2016 transportaient un *ransomware*.[40] Ce dernier est soit une pièce jointe vérolée, soit un lien vers un site web infecté. Dans le premier cas, des macros vérolés ont été identifiés comme étant à l'origine de la propagation de certains *ransomwares*[41]. Dans le cas d'infection *via* sites web, il ne s'agit pas seulement de ne pas visiter des sites un peu louches : des publicités vérolées ont par exemple été identifiées sur de nombreux sites respectés (par exemple, celui de la BBC) et ont pu ainsi se propager chez les visiteurs[42].

Vous avez probablement tiré les conclusions qui s'imposent jusque-là : faire attention aux e-mails reçus, ne pas cliquer partout[26], désactiver les macros par défaut, installer et activer un bloqueur de publicités (par exemple, uBlock[27]), toujours installer les mises à jour de son navigateur et éviter l'utilisation de technologies obsolètes et réputées peu fiables (par exemple, Adobe Flash). De nombreux rançongiciels vous laissent accéder de nouveaux à vos données, mais emportent des souvenirs, notamment des adresses e-mail – pour les utiliser pour l'envoi de spams ou pour un *phishing* par la suite – ou récupèrent les identifiants et mots de passe enregistrés, ou « recrutent » votre ordinateur, surtout sous Windows, pour faire partie d'un *botnet*[28]. Il est ainsi recommandé de bien séparer les sessions utilisées sur l'ordinateur. Sur Windows, c'est par défaut une session pour vous seul avec les permissions d'administrateur (vous pouvez administrer la machine, que vous sachiez ou pas le faire). Il vaut encore mieux créer une autre session que vous utilisez dans votre quotidien qui n'a pas ces permissions. Le but étant de prévenir qu'une infection ne se transforme en désastre.

26 : Vous pouvez utiliser l'outil du site de référence Virus Total pour vérifier qu'un nom de domaine est propre : https://virustotal.com/

27 : AdBlock Plus était la solution privilégiée jusqu'il y a peu. Cependant, leur politique de blocage a changé : l'entreprise qui édite le logiciel s'est lancée dans... la vente de publicités. http://www.lemonde.fr/pixels/article/2016/09/14/ le-bloqueur-de-publicite-adblock-plus-va-vendre-des-publicites_4997359_4408996. html

28 : Réseaux de machines infectées utilisées à l'insu de leurs propriétaires, en général pour des usages malveillants (envoi de spam, virus informatiques). Mirai, dont nous avons parlé plus haut, est le botnet responsable de l'attaque contre la société Dyn.

VULNÉRABLES CERTES, MAIS VIGILANTS

Ces réflexions nous ramènent au propos de départ : évaluer les menaces permet d'être vigilant et de mieux se protéger. La sécurité absolue n'existe pas, quel que soit le domaine, mais ce n'est pas parce que la probabilité de se casser la jambe existe que cela arrive obligatoirement. Citons quelques approches formalisées de la prévention des risques informatiques (dont vous pouvez vous inspirer dans votre utilisation quotidienne).

STRIDE

Acronyme de *Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege*. En français simple, il s'agit d'évaluer les vulnérabilités permettant une prise de contrôle abusive (et potentiellement illégale) du système. Cette intrusion peut survenir en utilisant les informations de connexion d'un des utilisateurs : c'est le *spoofing*. C'est un exemple de cas suggéré plus haut dans notre explication du *spearphishing*. Une fois dans le système, l'intrus peut altérer des données qui sont par nécessité sauvegardées à long terme ; c'est l'étape *tampering*. Parmi ces données, citons par exemple les logs d'activité : le système « note » chaque connexion, chaque opération, etc. Pour couvrir ses traces (l'étape *repudiation*), un attaquant peut ainsi effacer ce qui reflète son activité. La collecte d'informations et leur publication subséquente peuvent être un but pour l'intrus au même titre que le déni de service (*denial of service*). Dans ce dernier cas, le système n'assure plus le service que l'on attend de lui. Enfin, l'intrus peut s'arroger les permissions administrateur (c'est le cas *elevation of privilege*) court-circuitant ainsi les gestionnaires légitimes des machines et prenant abusivement le contrôle de leur fonctionnement. D'autres modèles de prévention des risques existent, basés cette fois sur une priorisation des risques en fonction de leur criticité.

DREAD

Acronyme pour *Damage, Reproducibility, Exploitability, Affected users, Discoverability* . Chaque mot est une caractéristique pouvant être appliquée à une compromission ou une attaque. Ainsi, quel est le dommage causé ? Ou encore, est-il facile pour un autre attaquant de reproduire l'attaque ? Combien d'utilisateurs sont affectés par une telle compromission ? Avec quelle facilité et au bout de combien de temps l'attaque a-t-elle été découverte ? D'après ce modèle, une échelle de 0 à 10 – où 0 est « insignifiant » et 10 « critique » – est utilisée, pour chaque catégorie et pour chaque menace. Même si votre approche quotidienne n'est probablement pas aussi consciente, elle n'en reste pas moins méthodique : le dommage causé par la consommation d'aliments avariés peut grandement varier selon que c'est vous ou un enfant de moins de 3 ans qui les a mangés. Du coup, vous ne risquez pas de recommencer (la probabilité de reproductibilité d'une telle situation est donc de 0).

Si nous insistons lourdement sur la nécessité de prendre du recul, c'est aussi parce qu'il faut comprendre qu'une attaque peut se manifester de nombreuses façons et amène souvent à se poser beaucoup de questions dont la majorité restera sans réponse. Décortiquons ensemble la complexité des menaces, de leur attribution et de leurs conséquences à travers un exemple qui a fait couler beaucoup d'encre (et de pixels).

LES RUSSES ONT-ILS VRAIMENT PIRATÉ L'ÉLECTION AMÉRICAINE ?

42. C'est la réponse à la grande question sur la vie, l'univers et le reste[29]. Aussi devrait-elle bien convenir à cette question russo-américaine…

29: Dans l'œuvre de science-fiction de Douglas Adams, *Le Guide du voyageur galactique*, il s'agit de la question ultime sur le sens de la vie. Une réponse est proposée : le nombre 42, mais le problème est que personne n'a jamais su la question précise…

Lors des élections américaines de 2016, des groupes de « cybermalveillants »[30] auraient fait de leur mieux pour s'introduire dans les boîtes e-mail du parti Démocrate aux États-Unis. Ces « cybermalveillants » seraient téléguidés par le Kremlin et son impérieux maître, Vladimir Poutine. Ce dernier, ayant prétendument développé une affection pour Donald Trump, se serait donc donné les moyens de jeter le discrédit et l'opprobre sur Mme Clinton, la candidate du parti Démocrate à l'élection présidentielle. Grâce à l'intervention de ces « cybermalveillants » sous le commandement poutinien, les e-mails fuités du parti Démocrate et de la campagne de Clinton auraient significativement contribué à faire élire l'actuel président américain, Donald Trump, surnommé avec un certain humour « Agent Orange » par certains de ses détracteurs.

L'utilisation du conditionnel est intentionnelle : rien dans les documents révélés jusqu'à présent (début février 2017) ne permet d'affirmer une telle chaîne de causalités. On sait quelque chose avec certitude : on n'est sûr de rien dans cette affaire. Il y a d'une part des intérêts géopolitiques très complexes en jeu, que l'on peut tenter de deviner. D'autre part, des cadres de lecture trop calqués sur ceux de la guerre froide s'imposent sans que l'on se demande s'ils sont toujours pertinents en 2017. Enfin, il ne faut pas perdre de vue que les informations principales sont publiées lors de périodes troublées et de tensions géopolitiques, environnement guère propice à un traitement de l'information dépassionné et le moins instrumentalisé possible. La polarisation de la sphère politique est immense, aussi bien en décembre 2016, lorsque l'idée d'un piratage russe a pris vraiment beaucoup d'importance, qu'en février 2017 soit juste quelques semaines après l'entrée en fonction du très controversé président Trump. Des théories du complot (très bien documentées

30 : L'utilisation de ce mot et des guillemets ici indique qu'il est difficile de qualifier les attaquants dans ce cas. Comme nous l'avons dit plus tôt, « cyber » est utilisé à toutes les sauces : son utilisation reprend une façon concise de nommer les attaquants ayant fait usage d'outils numériques.

avec des sites louches qui se citent entre eux et se référencent les uns les autres pour donner l'impression de volume) circulent également. Ils se résument au stratagème suivant : des hackers ultranationalistes ukrainiens ont procédé à ces attaques pour que les États-Unis blâment la Russie. Des Ukrainiens animés d'une profonde détestation de la Russie se donneraient tout ce mal pour faire élire celui qui est donné comme le favori de Poutine, pour jeter l'opprobre sur la Russie ? La logique est un peu… floue.

Pour ne rien arranger à cette ambiance de complotisme aigu, les arguments techniques disponibles ne sont quasiment jamais évoqués dans le traitement de l'affaire par les différents protagonistes[31]. Laissons donc de côté les considérations politiques et concentrons-nous sur les éléments connus pour tenter de délimiter le probable, le possible et le spéculatif[43].

1/ Est-on sûr et certain que la Russie a « hacké » les États-Unis ? Autrement dit, a-t-on à notre disposition des faits tangibles, concrets et sourcés permettant de dresser un tel constat avec un degré de *plausibilité acceptable* ?

2/ Est-on sûr et certain que ces « hackings » ont véritablement changé le cours de l'histoire et ont infléchi les décisions des électeurs américains ? Autrement dit, a-t-on à notre disposition de quoi décrire et soutenir une *causalité plausible* ?

RUSSIE/ÉTATS-UNIS : REVENONS-EN AUX FAITS

L'histoire commence par les attaques ayant finalement mené à la fuite des e-mails du parti Démocrate (le #DNCleak) et à ceux de divers membres du premier cercle de la campagne de Hillary Clinton (voir chapitre 02). Il est très étonnant de se rendre compte que personne dans ce parti n'a pensé à porter une attention parti-

29 : Nous utiliserons, malgré les réserves, ce cas comme point de discussion principal, car sa complexité permet d'apprécier les difficultés rencontrées par les enquêteurs numériques dans le cadre d'un grand nombre d'accidents.

culière aux divers systèmes informatiques. On était quand même en pleine bataille pour la présidence américaine, la moindre des choses aurait été de s'attendre à de nombreuses tentatives de compromission. Par ailleurs, les Démocrates n'étaient pas les seuls visés en juin 2016, le FBI avait déjà prévenu la branche du parti Républicain en Illinois que des compromissions avaient été probablement tentées[44]. De quoi mettre la puce à l'oreille.

Côté russe, on est face à des miettes laissées par plusieurs Petits Poucet. La Russie a une tradition connue, et datant de peu après la chute du Mur de Berlin, de recrutement d'experts désœuvrés pour contribuer aux opérations de ses services de sécurité. Dans les années quatre-vingt-dix, les activités comprenaient par exemple la collecte de *kompromat*, soit de matériels pouvant servir à compromettre la réputation de quelque figure publique (ébats avec des prostituées filmés sans que le client soit au courant, etc.) ou encore l'infiltration dans les milieux de fraude financière en ligne. Souvent ces personnes sont des « pots de miel » attirant ainsi des experts et hackers qui ne soupçonnent rien vers des activités ouvrant à des recrutements par les services de renseignements russes. Un « hacker » peut toujours faire ses petites affaires de son côté, s'il se fait prendre, le gouvernement peut également lui proposer un arrangement : soit un pénitencier peu accueillant en Sibérie, soit une petite collaboration. Il y en a qui sont très frileux, alors ils choisissent la collaboration[45]. Divers pays ont cette approche. Pour ne pas alourdir inutilement le récit, disons seulement que des investigations par ThreatConnect[46] ont montré que la marque de certains « hackers » repentis ayant rejoint les services secrets a été identifiée dans quelques attaques assez louches en Allemagne, Turquie, Ukraine et dans celle contre le parti Démocrate en 2016. Cependant, il n'est pas clairement identifié que ces trouvailles pointent les véritables coupables ou seulement des intermédiaires utilisés plus ou moins à leur insu[47].

Retraçons donc les différentes étapes et les tentatives d'attribution des attaques pour tenter d'y voir plus clair. Le FBI avait déjà prévenu le parti Démocrate de tentatives d'intrusion

en novembre 2015[48]. Une campagne de *spearphishing* avait été détectée et analysé par SecureWorks[49], la branche sécurité du constructeur informatique Dell. D'après leurs conclusions, le *spearphishing* s'est étendu sur la période mars-avril 2016. C'est ce rapport qui attribue, avec une « *confiance modérée* » et pour la première fois, les attaques à un groupe, nommé APT28 ou Fancy Bear[32]. Ce groupe opérerait, selon le rapport, pour les services de renseignement russes.

WINNIE L'OURSON A GRANDI (ET BIEN CHANGÉ)

En mai 2016, le parti Démocrate s'est enfin résolu à impliquer des spécialistes externes. C'est la société CrowdStrike qui est appelée à la rescousse pour assurer la réponse à incident et l'investigation numérique. En juin 2016, CrowdStrike publie donc un rapport identifiant deux attaques distinctes[50]. Les conclusions sont tirées sur la base de codes vérolés récupérés par les experts ainsi que sur l'observation du comportement d es attaquants alors que la brèche était encore ouverte. Ainsi, l'une des attaques est attribuée à Fancy Bear ; l'autre semble émaner d'un autre groupe, toujours réputé opérer pour les services de renseignement russes, nommé APT29 ou Cozy Bear[51]. Cela fait deux ours (de l'anglais *bear*) : le Fancy (chic) et le Cozy (douillet).

À partir de ce moment, deux compromissions distinctes prennent forme : l'une est celle des systèmes du parti Démocrate, et l'autre est celle du QG de campagne de Hillary Clinton. Les deux compromissions ont mené à la publication de correspondance électronique privée, par le site web WikiLeaks. Dans le premier cas, on parle de #DNCleaks, dans le deuxième, il s'agit des Podesta E-mails (du nom du directeur de campagne

32 : Divers noms sont connus pour ce groupe de « hackers » : Sofacy, Strontium, Pawn Storm. Sa trace a été identifiée dans divers cas de compromissions de systèmes opérés par des militaires, des administrations publiques, des journalistes, des associations, etc. Les campagnes incriminées dans ces cas sont le plus souvent des attaques par *spearphishing* (donc ciblage précis de personnes clés).

de Clinton, M. John Podesta). Nous en reparlons en détail dans le chapitre 02. Fait amusant, on peut toujours voir sur WikiLeaks[52] l'un des e-mails de *spearphishing* envoyé au directeur de campagne de Clinton.

Donc, à cette étape, que peut-on conclure ? Que les moyens utilisés par les attaquants (que nous ne détaillerons pas ici pour éviter la surcharge avec des éléments techniques abscons) semblent créés pour mener des opérations d'espionnage. Les cibles précédemment identifiées et connues de Fancy Bear relèvent souvent de professions sensibles : des haut gradés de différents pays membres de l'OTAN, des experts sécurité et défense connus pour être prestataires pour les services idoines de divers États membres de l'OTAN, etc. Par ailleurs, c'est également à Fancy Bear qu'est attribuée l'attaque par *spearphishing* contre le Comité olympique international après la médiatisation du scandale de dopage d'État des athlètes russes[33]. Quoi qu'il en soit, l'analyse technique montre clairement un investissement – financier, technique et humain – constant et à long terme. Il ne s'agit donc pas d'un travail d'amateur, mais d'une activité bien financée, d'une équipe qui tient ses outils à jour et qui les adapte aux diverses plateformes techniques ciblées. On parle donc d'une entité dotée de capacités offensives sérieuses, stratégiques et planifiées.

Existe-t-il des détails établissant des liens supplémentaires avec la Russie ? La société de sécurité FireEye avait identifié que le code malveillant était écrit par ce qui semble être des russophones et que les horaires de travail correspondent à la zone Moscou-Saint-Pétersbourg[53]. Bien sûr, il n'y a pas que les services de renseignement de la fédération de Russie qui parlent russe ; par ailleurs, Saint-Pétersbourg

33 : Il ne s'agit pas là d'une anecdote « en passant », mais d'un exemple parmi tant d'autres de l'implémentation de la doctrine militaire russe (dont les prémisses en lien avec le numérique datent de 2000) : le cyberespace russe n'est pas un repaire de malfrats cherchant à apporter « le péril rouge », mais est gouverné par une législation qui illustre son importance politique. Plus encore, cette législation situe l'ambition du cyberespace d'intégrer le pays et sa culture au sein de l'espace informationnel international. La place de l'élément civilisationnel est essentielle : il s'agit de mobiliser le numérique pour promouvoir et faire respecter les valeurs nationales.

est connu pour abriter des « fermes à trolls », des agences de propagande où des étudiants gagnent de quoi mettre du beurre dans les épinards en publiant des commentaires par centaines d'après les éléments de langage fournis par le management. Ces « fermes » ont été assez solidement liées à des proches du président Poutine et son parti, Russie Unie[54].

Ainsi, les attaquants, dans le cas américain, ne sont pas nécessairement liés au renseignement russe. Enfin, l'hypothèse de recours à des « cybermercenaires » a également été évoquée : il n'est effectivement pas impossible que quelque tierce partie avec suffisamment de moyens fasse appel à des experts russophones montant une opération d'envergure qui a tout l'air d'émaner des services de renseignement russes[48]. Par ailleurs, WikiLeaks (le site où les e-mails ont été rendus publics) a toujours nié avoir obtenu ces informations du gouvernement russe. Assertion qui ne veut pas dire grand-chose, soit dit en passant…

Comme on le voit, toutes les hypothèses sont envisagées et, même si certaines ont l'air plus plausibles que d'autres, aucune ne peut être considérée comme insensée. La seule chose qui puisse effectivement départager les avis serait une publication des éléments techniques par le gouvernement américain. Des expertises indépendantes permettraient ainsi de les auditer et d'en savoir plus avec davantage de certitude. Un rapport avec de tels éléments a en effet été publié fin décembre 2016 : nous nous y arrêterons en quelques paragraphes pour expliciter la complexité de l'attribution.

LE GRIZZLY DES STEPPES LOIN À L'EST

Une partie des détails techniques concernant les outils et moyens d'intrusion proviennent du rapport[55] publié le 29 décembre 2016 par l'équivalent du ministère de l'Intérieur (*Department of Homeland Security,* abrégé en DHS) et le FBI. Le rapport tente de résumer les activités malveillantes prétendument menées par la Russie sous le

nom GRIZZLY STEPPE. Ce rapport vient conforter la déclaration publique en date du 7 octobre 2016 du DHS et du directoire des agences de renseignement américaines accusant la Russie d'implication dans les affaires intérieures des États-Unis[56]. Le rapport d'enquête fait donc mention de deux types d'éléments techniques ayant été examinés et confirmant, d'après les services américains, que la Russie a vraiment « hacké » les États-Unis : il s'agit d'adresses IP et d'un code vérolé écrit dans le langage de programmation PHP.

WorldFence, une entreprise spécialisée en sécurité avec un focus sur le logiciel de gestion de contenus WordPress, s'est intéressée au code vérolé écrit en PHP[57]. WordPress est le logiciel que l'on déploie très souvent pour faire un site ou un blog ; il est écrit en PHP. Il est donc un peu logique qu'une entreprise dont c'est le cœur de métier se saisisse de l'examen d'un exécutable malveillant écrit en PHP. Le résultat de leur enquête est que le code malveillant a très probablement été créé par une société qui s'identifie comme ukrainienne, pas russe, et que sa version est vieille. Étant donné les capacités offensives dont disposent les services de sécurité russes, on peut s'étonner que du code malveillant utilisé dans une telle attaque soit probablement produit par des tiers. On n'est jamais mieux servi que par soi-même, alors pourquoi pas dans ce cas aussi ? Il est bien sûr évident que cette identification ukrainienne pourrait être erronée ou que l'association avec l'Ukraine pourrait être voulue pour détourner les soupçons. Il s'agit là de pure spéculation cependant. Le fait est que les signatures du code vérolé correspondent à une organisation ukrainienne, pas russe.

Quant aux adresses IP communiquées par le rapport officiel américain, elles sont censées pouvoir fournir des informations telles que l'emplacement des machines à partir desquelles l'attaque s'est produite. Le problème est qu'environ 15 % de celles-ci correspondent à des relais Tor. On parlera davantage en détail de Tor dans le chapitre 03 : l'important à retenir d'ores et déjà est que Tor anonymise le trafic web. Tout le monde, vous et moi, peut s'en

servir. Autrement dit, on sait que 15 % des adresses IP répertoriées dans le prétendu « hacking » ne peuvent pas être attribuées. Elles correspondent à des machines faisant partie d'un logiciel qui rend la navigation web anonyme. Donc les personnes s'en étant servies peuvent être – ou pas – impliquées dans la compromission des e-mails du parti Démocrate. Le reste des adresses IP correspond à des services hébergés chez des entreprises respectées (le français OVH, l'allemand Hetzner, etc.). Si l'on regarde le nombre d'adresses IP par géolocalisation, il y en a davantage qui situent la machine aux États-Unis qu'en Russie – et la France y tient une position de choix également.

En réalité, des analyses supplémentaires ont montré que plus de 30 % des adresses IP correspondent en fait à des relais Tor, des proxies connus, etc. Soit, on est face à un tiers des adresses IP correspondant à des outils d'anonymat et d'obfuscation de trafic que n'importe qui peut utiliser[58]… Bien sûr, l'adresse IP est une donnée fluide et n'est pas vraiment une preuve très solide[34]. Cependant, le rapport officiel joue précisément sur les deux registres : ce n'est pas très solide, mais c'est une preuve ; or la tête de la preuve n'a pas l'air tellement à charge contre la Russie, donc retour à la case de départ.

Si l'on voulait résumer ces observations, on pourrait dire que les éléments techniques fournis dans ce rapport ne permettent pas d'établir un lien entre la Russie (et ses services de renseignement) et l'attaque ayant compromis les serveurs e-mail du parti Démocrate américain en 2016. En effet, le code malveillant écrit en PHP n'indique pas de lien avec la Russie et les adresses IP peuvent avoir été utilisées par n'importe qui.

Oui mais, direz-vous, ce rapport n'a pas pour but de fournir des preuves techniques pour l'attribution : son but principal est de

34 : Voir, à titre d'exemple, l'excellente explication de Jérôme Nicolle et Arnaud Fenioux dans le magazine de sécurité informatique *MISC*, « IP squatting appliqué au spam » (*MISC* n° 89 : https://boutique.ed-diamond.com/home/1157-misc-89.html). L'article contient des détails techniques mais le mécanisme de détournement d'adresses IP pour en faire des émettrices de spams qui y est décrit reste compréhensible pour un néophyte.

contribuer à une meilleure qualité des défenses et des modèles de menaces. Pour ce faire, le rapport contient un mélange de données émanant du gouvernement et d'acteurs privés. Ces données sont déclassifiées pour l'occasion et visent ainsi à permettre aux professionnels de mieux connaître la cybermenace russe. « C'est super intéressant ! », a dû se dire tout professionnel… ce qui augmente d'autant le sentiment de déception.

Le rapport est ainsi l'équivalent d'une brochure marketing, les images en moins. Dans tout le texte, l'attribution est affirmée avec certitude, mais il n'y a aucune preuve tangible qui soutienne une telle assertion. Le rapport cite par ailleurs des groupes généralement connus pour travailler avec les services russes. Cela aurait été intéressant et très pertinent si la liste ne souffrait de quelques défauts : un même groupe y est listé avec tous ses noms connus, mais le nommage laisse à penser qu'il s'agit de groupes différents et distincts. En outre, les noms de groupes d'attaquants présumés sont mélangés avec les noms de logiciels vérolés ou – pire ! – avec le nom générique de vulnérabilité (« Powershell backdoor »).

Mais regardons les données présentées comme une combinaison d'informations déclassifiées émanant du gouvernement et du secteur privé. Pour rappel, ces données sont censées fournir des informations quant à la nature des menaces et aider les professionnels à l'amélioration de leurs défenses et modèles de menace. Premier bémol : le rapport ne fait aucune distinction entre données issues du secteur public et celles du secteur privé. Ce point a l'air d'être l'apanage d'un pinailleur. Une distinction claire[59] a son importance : chaque type de données est soumis à un niveau de vérification et de secret différent. Ainsi, ce n'est pas la même chose de savoir qu'un élément X provient d'une équipe du FBI spécialisée dans l'étude de la façon dont opèrent les logiciels vérolés d'acteurs étatiques hostiles et qu'un élément Y est une adresse IP identifiée par le stagiaire d'une PME sur un site de vidéos en ligne. Le degré de confiance à accorder à chacun de ces éléments varie et il en sera de même

avec la signification que l'on peut leur attribuer dans le cadre d'une prise en compte pour l'amélioration des pratiques. Dans le rapport, ces sources ne sont pas clarifiées et les données sont mélangées. Comment, dans ce cas, qualifier les menaces ?

En parlant d'outils et d'éléments techniques, nous voyons la liste d'une trentaine de signatures de logiciels malveillants. « Chouette », se dit-on. Puis, on va sur VirusTotal (le catalogue d'outils de « cyberméchants », si vous me passez l'expression) et on se rend compte que, à l'exception de deux signatures, tout est déjà répertorié. On en revient donc à la critique du manque de contexte et de clarification quant à ce qui est de l'information du gouvernement et ce qui provient du secteur privé. Ainsi, on se retrouve avec une liste d'éléments potentiellement intéressants mais on ne sait absolument pas à quel acte de cybermalveillance chaque élément est associé et encore moins quel est le niveau de confiance de l'attribution. Du coup, le risque de faux positifs est très élevé. Comment peut-on aider les professionnels à reconnaître et mieux se protéger contre des cyberattaques russes sans aucun détail tangible concernant lesdites attaques et leurs outils ?

Heureusement, le tir a été corrigé le 10 février 2017 avec la publication par le DHS[60] d'un rapport technique détaillé de meilleure qualité. Son contenu ne discute pas de l'attribution (elle semble acquise), mais fournit toutes les informations nécessaires à la description et l'identification techniques des outils numériques utilisés par les attaquants. Ces informations sont une compilation de toutes les analyses techniques d'intrusion concernant les groupes Fancy Bear et Cozy Bear connues à ce jour.

RUSSES OU PAS ?

On se retrouve ainsi avec un faisceau d'indices certes assez concluants, mais issu principalement des investigations d'acteurs privés. Bien sûr, tout enquêteur vous dira qu'il est quasiment impossible d'avoir autre chose qu'un solide faisceau d'indices

(les coupables dans ces cas-là ne se bousculent pas au portillon pour expliquer le *modus operandi*). Ces indices n'ont pas été abordés en détail plus haut mais des exécutables malveillants retrouvés dans le cas du « hack » du parti Démocrate ressemblent fort à ceux retrouvés dans la compromission des systèmes du parlement allemand[61] il y a quelques années[62]. D'autres bouts, plus amusants, incluent le pseudonyme d'un des attaquants, découvert dans les métadonnées de certains documents : « Фе́ ликс Эдму́ндович » (Félix Edmoundovitch) en référence à Félix Dzerjinskiy, un célèbre bolchevik ayant dirigé l'Union soviétique pendant un temps. Une immense statue du monsieur décorait la place Loubyanka, située en face du bâtiment du KGB jusqu'en 1991. Le KGB s'appelle aujourd'hui le FSB… les services de renseignement russes qui seraient responsables des attaques *via* Fancy Bear et Cozy Bear.

Bien sûr, il ne faut jamais perdre de vue les enjeux d'une attribution, surtout dans ce cas très complexe. Pour reprendre les mots de l'écrivain français Marcel Pagnol, « *les coupables, il vaut mieux les choisir que les chercher* ». Ramenée au cas qui nous occupe, cette remarque fait écho à celle de Guillaume Poupard, le directeur général de l'ANSSI d'après qui l'attribution n'est pas tant une décision technique qu'elle est politique :

« La question de l'attribution des attaques est le grand problème du cyber. On a la plupart du temps une idée de qui est derrière, mais on ne peut pas prouver l'origine devant un juge par exemple. Voyez aux États-Unis, la parole présidentielle accuse les Russes mais n'a pas de preuves (ou ne peut les révéler) et on ne les aura sans doute jamais. Ce que peut dire l'ANSSI c'est que l'attaquant travaille sur le fuseau horaire de Moscou, laisse des commentaires en cyrillique dans les codes d'attaque... Mais tout cela peut aussi bien être une ruse pour orienter l'attribution de manière délibérée. Il n'y a pas de « smoking gun » dans une attaque cyber. L'attribution est in fine une décision politique de très haut niveau, orientée par un faisceau d'indices. »[63]

En conclusion, les deux rapports officiels du gouvernement américain fournissent des éléments tangibles et détaillés sur les modes opératoires, approches techniques et outils utilisés par ce qui semble être les groupes Fancy Bear et Cozy Bear. Ces derniers sont potentiellement associés aux services de renseignement russes (le FSB plus spécifiquement). L'attribution est raisonnablement plausible[35]. Le fait que beaucoup de personnes ont été la cible d'une attaque par *spearphishing* attribuée à ces groupes spécifiques suggère que suspecter une imposture de la part de tiers tentant de se faire passer pour les services russes est peu plausible. Ceux qui doutent de la responsabilité russe se positionnent surtout au niveau de la motivation : pourquoi le gouvernement russe aurait voulu nuire à Hillary Clinton et favoriser Donald Trump ?

LES RUSSES ONT-ILS FAIT ÉLIRE DONALD TRUMP ?

Est-on sûr et certain que ces attaques ont véritablement changé le cours de l'histoire et infléchi les décisions des électeurs américains ? Autrement dit, a-t-on à notre disposition de quoi décrire et soutenir une causalité plausible ?

Ainsi, si l'on admet que les attaques ont véritablement compromis les systèmes informatiques des Démocrates et que l'étalage des e-mails de la candidate Clinton a été monté en épingle pour la discréditer au profit de Trump, on devrait répondre par l'affirmative. Déjà on voit que ce cheminement de causes et conséquences est loin

35 : Des échanges avec divers experts et certaines victimes d'attaques précédemment imputées à ces groupes accordent également une confiance élevée à cette attribution. Voir par exemple l'étude très détaillée d'une attaque contre un groupe de journalistes très critiques envers les politiques russes en Ukraine et en Syrie https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/
Par ailleurs, certains experts sont passés de l'incrédulité à la conviction après consultation des informations à disposition (http://www.npr.org/2017/01/04/508151142/cybersecurity-expert-is-convinced-russia-was-behind-dnc-hacking). Cette certitude est par ailleurs partagée par des figures connues pour leur conservatisme et leur scepticisme (https://www.lawfareblog.com/need-official-attribution-russias-dnc-hack).
Enfin, les sceptiques existent évidemment, mais leurs arguments semblent surtout concerner la motivation des intrusions (https://medium.com/@jeffreycarr/can-facts-slow-the-dnc-breach-runaway-train-lets-try-14040ac68a55#.sflecc5bn).

d'être clair et certain. De là à affirmer que des actions – somme toute peu originales – d'espionnage émanent du président russe et soutiennent une stratégie de longue date en faveur de Donald Trump est se fourvoyer (et faire du mauvais James Bond). Retracer l'histoire de tous les évènements géopolitiques dans lesquels la Russie a été impliquée pendant que la campagne présidentielle américaine battait son plein – l'intervention en Syrie, au hasard – est certes un exercice de contextualisation intéressant, mais il n'a aucunement sa place ici et n'est pas pour autant une preuve.

Cependant, si l'on parle de ce cas spécifique ici, c'est pour bien embrasser la complexité d'une attaque de nature technique et de ses conséquences. Tout comme pour le groupe Vinci, la sophistication de la compromission dépasse la prouesse technique. Dans le cas de Vinci, la motivation des personnes à l'origine du canular (voire de l'escroquerie) élaboré n'est pas claire et n'a pas été communiquée (le coup n'a pas été publiquement revendiqué). Dans le cas des élections américaines, établir des causalités est encore plus complexe. Il y a plusieurs choses qui se détachent et qui peuvent soutenir ou au moins nourrir un lien de causalité. Tout d'abord, pour naviguer dans le monde assez tumultueux de la sécurité lorsque l'on « joue dans la cour des grands », il vaut mieux connaître les bases des techniques d'espionnage du XX^e^ siècle.

On pourrait par exemple spéculer que les attaques *spear-phishing* contre les Démocrates américains et les publications d'e-mails qui ont suivi furent un cas d'école d'influence russe. L'information est utilisée comme une arme et la stratégie dite « des 4 D » est appliquée plus ou moins d'après le manuel. « Les 4 D », comme les Anglo-Saxons ont l'habitude de dire, désignent *dismiss* (rejeter), *distort* (déformer), *distract* (distraire), *dismay* (consterner). En bref, l'approche consiste d'abord à rejeter les rapports négatifs et les accusations fondés sur des observations de terrain. Puis survient la déformation des choses pour les faire paraître différentes, distraction supplémentaire qui s'ajoute à celle provoquée par des attaques à l'encontre d'autres acteurs. Enfin vient la consternation :

attention, si Untel fait ceci (quelque mouvement auquel la Russie s'oppose), les conséquences seront terribles.

Dérouler « les 4 D » dans le cadre des élections américaines serait facile mais un peu hors sujet. Disons seulement que l'approche tombe sous le sens et que cela constitue pour beaucoup une preuve que voilà, les Russes ont fait élire Trump. On peut beaucoup discuter de cette si (peu) certaine relation de causalité – ou juste admettre qu'une partie significative des électeurs américains a décidé de s'aligner sur les idées véhiculées par Trump. Ajoutons à ces incertitudes l'émoi suscité par les *fake news,* ces informations déformées ou entièrement fabriquées, qui ont été disséminées pour porter préjudice à l'image de la candidate Clinton au profit du candidat Trump. Pour beaucoup, les *fake news* ont autant contribué à faire élire Donald Trump que les Russes. Une étude récente menée par deux chercheurs de l'université de Stanford[64] montre que l'impact décisif des fausses informations diffusées sur les réseaux sociaux n'est pas aussi clair : les données dont on dispose ne permettent pas de conclure sur une causalité. Ce que l'on y lit, c'est surtout une démonstration supplémentaire de l'effet polarisant de certains réseaux où les joutes verbales ne sont plus des débats, mais des preuves souvent par l'insulte que « nous » avons raison face à « eux ». Toutes ces considérations rappellent justement que la désinformation est un processus social et que la déformation de faits relève de la lecture que chacun en fait et des intérêts qui sont les siens[65]. Ainsi, on est surtout face à la promotion, sans scrupule ni éthique de la part de certains, de leur opinion politique. Établir une causalité entre quelques évènements de nature numérique et cette évolution du discours politique est tout simplement une gageure.

Et justement, il paraît plus raisonnable de s'intéresser au vrai problème qui se cache derrière cette causalité aussi délicate. Le problème n'est pas seulement technique. Il y a de bonnes raisons de considérer que les intrusions dans les systèmes du parti Démocrate ont été opérées par des groupes affiliés d'une façon

ou d'une autre avec le gouvernement russe. Le « hacking » à des fins d'espionnage est le pain quotidien de beaucoup de services disposant de capacités offensives, que leur gouvernement soit ou pas considéré comme démocratique.

La combinaison entre intrusion et publications subséquentes des informations volées opérée par un acteur du renseignement d'un gouvernement étranger va cependant au-delà de ce quotidien. L'influence politique pouvant être exercée *via* ce procédé d'obtention d'informations est une partie des conséquences possibles. Mais si l'on part du principe que l'offensive a été faite dans le but d'exercer une influence ou une pression politique sur le processus électoral en cours, on passe de l'espionnage usuel à l'ingérence. D'où notre insistance à bien différencier les faits des motifs.

Ainsi, la rigueur et la précision sont plus importantes que jamais dans la lecture des évènements, qu'ils soient techniques ou géopolitiques, ou techno-géopolitiques. Dire que la motivation principale d'une telle attaque informatique est la perturbation d'un processus démocratique et l'élection d'un candidat pas spécialement favorisé par les électeurs pose par exemple la question très délicate de la réponse. Comment un État réagit-il face à un autre État aux intentions hostiles ? Quelles actions sont appropriées et sont-elles proportionnées ?

PIRATER UNE ÉLECTION, EST-CE POSSIBLE ?

L'inquiétude d'un « piratage » de l'élection présidentielle en France n'était pas vraiment médiatisée jusqu'à la mi-février 2017, lorsque le candidat Emmanuel Macron a envoyé certains membres de son équipe de campagne expliquer que le Kremlin voudrait torpiller sa candidature. Ces déclarations ont, semble-t-il, donné le feu vert à une hystérisation inutile et potentiellement dangereuse de la question de cyberinfluence étrangère sur les élections françaises. Prenons du recul.

Il serait mal avisé de nier une probable ingérence d'un État étranger dans les processus d'un autre État. En fin de compte, c'est un peu ce que font les diplomates : promouvoir l'intérêt du pays qui est le leur et s'assurer que celui-là est bien considéré dans les évolutions de l'État où ils sont en poste. Comme on vient d'en discuter aussi, l'ingérence technique pilotée par les services de renseignement d'un gouvernement peut également dessiner une nouvelle forme d'influence, mais à ce stade, on n'en sait pas grand-chose de plus.

Revenons donc aux risques pour la France. Quelles attaques informatiques pourraient toucher le pays de façon à significativement altérer les résultats d'un scrutin présidentiel ? La première chose qui vient à l'esprit de beaucoup est : des « piratages » au niveau des sites web des candidats. Rappelons par exemple que les équipes de campagne ont déjà été averties de failles relatives à l'outil de gestion de contenus utilisés sur leurs sites respectifs (WordPress)[66]. On ne fera pas un inventaire des failles potentielles ici, elles dépendent de divers facteurs. On se retrouve donc dans la situation où un site web peut être « défacé » (c'est-à-dire que des contenus de tiers peuvent être introduits pour remplacer des contenus d'origine) ; rendu inaccessible (par le biais d'une attaque en déni de service) ; etc. Plus largement, un *défacement* est une atteinte à l'image qu'un candidat projette à l'extérieur. On pourrait donc ajouter à une attaque du site web (un moyen de communication au public) les réseaux sociaux, les déclarations publiques et les meetings. Ainsi, le détournement d'outils numériques de communication sortante des candidats peut être considéré comme une attaque : si l'on se fait « pirater » son compte Twitter qui se met à débiter des insanités, il y a des chances pour que l'impact sur l'image soit négatif. Il en est de même avec le site web. Cependant, la conséquence de ces compromissions n'est pas très grave : si vous souhaitez être député ou prétendez à l'investiture suprême, prendre des coups de ce genre fait partie du jeu politique.

Outre les outils de communication sortante, de nombreux candidats et partis disposent également de systèmes de communication interne : les e-mails, les *chats* de coordination, les bases de données des adhérents ou des donateurs, etc. Le risque de voir ne serait-ce qu'un des composants de cette infrastructure technique compromis est autrement plus important. Accéder aux reportings et stratégies internes est une compromission sérieuse de la sécurité de l'information stratégique de l'organisation. Par ailleurs, même si on n'accède pas nécessairement aux fonds d'une campagne électorale, on peut récupérer les données bancaires des donateurs. Les conséquences d'une compromission de la stratégie peuvent être (politiquement, économiquement, etc.) sérieuses ; celles de la compromission des données à caractère personnel dont l'organisation a la charge ne sont pas des moindres non plus : la collecte et les opérations sur des données à caractère personnel sont réglementées. Les mésusages et les manquements de sécurité de ces données dont vous êtes l'opérateur sont punissables. Pour le dire avec un peu d'humour, les livres que l'on n'a pas lus se vengent à leur façon ; prenez par exemple le Code pénal. L'article 226-17 le stipule assez clairement : « *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.* » En français simple, si vous stockez des données de vos adhérents et donateurs, mais ne faites rien pour assurer que les failles les plus évidentes sont colmatées, une fuite peut vous tomber dessus et ce sera possiblement de votre faute, y compris au regard de la loi.

On voit donc que les outils numériques ont des exigences et des objectifs différents et distincts. À ceux-là sont associées des menaces diverses et dont la criticité varie. Avant de reparler du modèle de menaces, discutons rapidement de l'identification des attaquants. Comme nous l'avons vu dans les pages précédentes, l'attribution des attaques est un exercice difficile. D'aucuns peuvent affirmer avec certitude que des compromissions (prétendues ou réelles) à leur

encontre proviennent de la Russie. En soutien à ces dires, on peut voir donnée l'origine de l'adresse IP d'où les attaques émaneraient. Mais, comme signalé plus tôt, l'adresse IP est une donnée fluide et peut être modifiée et/ou obfusquée ou cachée. À elle seule, une adresse IP ne constitue pas une preuve, et elle est encore moins l'argument d'attribution le plus fiable. Comme nous l'avons vu avec l'étude de l'exemple américain, la simple géolocalisation d'adresses IP ne suffit pas à déterminer l'origine des attaques. En pratique, elles sont le plus souvent effectuées en utilisant des machines intermédiaires (des proxies). De très nombreux bots, des programmes de reconnaissance qui scannent Internet à la recherche de serveurs, de sites ou de base de données vulnérables, sans cibler spécifiquement telle ou telle organisation, existent également. Ce genre de trafic est de l'ordre du quotidien, tous les administrateurs de sites en voient passer dans leurs fichiers journaux[36].

Il semble que dire de n'importe quelle cyberattaque – quoi que cela signifie – qu'elle est la faute des Russes soit à la mode. Il y a quelques années, c'était la Chine. Votre site web était mal configuré et vous vous êtes retrouvé « hacké » ? La faute aux Chinois ! Vous avez oublié d'utiliser Windows Update pendant deux ans, du coup quelqu'un vous a « piraté » et volé les données contact de vos clients ? Les Chinois, aucun doute ! Un e-mail de *phishing* avec une pièce jointe contenant du code vérolé dont vous n'arrivez plus à débarrasser votre machine ? Les Chinois, on vous dit ! Une fois que cette mode fut un peu passée, ce fut la faute aux Iraniens, puis au Cybercalifat, le prétendu groupe de cyberattaques de l'organisation terroriste État islamique. Depuis la deuxième moitié de 2016, c'est la faute aux Russes. Bien sûr, il serait mal avisé et naïf de complètement exonérer la Russie ou un quelconque autre gouvernement de tentatives d'influence plus ou moins discrètes. La Russie est considérée comme très active du point de vue des attaques informatiques et ce, sans doute à juste titre. Mais elle n'est sans

36 : Fichiers contenant des messages relatifs au système, aux services et aux applications qui s'y rapportent.

doute pas le seul acteur en jeu, qu'il s'agisse d'autres pays, d'activités criminelles, ou, on est en droit de l'imaginer, de partis politiques concurrents. L'attribution d'une attaque, l'identification de son origine est un exercice très difficile, on l'a vu avec le cas américain. Et encore, ce dernier fait plutôt figure d'exception dans le sens où on dispose rarement d'autant d'informations sur un attaquant. Fancy Bear, l'un des groupes identifiés à l'origine des compromissions américaines, est surtout connu parce qu'il est très actif à l'encontre de cibles très spécifiques (haut gradés et hauts fonctionnaires[37]) et qu'il a des buts précis (espionnage). On connaît ses activités depuis une décennie et malgré cela, on ne peut affirmer que très peu de chose les concernant. Par exemple, personne ne sait combien de personnes travaillent au sein de Fancy Bear de façon permanente. On ne sait pas où ils sont localisés : dans la même ville (laquelle ?), dans différentes villes (lesquelles ?), etc. On ne sait même pas comment ils s'appellent eux-mêmes…

Ces effets de mode sont en bonne partie dus à des effets de communication : il est évident que vous allez attirer de nombreux nouveaux clients si vous assurez avoir protégé les vôtres d'attaques très sophistiquées émanant d'acteurs excellemment outillés, voire soutenus par des États. La banalité d'une macro activée par défaut dans un document Word ne vend pas beaucoup. Si vous êtes la victime d'une compromission, que préférez-vous ? Admettre que vous avez été attaqué (et que vous avez potentiellement enfreint la loi en ne faisant pas suffisamment attention à la sécurité de vos infrastructures) ou dire que l'attaquant semble être piloté par un gouvernement étranger hostile qui vous en veut ?

Que ce soit contre des outils de communication sortante ou interne aux candidats, il faut donc se garder de conclusions hâtives.

37 : Les exemples sont nombreux : l'OTAN (https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff), la Géorgie (https://www.wsj.com/articles/hacking-trail-leads-to-russia-experts-say-1414468869), des ministres des Affaires étrangères de différents pays européens (https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html), etc.

Il serait mal avisé de transformer une très probable mauvaise infogérance en une déclaration d'ingérence hostile d'un gouvernement étranger dans la politique française.

Enfin, on pourrait mentionner les probabilités de compromission des ordinateurs de vote en France. En cohérence avec notre exemple américain, précisons que la prééminence du vote électronique est beaucoup plus importante aux États-Unis qu'en France. Les votes ont été recomptés dans trois états américains jugés problématiques[67], les doutes portaient sur une possible manipulation des machines et, par conséquent, des résultats. D'après les enquêtes américaines, aucune compromission n'a été constatée de ce côté dans le scrutin présidentiel de 2016. En France, la proportion des communes où le vote est exclusivement par ordinateur (non-papier donc) est très basse en comparaison avec les États-Unis. Comme nous le verrons dans les prochaines pages, les ordinateurs de vote présentent de très nombreuses défaillances constituant ainsi un problème démocratique fondamental. Techniquement parlant, leur vulnérabilité est déjà un fait : en France, ils sont vieillots, leurs logiciels ne sont pas mis à jour, de nombreux dysfonctionnements ont été amplement relevés et documentés depuis 2004… Si des suspicions existent quant à une ingérence étrangère, ce sera à l'État d'enquêter et, en cas de question formulée auprès du Conseil constitutionnel, ce sera à celui-ci de décider si d'éventuels changements peuvent être de nature à modifier le résultat final du scrutin.

ÉVALUER LES RISQUES

À propos d'espionnage et de compromission, il faut être réaliste et surtout ne pas céder à la panique. En effet, si quelqu'un (au hasard, Poutine) vous en voulait personnellement, les mesures auraient été prises plusieurs mois auparavant pour s'infiltrer et récupérer les informations jugées utiles. Comme nous l'avons mentionné plus haut, les premiers articles de presse parlant d'intrusion malveillante ou de tentative chez le parti Démocrate américain

datent de mars 2016, soit plusieurs mois avant que le monde entier n'apprenne que Hillary Clinton écrit des e-mails.

En matière de sécurité informatique, l'inquiétude raisonnable est de rigueur. Cela signifie qu'il faut avant tout mesurer les risques. Défigurer le site d'un candidat pendant quelques heures aura des conséquences sans doute négligeables. Une intrusion sur le réseau connectant diverses infrastructures gérées par l'État et permettant de faire remonter les votes aura en revanche un effet très important. L'ANSSI et le ministère de l'Intérieur veillent sur cette infrastructure ainsi que sur divers aspects de la sécurité de ce que l'on appelle des « opérateurs d'importance vitale » (OIV). Ces derniers incluent Orange, EDF, Areva, etc. Depuis l'élection de Donald Trump, les « piratages » du parti Démocrate et de la candidate malheureuse Hillary Clinton sont considérés comme une certitude au même titre que l'est leur grande influence sur l'issue du scrutin. Comme nous l'avons vu, certaines de ces certitudes mériteraient un œil plus critique, d'autant plus que cette ambiance délétère a tendance à hystériser les débats autour de cette question.

Mais voyons le bon côté des choses : ce précédent a contribué à une prise de conscience. Il est important que les formations politiques et les candidats prennent l'habitude de sécuriser leurs communications, leurs bases de données, leur matériel, etc. Et parlant de communications justement, il ne s'agit pas seulement des e-mails, et autres SMS. La sécurité IT est une composante parmi d'autres et le facteur humain ne doit pas être négligé. Ainsi, si l'on garde le même exemple français, on pourrait se demander : quel est le modèle de menaces des candidats à l'élection présidentielle ou aux législatives, ou des députés eux-mêmes ? Face à une communication sortante alarmiste de la part de ces personnes, on peut légitimement se demander ce qu'il pourrait y avoir de si précieux sur leur site web qui mériterait qu'une puissance étrangère s'acharne à s'y introduire ? C'est peut-être une question autrement plus importante (y compris légalement parlant) que de gesticuler.

Puisqu'on parle beaucoup du facteur humain, concluons cette partie en rappelant que la sécurité informatique est, selon la célèbre citation de Bruce Schneier, l'un des experts les plus connus[68], « *un processus et non pas un produit* ». Mettre les bons mots de passe, sécuriser ses serveurs sont des approches nécessaires mais insuffisantes. Le but, en disant cela, n'est pas de créer de l'anxiété, mais de sensibiliser : nous devons veiller en continu au maintien et à l'amélioration des procédures de sécurité[38]. En pratique, on peut par exemple revoir régulièrement la nécessité de nos bases de données à être connectées à Internet : si cette connexion n'apporte rien, pourquoi la maintenir ? Certains canaux de communication (les SMS, les messages *via* l'application Telegram, etc.) sont moins fiables que d'autres (les applications Signal ou Silence, par exemple)[39]. Si vous avez de nombreux terminaux, il est recommandé d'inventorier de façon régulière quel membre de la famille a accès à quoi, etc. Enfin, si vous êtes un parti politique, en période préélectorale ou, en tout cas, si vous avez un rôle significatif dans un pays, il est fort probable que des pays tiers aient déjà tenté et peut-être réussi à vous compromettre depuis un moment. Se savoir vulnérable et cible potentielle d'attaques permet d'aborder la question de l'évaluation des risques et des conséquences potentielles d'une compromission. Et le plus important : préparer une stratégie de réponse et apprendre de ses erreurs pour mieux se prémunir à l'avenir.

38 : « Sécuriser » signifie que l'on fait en sorte que le coût de la compromission sera supérieur au gain attendu.

39 : Nous détaillerons ce qu'est le chiffrement dans le chapitre 03. D'ici là, il est important de rappeler que chiffrer ses communications reste le moyen le plus simple d'assurer leur confidentialité et leur intégrité. Le plus simple pas seulement parce que de nombreuses applications permettent de l'utiliser sans même s'en rendre compte, mais aussi parce que son utilisation permet de réduire les distractions dans le processus d'amélioration des pratiques. En effet, chercher à attribuer une attaque ou à deviner qui sera notre prochain attaquant est une distraction. Donc, mieux vaut essayer de se protéger contre toute intrusion non autorisée, qu'elle soit chinoise, russe ou celle du gamin des voisins.

02

. . . .

L'ÉTERNELLE TENSION ENTRE PROTÉGER ET RESPECTER

Comme nous l'avons vu au début de ce chapitre, les États peuvent recourir à l'outil numérique pour en faire un levier d'influence géopolitique. Mais qu'en est-il sur le plan intérieur ? Un gouvernement utilise-t-il toujours le numérique pour le bien de ses citoyens ?

CHAQUE E-MAIL QUE TU ÉCRIRAS, JE LIRAI

En juillet 2012 se tient au Kenya le sommet international du média citoyen Global Voices. L'un des thèmes couverts par ce média est « communiquer sur les enjeux du numérique de par le monde » en s'appuyant sur une large base d'auteurs bénévoles du monde entier. Le dernier jour du Sommet a lieu la remise des Breaking Borders Awards, sponsorisés par Google.

C'est la belle époque de l'activisme numérique : un peu plus d'un an après les « révolutions arabes », le désenchantement n'a pas encore (totalement) gagné les cœurs, et beaucoup croient toujours au pouvoir mobilisateur des réseaux sociaux tels que Facebook. Les émotions des retrouvailles et discussions sont rapidement remplacées par la joie de voir Mamfakinch, un média marocain, bénévole et avec du caractère, remporter le Breaking Borders Award[69]. Le lendemain, dernier jour de séjour pour beaucoup, nous jouons les touristes au Masaï Market. Nous nous y perdons un peu avec

l'un des fondateurs de Mamfakinch, ce qui nous donne le temps de discuter de la signification du prix pour le média et pour la liberté d'expression au Maroc. Le mouvement protestataire ayant débuté le 20 février 2011 s'essouffle, la popularité de Mamfakinch décline aussi. Ils ont même subi des attaques DDoS début 2012. Revigorés par le prix, par l'engagement des gens croisés (et le chemin vers l'hôtel retrouvé), notre discussion se conclut en nous disant que la route est longue, mais la voie se libère.

À peine quelques jours plus tard, des messages alarmés nous parviennent : « Tentative de piratage malveillant chez Mamfakinch, faites attention aux e-mails que vous recevez. » En effet, comme la grande majorité des sites web, celui de Mamfakinch a une page contact avec un formulaire *via* lequel les lecteurs et autres visiteurs peuvent écrire à l'équipe. C'est ainsi qu'un e-mail avec le sujet « *Dénonciation* » est reçu, puis transféré à la quinzaine de membres de l'équipe. Une seule ligne dans l'e-mail (reproduite sans correction) :

« Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles… »

Rien de particulièrement bizarre : au Maroc, si vous manifestez vos griefs politiques un peu trop haut, vous risquez la prison. L'e-mail, envoyé par *i-imane11@yahoo.com* contient aussi une pièce jointe nommée « scandale(2).doc ». Sept des quinze membres de l'équipe ont ouvert ce document… qui s'est révélé vide. Et ça, c'est bizarre.

La personne chargée du SI (systèmes informatiques) de Mamfakinch s'aperçoit rapidement qu'il s'agit d'un logiciel malveillant. Le tout atterrit chez Morgan Marquis-Boire, un Néo-Zélandais qui travaille à l'époque chez Google sur des projets de sécurité. Lors du sommet de Global Voices au Kenya où il était également présent, il a été question de surveillance et des découvertes sur les usages de tels logiciels par le gouvernement du Bahreïn. Ces découvertes

ont été faites par le Citizen Lab, un groupe de recherche sur la sécurité informatique et son impact sur les droits de l'homme, basé à l'université de Toronto au Canada. Pour prévenir les manifestations et éliminer les opposants, le gouvernement du Bahreïn utilise des logiciels de surveillance dont le but originel est de fournir des informations au sujet de criminels[70]. Morgan Marquis-Boire aide bénévolement Citizen Lab pour ces recherches et c'est en cette qualité qu'il a reçu le logiciel malveillant de Mamfakinch pour analyse[71].

En août 2012, l'équipe de Mamfakinch a la confirmation[72] que le fichier « scandale(2).doc » est bien un leurre et contient un logiciel malveillant. Un exécutable, « adobe.jar », s'installe sur l'ordinateur de la personne ayant ouvert le document, et lance le déploiement d'une porte dérobée. Cette dernière fonctionne aussi bien sur un ordinateur avec Windows que sur un Mac. Le *spyware*[40] ainsi installé capte donc tout ce que l'utilisateur tape sur le clavier (mots de passe aussi, bien entendu), intercepte les e-mails envoyés et reçus, enregistre les discussions Skype, prend des captures d'écran et collecte des données *via* le micro et la webcam. Le tout sans être remarqué par les antivirus et sans que l'utilisateur suspecte quoi que ce soit. Ainsi, l'ordinateur de toute personne ayant ouvert le document joint est infecté…

L'investigation menée par Citizen Lab[73] a établi deux faits essentiels. Le premier est que l'e-mail avec la pièce jointe vérolée ayant propagé le *spyware* provient d'un ordinateur dont l'adresse IP correspond à la capitale administrative du Maroc, Rabat ; plus précisément, l'IP correspondait à l'une de celles appartenant au conseil suprême de la Défense nationale marocain, l'entité chapeautant

40 : Nom générique pour dire logiciel d'espionnage (un « espiongiciel », si l'on voulait franciser selon les règles du français). Le mot « mouchard » conviendrait, mais il est un peu trop généraliste, or ce que l'on veut dire ici, c'est qu'il s'agit d'un logiciel et non pas d'un autre moyen d'interception.

les divers services de renseignement du royaume[41]. Le deuxième fait établi par Citizen Lab est l'identité du logiciel et de son créateur : le spyware s'appelle RCS, pour *Remote Control Systems* (« systèmes de contrôle à distance »), le produit phare commercialisé par la société italienne Hacking Team[42]. Citizen Lab a également établi qu'un activiste de renom aux Émirats arabes unis a aussi reçu un mail vérolé par le même *spyware*.

Ces cas, documentés par Citizen Lab, ont fait beaucoup de bruit : des logiciels vendus à des gouvernements pour traquer les criminels se retrouvent utilisés pour réduire au silence des opposants politiques. Depuis le début de 2014, Mamfakinch est officiellement inactif ; d'après certains, la toxicité de la surveillance gouvernementale en est le premier responsable[74]. Qu'il ait raison n'est pas la question ici. Il s'agit en réalité de confiance. Notre ordinateur, notre téléphone, c'est notre chez-nous ; l'idée d'un inconnu qui vient chez nous, ouvre nos placards, touche nos souvenirs d'êtres chers, se gausse de nos photos du premier amour est pour le moins perturbante. Savoir que nous n'y pouvons rien malgré tous les efforts déployés pour maintenir une bonne hygiène numérique fait froid dans le dos.

Ce cas ainsi que les pages suivantes constituent une autre facette de notre discussion à propos de la confiance à l'heure

41 : Nous avons dit plus haut que l'adresse IP seule ne peut pas, le plus souvent, constituer la preuve la plus sérieuse d'attribution. Cette règle souffre exception, ce qui est précisément le cas ici. En effet, la plage d'adresses IP (un groupe d'adresses) correspondante à divers acteurs est connue, qu'ils soient étatiques ou privés. Compromettre une telle infrastructure pour se faire passer, de façon continue et légitime, pour l'entité en question quand cette dernière est un État n'est pas une mince affaire. Ainsi, dans le cas présent, la probabilité que le *spearphishing* émane d'un attaquant aléatoire s'étant approprié les données d'infrastructure réseau de l'État marocain est très faible. L'incrimination des services de l'État est largement plus probable (la qualité du *spyware* ajoute à cette certitude : quel attaquant aléatoire paierait des centaines de milliers d'euros un logiciel d'espionnage pour s'en servir dans des cas avec un gain potentiel minime ?).

42 : http://surveillance.rsf.org/hacking-team/

du numérique. Les questions autour de la tension entre sécurité et libertés fondamentales sont prégnantes et se rappellent de plus en plus souvent à nous.

LE RÔLE DE L'ÉTAT

Au début du mois de juin 2016, une puissante fusée décolle de Cap Canaveral. Elle n'ira pas plus loin que l'orbite géostationnaire où elle déploie le satellite Mentor, aussi appelé Advanced Orion, la plus grande machine d'interception de communications électroniques jamais conçue. Ces « grandes oreilles » sont mises en œuvre par le National Reconnaissance Office (NRO) américain et développées avec la contribution de la Central Intelligence Agency (CIA). À ce jour, il existe sept satellites Advanced Orion. D'aucuns reconnaîtront ici l'héritier du réseau Échelon[75]. Comme beaucoup des activités liées à la sécurité, les missions et modes opératoires de ces machines sont confidentiels (dans le cas présent, ils sont même secret-défense).

Ironiquement, le déploiement d'Orion à l'été 2016 correspond au début du dernier semestre de la présidence d'Obama. Un puissant hommage à l'homme d'État charismatique ayant créé l'état de surveillance le plus puissant que le monde ait jamais vu. Bien sûr, d'autres dirigeants tels que le roi du Maroc ou celui du Bahreïn ont créé des régimes d'espionnage de la population plus oppressifs , voire plus sanguinaires. Mais aucun n'a réussi à en construire un de taille équivalente en termes aussi bien de coûts que de pouvoir intrusif. On parle donc de sept satellites Advanced Orion en orbite autour de la Terre transmettant des interceptions électroniques ; d'un bâtiment en plein désert de l'Utah[76] dont la superficie totale dépasse les 90 000 m² et qui stocke des données interceptées à partir de téléphones personnels, courriels et autres comptes

de médias sociaux ; de câbles sous-marins[77] dans lesquels au moins le quart de télécommunications transmises peut être lu par les États-Unis ; … Alors, oui, les deux mandats successifs d'Obama ont énormément développé les capacités de surveillance des États-Unis.

BIG BROTHER IS LISTENING TO YOU

Les fondements de cet État dans l'État remontent surtout à la période immédiatement postérieure aux attentats du 11 septembre 2001. Six semaines après les attaques et suite à une lecture précipitée par le Congrès américain, le président de l'époque, George W. Bush, promulgue le *Patriot Act*[43]. Ce dernier élargit considérablement les pouvoirs de surveillance du gouvernement[78]. Le dispositif le plus controversé du *Patriot Act* permet ainsi aux agences de renseignements, du FBI à la CIA en passant par la NSA, de récupérer auprès des opérateurs de télécommunication privés des informations personnelles d'usagers, de mettre ces derniers sur écoute, d'archiver et d'exploiter des données issues de surveillance électronique. Un simple soupçon suffit pour intervenir auprès des fournisseurs de services. Et cette collecte et son exploitation se font sans que les usagers en soient avertis. Le *Patriot Act* prévoit également la possibilité de perquisitionner chez un suspect ainsi que de saisir ses biens en son absence, sans avoir besoin de le prévenir. Et comme nommer les choses, c'est les faire exister, cette loi crée aussi des statuts juridiques particuliers : « *ennemi combattant* » ou encore « *combattant illégal* » ; ces nouvelles définitions permettent d'arrêter, d'inculper et de détenir sans limite de durée toute personne soupçonnée de terrorisme.

Le *Patriot Act* prévoit l'émission, par le FBI, d'injonctions, les NSL, pour *National Security Letters* (« lettres de sécurité nationale »). Celles-ci permettent au FBI d'avoir accès aux données

43 : On notera que le nom est un acronyme très explicite : *Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, soit fournir les outils appropriés pour déceler et contrer le terrorisme.

d'usagers de télécommunications. Concrètement, un ou deux agents du FBI se présentent à votre bureau pour vous transmettre la fameuse NSL en main propre. Et en fait, ce n'est pas une demande : vous devez obtempérer sans délai. Les détails qui suivent ont pu être portés à l'attention du public seulement après plusieurs années et constituent l'un des historiques les plus complets à ce jour des dérives d'une loi qui rappelle étrangement les lois scélérates.

Nicholas Merrill est directeur et fondateur du CalyxInternet Access, un fournisseur de services indépendant, chez qui sont hébergés de nombreux sites web et e-mails associatifs et appartenant à des agences de communication et de presse. À partir du moment où il réceptionne une NSL (on est en février 2004), il lui est interdit d'en parler à qui que ce soit, y compris à sa fiancée, ses parents, ses associés, etc. ; l'interdiction vaut tant qu'il est vivant. Il n'a même pas le droit de contacter un avocat… Après réflexion, Merrill prend l'attache de son avocat et après échanges avec plusieurs autres avocats, il refuse d'obtempérer. Traduction : un individu se dresse contre l'État pour la première fois depuis que le *Patriot Act* est en vigueur. Merrill est venu parler de cette situation lors du Chaos Computer Congress (CCC, le plus grand festival activiste de cultures alternatives et numériques) fin 2010[44] ; et même à ce moment-là, il ne pouvait pas parler de tout librement[79] sinon il risquait dix ans de prison pour violation du secret de l'instruction… La suite de l'histoire est digne d'un film hollywoodien.

Précisons qu'à la fin de l'année 2003, l'administration Bush crée l'Information Awareness Office au sein de la DARPA (Defense Advanced Research Projects Agency ou « Agence pour les projets de recherche avancée de défense »). Un programme dédié, le Total Information Awareness Programme (TIA), est ensuite élaboré ; sa mission est de gérer le traitement de grandes quantités de données personnelles des citoyens, telles que des transactions bancaires,

44 : Vous pouvez revoir la vidéo de son intervention https://www.youtube.com/watch?v=eT2fQu50sMs (en anglais)

des documents de voyage et même des dossiers médicaux. Grâce à la collecte et au traitement de ces données, le programme vise à développer des modèles prédictifs servant à anticiper et prédire des crimes sur le territoire[45]. La collecte et le traitement des données personnelles du TIA sont faits sans passer par un juge ni en informer les individus : c'est ce que l'on appelle la surveillance administrative généralisée. Les médias ont mis au jour les prérogatives de ce programme[80], s'en sont émus et l'ont critiqué, ce qui a poussé le Congrès à l'arrêter fin 2003.

Le TIA n'est cependant arrêté qu'en apparence : une annexe du budget pour 2004 du département de la Défense, classée secret-défense, fait état d'un budget maintenu, mais d'un transfert opérationnel à la NSA[81]. Le pot aux roses est découvert lorsqu'en 2005, le journal *The New York Times* révèle que Bush a autorisé la NSA à surveiller les communications électroniques internationales « *de centaines, voire des milliers de personnes aux États-Unis* »[82]. Le nom de code de ce programme est Stellar Wind ; il collecte les conversations téléphoniques, les e-mails et les métadonnées directement auprès des fournisseurs d'accès tels qu'AT&T.

Le cas de Merrill est concomitant à ces développements. Son procès contre l'État fédéral débute dès avril 2004[83]. Le juge se prononce sur l'inconstitutionnalité des NSL en 2005[84]. Bien sûr, le gouvernement fait appel. Entre-temps, des modifications au texte du *Patriot Act*, dont celles dont on vient de parler, sont introduites. En 2005, une semaine après la découverte de l'existence de Stellar Wind, Barack Obama, alors sénateur, prononce un discours défendant les libertés civiles et demande au Sénat de retarder le vote d'autorisation de la nouvelle version du *Patriot Act*. Ce dernier est à nouveau autorisé en 2006. En 2007, le nouveau juge s'occupant du cas de Merrill se prononce sur l'appel du gouvernement : il maintient

45 : Murray, N. "Profiling in the age of total information awareness", *Race & Class*, 52 (2): 3–24, 4 octobre 2010. http://rac.sagepub.com/content/52/2/3.abstract . Voir aussi le film *Minority Report* , grand classique de la culture populaire geek qui traite de l'anticipation de crimes et les dérives potentielles.

la première décision sur l'inconstitutionnalité des NSL[85], en réponse à quoi le gouvernement se pourvoit en cassation. On parle de procédures qui durent plusieurs années : Merrill a dit que cette affaire a été instruite par quatre procureurs généraux (l'équivalent du ministre de la Justice en France). Pendant toutes ces années, il n'a pas dit un mot sur le cas à qui que ce soit en dehors de ses avocats, cachant les documents dans des coffres secrets chez lui, dissimulés même aux yeux de sa compagne.

Voilà ce qu'est le *Patriot Act* et les dégâts que ses prérogatives ont causés. À la suite des attentats contre *Charlie Hebdo* en janvier 2015, certains hommes et femmes politiques en France ont appelé à la création d'un *Patriot Act* à la française. L'idée sous-jacente renvoie donc, dans l'esprit de ses promoteurs, à une augmentation des moyens de surveillance des télécommunications pour prévenir les actes de terrorisme. Un tel appel ne résiste cependant pas à l'épreuve de réalité. Si on laisse de côté l'effet d'épuisement nerveux et émotionnel de l'individu face à un tel adversaire pour se concentrer sur l'efficacité du dispositif, quelles conclusions ?

Selon l'ACLU (American Civil Liberties Union, l'« Union américaine pour les libertés civiles »), entre 2003 et 2006, plus de 200 000 NSL ont été distribuées aux fournisseurs d'accès et services de télécommunications. Les données ainsi récupérées ont été archivées et traitées. Des documents obtenus en 2015 ont démontré que l'utilité de Stellar Wind a été quasi-nulle[86] : un rapport (747 pages) rédigé en 2009 précise que les indices obtenus via ce programme de surveillance sur la période 2001-2004 ont été des « *contributions significatives* » dans la lutte antiterroriste dans seulement 1,2 % des cas. Eh bien, 1 %, c'est peu… Le rapport continue en précisant que pour la période 2004-2006, aucun des indices fournis n'a été utile. Enfin, le *Patriot Act*, initialement prévu pour lutter contre le terrorisme, a été utilisé à d'autres fins : d'après l'Electronic Frontier Fondation (EFF), sur 11 129 demandes de perquisition dans le cadre du *Patriot Act* en 2013, seuls 51 avaient trait au terrorisme ;

les demandes concernaient pour l'essentiel le trafic de drogue (9 401). Des millions dépensés par le trésor public pour espionner les citoyens américains et étrangers, pour un résultat bien médiocre en somme.

FAITES CE QUE JE DIS...

Dès lors, interrogeons-nous sur les évolutions des activités de surveillance pendant les deux mandats de Barack Obama. Suite à ses déclarations de défenseur des libertés en 2005, le débat public est lancé. La première prolongation du *Patriot Act* est votée. L'opinion publique est (très) négative sur la surveillance de masse[87]. Se lançant dans la course à la Maison Blanche, Obama maintient sa position. À la fin de 2007, il promet publiquement[88] :

« Assez de secrets. Voilà l'engagement que je vous fais, en tant que président ! […] Cela signifie la fin des écoutes illégales des citoyens américains. »

Le futur président des États-Unis a même promis de soutenir une obstruction systématique à tout projet de loi qui viserait à donner l'immunité rétroactive aux entreprises fournissant une assistance aux espions du gouvernement. Obama est l'un des grands soutiens politiques des lanceurs d'alerte : d'après lui, ce sont ces personnes qui permettent d'améliorer le fonctionnement de la gouvernance en braquant les projecteurs sur des agissements pour le moins discutables, si ce n'est illégaux.

Durant les derniers mois de son mandat, le président Bush décide d'inscrire les programmes de surveillance administrative généralisée dans la loi de manière permanente. Le *Patriot Act* est prolongé de nouveau début 2006, mais avec des changements. Le pérenniser s'impose donc comme un choix intéressant pour l'administration Bush car cela permettrait de mettre fin aux tractations et à la contingence des décisions budgétaires. La défense de Bush face aux critiques change aussi : alors que jusque-là,

il prétendait que l'article 2 de la Constitution lui permettait de se passer du Congrès, il décide en 2007 de porter le débat auprès des parlementaires. Ce n'est pas une grande avancée démocratique cependant. Les amendements au *Patriot Act* sont portés auprès de la commission parlementaire sur le renseignement ; ils prévoient l'élargissement des prérogatives des agences de renseignement à toutes les investigations estimées légitimes en rapport avec la sécurité extérieure. Ainsi, on passe de la traque d'Al-Qaïda à une surveillance générale pour capter tout ce qui touche au renseignement extérieur. Les débats auprès de la commission parlementaire sur le renseignement se font à huis clos. Si les amendements proposés étaient acceptés et inscrits dans la loi, cela permettrait de ne plus tenir compte des réserves exprimées par le ministre de la Justice ou encore par le FBI. Suite aux révélations de Snowden en 2013, on apprit que ce programme de surveillance généralisée désiré, connu sous l'acronyme PRISM, a été lancé en 2007.

Ces développements poussent Obama à durcir sa position. Ses détracteurs le voient comme un jeune sénateur dont l'expérience en matière de sécurité et de lutte antiterroriste est au mieux risible. Les chaînes de télé font régulièrement état d'attentats-suicides en Irak, coûtant la vie à des dizaines de soldats américains. Au milieu de ces sables politiques mouvants, le candidat Obama s'attache les services de John Brennan : cet ancien sous-directeur de la CIA en charge de divers programmes de lutte antiterroriste sous Bush devient ainsi son conseiller en chef en matière de renseignement et de sécurité. En juillet 2008, Obama retourne sa veste : il revient complètement sur ses promesses antérieures, annonçant son soutien à une loi de surveillance généralisée qui légalise largement le programme d'écoute de la NSA et accorde l'immunité aux entreprises de télécommunications qui y contribuent.

Après avoir été élu pour son premier mandat, Obama nomme John Brennan conseiller à la sécurité nationale à la Maison Blanche

en 2009 ; Brennan prend la direction de la CIA en 2013[46]. Encore plus notable, le président Obama décide de garder le chef de la NSA en place, Keith Alexander, un général trois étoiles, à la tête de la NSA depuis 2005, surnommé « Empereur Alexander » : il obtient tout ce qu'il veut, dit-on dans les couloirs. Sous son règne, toutes sortes d'informations sont collectées et exploitées, en Irak et sur le territoire américain. Malgré les réserves de certaines sommités du système judiciaire[89], Obama non seulement garde le général Alexander, mais il lui attribue aussi une quatrième étoile en 2009, agrémentée de la direction du fraîchement créé et top-secret US Cyber Command. Enfin, plutôt que de limiter la surveillance généralisée opérée par la NSA, le président Obama autorise son expansion. Ainsi, le *Patriot Act* n'a jamais été abrogé, au contraire, elle est pérennisée en 2006 et toujours en place, même si Barack Obama a appelé à la « *réformer* » en 2013, à la suite de l'affaire Snowden.

LES RÉVÉLATIONS DE SNOWDEN

Si l'on peut aujourd'hui retracer les influences ayant contribué au déploiement du système de surveillance le plus titanesque au monde, c'est grâce à Edward Snowden. Ex-consultant pour la NSA, Snowden a révélé en 2013 l'organisation des programmes de surveillance américains et britanniques. Ces informations sont vitales pour appréhender l'ampleur de ce système et comprendre les intérêts des acteurs qui font partie intégrante de notre vie quotidienne, que ce soit Facebook ou tout type de gouvernement.

46: Entre 2009 et 2012, Brennan est aussi la personne qui mène le programme Drones de l'administration Obama. Il est également la première personne à reconnaître publiquement que les États-Unis font des frappes ciblées par drones au Pakistan, Yémen, en Somalie, etc. (voir http://www.boston.com/news/nation/articles/2012/05/21/who_will_drones_target_who_in_the_us_will_decide/).
Ce charmant personnage a ainsi toujours insisté sur la légalité et l'éthique (sic) des assassinats par drones. Enfin, Brennan est connu pour avoir bloqué une enquête du Sénat américain visant à mettre à plat la chaîne de commandement dans des cas de torture du temps du président Bush (voir http://time.com/14563/justice-considers-probe-of-senate-staffers-in-dispute-over-torture-report/).

D'après ces révélations, les premiers tests d'interception de communications électroniques hors du territoire américain débutent en 2009. Le président Obama signe le déploiement d'un programme, le SOMALGET, aux Bahamas, petit pays géographiquement proche des États-Unis. Le scénario de ce programme est loin de *Pirates des Caraïbes*[90]. L'installation des équipements de surveillance dans les systèmes de télécommunications des Bahamas est obtenue grâce à un subterfuge : l'agence américaine de lutte contre les stupéfiants convainc tout simplement le gouvernement de l'archipel que l'opération aidera à capturer des trafiquants de drogue. En réalité, ces équipements ouvrent une porte dérobée pour la NSA qui peut alors exploiter, enregistrer et stocker des données de conversations électroniques. Aucun mandat de juge n'est requis côté américain. Ainsi, en deux ans, SOMALGET aurait permis d'atteindre son objectif de 100 % de surveillance dans les Bahamas, à savoir l'espionnage des téléphones portables de quelque 6 millions de citoyens américains qui visitent ou résident dans le pays chaque année. Suite au succès de SOMALGET, la NSA a déployé le programme en Afghanistan, aux Philippines, au Mexique et au Kenya. Des documents de planification de la NSA datés de 2013 prévoyaient son utilisation dans d'autres pays.

Les documents fuités par Snowden révèlent également que l'administration Obama est partageuse. Des programmes de coopération avec des gouvernements étrangers sont implémentés pour accroître les capacités de reconnaissance. Cette coopération s'étend notamment à une alliance clandestine des agences de renseignement des États-Unis, du Royaume-Uni, de l'Australie, du Canada et de la Nouvelle-Zélande, qui remonte à la guerre froide et est connue sous le nom de code « Five Eyes » (Cinq Yeux). En outre, au cours des trois premières années d'Obama au pouvoir, le gouvernement américain a payé à l'équivalent britannique de la NSA, les *Government Communications Headquarters* (GCHQ), au moins 150 millions de dollars pour améliorer la surveillance des câbles sous-marins. Ces derniers partent de l'Amérique du Nord et du Sud

et transitent par le Royaume-Uni sur leur chemin vers l'Europe et le Moyen-Orient : le GCHQ est donc dans une position idéale pour y placer des oreilles. Pour passer en revue toutes les données ainsi récoltées, deux cent cinquante analystes de la NSA ont uni leurs forces avec environ trois cents collègues du GCHQ.

L'accélération de la surveillance a nécessité un boom de la construction d'une ampleur sans précédent dans l'histoire du renseignement américain. Le 5 mars 2012, l'« Empereur Alexander » a inauguré ce qui est probablement le plus grand poste d'écoute du monde, situé en Géorgie (l'État américain, pas le pays). À partir de 2013, la NSA a dépensé plus de 300 millions de dollars pour l'agrandissement d'une ancienne usine de fabrication de puces Sony en Californie et sa transformation en poste d'écoute principal de la NSA pour les Caraïbes, l'Amérique centrale et du Sud. Au nord-ouest, un nouveau bâtiment des opérations est construit près de Denver : on y recueille des communications interceptées par les satellites d'espionnage (tels qu'Orion dont il était question plus haut) pour les transmettre à d'autres avant-postes de la NSA. Les États-Unis justifient ces interceptions à l'étranger en les considérant comme des signaux vitaux pour la lutte antiterroriste à travers le monde[91]. La pièce maîtresse de tous ces avant-postes est le site de Bluffdale, dans l'État de l'Utah. Les révélations de Snowden ont montré ce qui y est sauvegardé : e-mails, messages texte, tweets, recherches Google, dossiers financiers, messages Facebook, vidéos YouTube, métadonnées d'appels téléphoniques et de *chat*, *chats* écrits, etc. Certaines zones du complexe contiennent des données considérées comme critiques, tels que les appels et les courriels en provenance et destinés à des membres clés d'Al-Qaïda et de l'organisation État islamique ; d'autres informations ont finalement été effacées pour faire de la place sur les serveurs. Un disque dur externe de taille monstrueuse, en somme.

La réélection d'Obama en 2012 s'est faite après une campagne centrée presque exclusivement sur les questions économiques et

domestiques ; peu d'attention a été accordée à la surveillance et la vie privée. Comme le montrent les révélations de Snowden intervenues quelques mois plus tard, la collecte de données n'a pas ralenti. Cette approche ne semble pourtant pas la plus optimale. Pour reprendre les mots de Tristan Nitot, « *on cherche une aiguille dans une botte de foin* » et pensant y voir plus clair, on continue à augmenter la taille de la botte… Se pose alors la question de savoir comment remédier au problème très complexe du traitement utile de ces données. Dans le sillage des fuites Snowden, des responsables du gouvernement américain ont essayé de justifier la collecte secrète des relevés téléphoniques des Américains en prétendant qu'au moins cinquante menaces ont été évitées grâce à cette information. Aucun exemple précis n'a été cité. L'« Empereur Alexander », quant à lui, a affirmé à plusieurs reprises que « *cinquante-quatre activités distinctes et liées au terrorisme* » avaient été déjouées. Sans aucun exemple concret à l'appui non plus. Le général est d'ailleurs revenu sur cette déclaration plus tard lors de son audition devant le Comité judiciaire du Sénat américain, en citant un seul exemple… La vie privée et la confidentialité des communications ont été totalement compromises sans pour autant que les citoyens y gagnent en sécurité.

En plus de cet échec se pose aussi la question de l'abus d'informations collectées. Les effets vont bien au-delà des violations des libertés constitutionnelles des Américains. La NSA communiquait par exemple régulièrement des interceptions brutes contenant des millions d'appels téléphoniques et de courriels d'Américains ayant de la famille en Israël et Palestine à son homologue israélien, l'Unité 8200[92]. Ce que cette dernière en faisait n'était pas très clair jusqu'à ce que quarante-trois membres de l'Unité 8200 démissionnent de leurs postes. Dans un article publié par le *New York Times*, ceux-ci ont publiquement accusé l'État d'Israël d'utiliser des communications interceptées, telles que celles envoyées par la NSA, pour infliger

une « *persécution politique* » à des Palestiniens innocents[93]. Les démissionnaires ont ainsi expliqué que des données sur l'orientation sexuelle, des infidélités conjugales, des problèmes d'argent, les conditions médicales de la famille, etc. ont été recueillies puis utilisées comme moyens de coercition. Les documents rendus publics par Snowden révèlent aussi les mémos organisant le recueil d'informations pour discréditer des personnes qui posent problème. Ainsi, une note de synthèse précise la nécessité de collecter des données de navigation web et d'utiliser le fait que des gens regardent des films pornos pour saper publiquement leur réputation[94]. Ces agissements rappellent le *kompromat* russe, l'utilisation par un KGB (en reconstruction durant les années folles suivant la chute de l'URSS) de prostituées pour attirer des hommes puissants et/ou riches dans des guets-apens filmés ensuite utilisés pour du chantage.

On peut regretter qu'Obama n'ait pris pratiquement aucune mesure pour limiter cet appareil de surveillance et d'espionnage. Après les révélations de Snowden, le président a appelé à mettre fin à la collecte de métadonnées des appels téléphoniques des citoyens américains effectuée par la NSA. Mais ce ne fut qu'une goutte dans l'océan de l'état de surveillance. Plus troublant encore, l'administration Obama est allée à la chasse des gens qui ont permis de faire la lumière sur les abus des agences de renseignement. Sous Obama[95], huit lanceurs d'alerte ont été poursuivis en justice au motif qu'ils tombaient sous le coup de l'*Espionage Act*, un nombre record pour le pays où cette loi avait été utilisée contre seulement trois personnes avant la présidence d'Obama[96]. En 2013, la presse spécialisée[97] met la main sur des programmes spécifiques du ministère de la Défense américain, qui visent à institutionnaliser une chasse aux sorcières permanente en formant des agents à l'identification de potentiels lanceurs d'alerte.

Depuis le changement d'administration, l'impulsivité de Donald Trump et des efforts intrusifs de membres de son cabinet inquiètent : ils compromettent en effet des personnes risquant

leur carrière et leur intégrité morale pour signaler des dysfonctionnements et des manquements éthiques dans les administrations publiques[47].

LA COURSE À L'ÉCHALOTE...

Il semble donc que des gouvernements se livrent à une véritable course à l'armement d'intrusion numérique. Cette tendance est préoccupante, comme le note un récent rapport de l'ONU[48] :

« Les TIC[49] ouvrent des possibilités immenses pour le développement économique et social et continuent à gagner en importance pour la communauté internationale. L'environnement informatique mondial présente toutefois des tendances préoccupantes, notamment la hausse spectaculaire du nombre d'actes de malveillance dans lesquels des États ou des acteurs non étatiques sont impliqués. »

Cette préoccupation n'est pas sans fondement. Citons à titre d'exemple les révélations de Snowden (oui, encore) qui ont en effet mis en évidence le programme Bullrun. Il s'agit du parte-nariat développé entre le gouvernement américain, géré conjointement par la NSA et le GCHQ, et de nombreux acteurs privés. Les agences de renseignement américaine et britannique collaborent ainsi clandestinement avec des géants du web et des fournisseurs de services ; la mission de ce « partenariat » est d'« *insérer des vulnérabilités dans les systèmes de chiffrement commerciaux* ».

47: Le directeur des SSI de l'État américain fédéral a une position très claire sur l'utilisation généralisée du HTTPS par exemple (https://https.cio.gov/). Ce genre d'incitation/obligation ne semble pas exister en France. Or, il s'agit là du déploiement d'un moyen simple (le protocole de navigation sécurisé HTTPS) aux sites web publics, moyen permettant d'assurer un transport de données sur Internet plus sûr et ainsi plus respectueux des dispositions de protection des données personnelles. On notera à ce sujet des initiatives citoyennes interpelant la CNIL (Commission nationale Informatique et Libertés) sur le manque de HTTPS sur divers sites web y compris d'administrations publiques https://tdelmas.eu/CNIL-001.pdf

48: Rapport du groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, A/70/174, 22 juillet 2015.

49: TIC : Technologies de l'information et de la communication.

Le programme, de loin le plus coûteux financièrement parmi ceux dévoilés par Snowden, exploite diverses approches pour s'introduire abusivement dans les communications des gens : intégrer – dès la conception – des portes dérobées dans les solutions de chiffrement de divers services web, récupérer des certificats de chiffrement ou même entreprendre des cyberattaques ou de l'espionnage à l'encontre de sociétés de services web pour leur voler leurs clés numériques[92]. Ainsi, l'interception et le déchiffrement se font pratiquement en temps réel.

Rappelons-nous aussi une autre facette de la mobilisation de moyens informatiques : les 0days. Acquises par des tiers (États, acteurs privés autres que les créateurs et éditeurs du logiciel concerné), ces vulnérabilités deviennent souvent des armes. Comme nous l'avons vu dans les pages qui précèdent, de plus en plus d'États se dotent de capacités offensives en plus de celles, défensives, dont ils disposent déjà. Si se défendre est rationnel et nul ne saurait s'y opposer, acquérir de l'offensif revient à s'engager dans une course à l'armement. Cet engagement est d'autant plus fort que certains textes de doctrine précisent désormais que les outils numériques peuvent être considérés comme une infrastructure critique/stratégique (et donc, d'importance vitale pour le pays) ou encore qu'une cyberattaque contre des installations vitales peut recevoir une réponse militaire.

Cet emballement n'est pas nouveau : c'est le résultat d'un sentiment d'insécurité face à d'autres États ou à une « menace intérieure ». Plusieurs tensions émergent ici : d'une part, une confusion toujours croissante (et d'autant plus dangereuse) entre le militaire et le policier. En effet, le propre du militaire est d'assure l'intégrité de l'État et ses intérêts face à une menace *extérieure*. C'est à la police que revient de maintenir l'ordre intérieur. En prenant comme prémisse que la menace informatique peut venir de partout, on gomme rapidement ces limitations et on en arrive à une situation où la (prétendue) menace intérieure se confond avec le chaos international. Cette confusion entre ces deux formes de

régulations est toxique. Ainsi, on arrive à définir une autre tension de cette militarisation de l'outil numérique : la diminution du niveau de sécurité générale en tentant d'assurer sa propre sécurité *via* une augmentation du risque de conflit. En effet, revenons à la question évoquée plus haut à propos des élections américaines : comment un État devrait-il réagir face à ce qu'il perçoit comme une ingérence dans ses affaires internes par un autre État par le biais d'intrusions informatiques ?

Avant de parler de régulations internationales et d'approches de maîtrise des armements (numériques), détaillons le rôle significatif de certaines entreprises dans cette situation complexe. Les acteurs privés dans ce domaine sont nombreux. Nous parlerons brièvement de la privatisation de données à caractère personnel par divers acteurs privés – souvent surnommés les GAFAM pour Google, Apple, Facebook, Amazon, Microsoft, et consorts – pour nous intéresser plutôt aux fournisseurs de ce que l'on appelle les technologies à double usage, tels que Hacking Team (voir page 40). Ces technologies (*dual-use* en anglais) sont ainsi qualifiées parce que leur utilisation peut être aussi bien civile (un but légitime et/ou socialement bénéfique) que militaire.

DOUBLE USAGE, DOUBLE JEU

Le développement croissant par les États de capacités offensives est grandement aidé par des acteurs privés. L'utilisation de telles capacités se fait dans divers cadres (conflit armé, renseignement, enquête judiciaire). La sécurité des systèmes informatiques et d'information est un enjeu de sécurité nationale, donc de nombreuses entreprises ont émergé et développé le marché. Celles-là proposent des outils d'intrusion et/ou de compromission, vendent des 0days ou encore des moyens de surveillance et/ou d'interception. Comme on le verra dans le chapitre 03, un écosystème plus large, souvent d'inspiration criminelle, existe aussi fournissant les mêmes services. Les buts de celui qui acquière et utilise ces

outils, indépendamment du fournisseur, sont toujours motivés par l'obtention d'un avantage : commercial, stratégique (par l'espionnage), purement financier, etc.

Mais qui sont ces fournisseurs privés ? Et quels sont les outils qu'ils commercialisent ? Si l'on prend comme exemple les travaux de Citizen Lab, le groupe de recherche canadien, on peut définir deux catégories principales de technologies à double usage : celles qui impliquent la gestion du trafic réseau (comme l'inspection approfondie des paquets et le filtrage de contenu) et celles qui permettent l'intrusion dans des appareils et, ainsi, une surveillance plus ciblée de l'individu – ou de l'organisation – et de ses interactions et communications. La gestion de trafic réseau avec mise en place de restrictions d'accès à des contenus est connue : elle se fait *via* des outils commercialisés par Blue Coat[98], Fortinet, NetSweeper, Qosmos, Bull/Amesys, etc. L'usage civil est ici celui d'une entreprise ou une université qui souhaite empêcher ses employés ou étudiants d'accéder à certains sites web. On peut comprendre que des ressources constituent des distractions sans rapport avec l'activité principale que l'on a à faire dans l'établissement en question. Donc, admettre qu'une entreprise ou une université filtre ne peut se justifier. Cependant, lorsque cette approche est imposée aux fournisseurs d'accès Internet à l'échelle d'un pays, la situation change radicalement : dans ce cas, le gouvernement en place contraint un filtrage appliqué à toute la population au motif que des contenus lui déplaisent. Ces situations sont connues[50] et décrites ainsi que des entreprises qui les fournissent[99].

La deuxième catégorie de technologies à double usage concerne l'utilisation de logiciels d'intrusion. Ceux-là sont

50 : Le document d'identification et de description de cette pratique, par l'initiative OpenNet, avait mis en évidence le commerce de l'Occident vers le Moyen-Orient et l'Afrique du Nord de tels outils : https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

souvent malveillants (le nom générique est *malwares*) et sont présentés comme moyen d'interception légale. Nous avons déjà abordé les *exploits* 0day ; il existe aussi des chevaux de Troie (des *Trojans* en anglais) qui permettent, *via* une porte dérobée[51], un accès à distance et la surveillance de l'appareil d'un utilisateur. Les recherches dans ce cas ressemblent à celles faites en épidémiologie : on cherche le « patient zéro », à savoir la première occurrence d'utilisation de la technologie sur une cible. Cette dernière peut avoir reçu un e-mail avec une pièce jointe vérolée ou l'invitant à cliquer sur une URL qui active l'installation du *spyware* sur la machine. La société italienne Hacking Team est l'un des exemples les mieux connus (en raison du « hacker » connu comme Phineas Fisher qui a compromis Hacking Team[52] et rendu publics des documents et échanges e-mails très instructifs) ; mais il y a également FinFisher, NSO Group, Procera Networks[100], etc.

Quels cas sont aujourd'hui répertoriés ? On peut citer la mobilisation de pas moins de trois 0days (!) identifiés dans le système d'exploitation des téléphones iPhone pour cibler un opposant de longue date aux Émirats arabes unis[101]. L'entreprise ayant développé le malware, l'israélienne NSO Group, s'est également illustrée en le déployant pour cibler un journaliste d'investigation mexicain. Procera Networks, domiciliée aux États-Unis, a quant à elle un contrat avec le fournisseur turc Türk Telecom selon lequel les outils développés par la société américaine servent à intercepter des identifiants et mots de passe, à collecter les IP desquelles chaque connexion émane et les sites web visités par chaque IP. Ces agissements ont été révélés lorsque des ingénieurs de Procera ont démissionné avec fracas pour dénoncer la contribution significative de leur employeur dans ce qui a les allures

51 : Fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel.

52 : http://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/

d'une purge à échelle nationale en Turquie[53]. Le mode de fonctionnement du logiciel de Procera rappelle celui de la NSA, nommé XKEYSCORE et abondamment décrit dans les documents fuités par Snowden[102]. L'approche de Procera déployée par Türk Telekom est puissante : un outil dédié suit le trafic réseau en temps réel et toute connexion en HTTP (*e.g.*, une identification d'e-mail en clair) est redirigée vers un autre outil. Ce dernier analyse les données pour en extraire les identifiants, mots de passe, IP, sites visités, etc. Ces données sont ensuite croisées avec la base client de Türk Telekom. Cet opérateur se vante d'avoir pratiquement 20 millions de clients de téléphonie mobile, pas loin de 10 millions de clients 3G/4G et d'être le plus grand fournisseur d'accès Internet gérant jusqu'à 80 % de l'équipement en fibre optique du pays. L'ampleur de la surveillance en jeu est gigantesque (on ne le répétera jamais assez : privilégiez, lorsque possible, les connexions en HTTPS).

L'approche surprend et met mal à l'aise. On peut bien sûr chercher la raison socialement utile qui ferait qu'une telle surveillance de la population serait bénéfique, et non pas intrusive et prétexte à répression. La raison officielle de l'interception opérée par Procera est la lutte contre la fraude. Assez ténu comme justification : connaissez-vous des cas d'enquête où une partie conséquente de la population d'un pays voit ses données de navigation web recueillies par un acteur privé dont le mandat légal pour ce faire n'est pas clair ? Les ingénieurs de Procera ayant révélé le pot aux roses avec leurs démissions ont trouvé la justification « fraude » très faible aussi. En effet, prétendre déployer une surveillance massive des communications électroniques de

53 : Citons quelques exemples pour illustrer : un ado de 14 ans s'est retrouvé à subir une peine de prison pour avoir critiqué le président Erdogan sur Facebook (https://news.vice.com/article/teen-arrested-for-insulting-erdogan-on-facebook-as-crackdown-in-turkey-continues) ; un médecin risque une peine de prison après avoir comparé des expressions faciales d'Erdogan avec celles d'un personnage de fiction (https://www.theguardian.com/world/2016/jun/23/rifat-cetin-erdogan-gollum-suspended-sentence-turkey) ; une répression dépassant toute commune mesure a cours, ainsi plus de 15 000 employés de l'Éducation sont détenus car suspectés d'avoir contribué à fomenter le coup d'état de l'été 2016 (http://www.reuters.com/article/us-turkey-security-education-idUSKCN0ZZ1R9) ; etc.

la population dans un cadre légal particulièrement opaque pour lutter contre la fraude est une première : aucun autre cas de ce genre ne semble documenté de façon publiquement accessible. Mais plus encore, une telle approche risque d'être infructueuse. En effet, on monitore et analyse des types d'activités spécifiques liées à la fraude ; les outils de détection doivent être construits pour caractériser ces activités. On pourrait spéculer sur la pertinence d'une telle approche dans un cas de fraude fiscale généralisée. Mais le cas turc laisse dubitatif : d'après les données de l'ITU[54] pour 2015, seulement 54 % de la population du pays utilise Internet[103], soit presque 41 millions de personnes. Quant aux usages de banques en ligne[104], on constate que seules 18 millions personnes ont utilisé de tels services en 2015 (21 millions fin 2016). La justification semble donc tirée par les cheveux et improbable, ce qui laisse comme seule conclusion plausible la contribution de Procera à une surveillance et un recueil abusif de données à caractère personnel appliqués à la population turque.

Autre fait troublant : aussi bien Procera que NSO Group font partie des entreprises pour lesquelles un fonds d'investissement, Francisco Partners, a des espoirs de profits financiers. Outre ces deux sociétés et Blue Coat, Francisco Partners a également investi dans Ability Inc., une autre société israélienne qui se spécialise dans l'« *interception illimitée* » des communications téléphoniques[105]. Ability Inc. se propose d'intercepter et de collecter les communications audio et texte de n'importe quel téléphone portable à partir du moment où vous disposez de son identifiant, l'IMSI. Acronyme de *International Mobile Subscriber Identity* – « identifiant international d'abonnement mobile » – ce numéro est unique pour chaque téléphone. Des engins appelés *IMSI-catchers* permettent de récupérer ce numéro. Si ces engins sont déjà déployés dans certains pays (police new-yorkaise[106] par exemple), leur portée n'est que très locale et soumise aux restrictions géographiques

54 : Union internationale des communications.

légales en vigueur. Les outils d'Ability Inc. ne s'embarrassent pas de ce genre de limitations et leur utilisation n'exige pas d'obtenir l'aval des opérateurs de téléphonie[107].

ON N'EST PAS SORTIS DE L'AUBERGE...

Ces quelques exemples permettent de mieux appréhender les abus que certains usages peuvent représenter[55]. On pourrait également se demander quel est le cadre légal de ces activités. D'une part, il est très difficile de définir ce qu'est une « arme informatique » : parle-t-on de moyens numériques d'influence informationnelle ? D'outils malveillants (offensifs donc) permettant l'intrusion et/ou la compromission de systèmes stratégiques ? Comment définir des choses à restreindre dont on peut en réalité se servir pour défendre nos intérêts ? À l'heure actuelle, il n'existe pas de consensus à propos d'une définition unitaire. D'autre part, la prépondérance d'acteurs privés est une difficulté supplémentaire dans l'établissement d'un tel cadre. En effet, les acteurs du droit international sont traditionnellement les États et les organisations internationales, non pas les individus. Depuis quelques années, divers États se saisissent de la question et promeuvent des règles et codes de conduite visant à restreindre, voire arrêter, la prolifération des « armes informatiques ». Malheureusement, leur respect est tout à fait optionnel. Ce qui est cependant important – et on en revient au rôle de l'État – est que ces technologies sont le plus souvent soumises à des autorisations (ou licences) d'export[56].

55 : Voir par exemple la base de données très complète et maintenue par l'ONG Privacy International des entreprises commercialisant des technologies à double usage : https://sii.transparencytoolkit.org/

56 : En France comme dans les autres États membres de l'UE, le règlement communautaire CE n°428/2009 du 5 mai 2009 modifié définit notamment les différents types de licence à l'exportation et fixe la liste des biens concernés. Ainsi, des contrôles s'appliquent à toutes les exportations vers des territoires hors UE. À l'exception de certains biens très sensibles inscrits sur une liste spécifique, les transferts au sein du territoire communautaire ne sont pas soumis à ces contrôles. Voir http://www.douane.gouv.fr/articles/a10922-biens-et-technologies-a-double-usage-civil-ou-militaire

Parlons brièvement de l'outil réglementaire le plus pertinent dans notre cas : l'Arrangement de Wassenaar[108]. Pour reprendre le langage dédié, il s'agit d'un régime multilatéral de contrôle des exportations mis en place par divers pays afin de coordonner leurs politiques en matière d'exportations d'armements conventionnels et de biens et technologies à double usage. L'Arrangement a été mis sur pied en décembre 1995 mais a été modifié à diverses reprises depuis. Les scandales sur la vente, par divers acteurs privés, de solutions de surveillance à des États qui ont peu de respect pour les droits fondamentaux de leurs citoyens ont émaillé l'actualité, notamment ces cinq dernières années. Tous les exemples mentionnés plus ou moins longuement dans les pages précédentes, qu'ils soient relatifs à la surveillance ou à l'usage de 0days, ont enrichi la réflexion sur l'évolution de l'Arrangement. Celui-ci vient en complément du droit international et de ses outils *via* lesquels les États peuvent endiguer la prolifération de certaines armes (notamment conventionnelles). Depuis 2013 notamment, la liste des technologies à double usage a été modifiée et augmentée pour inclure des outils malveillants, plus particulièrement les logiciels d'intrusion et les systèmes de surveillance du réseau[57]. Précisons que l'expression « logiciels d'intrusion » indique ici les outils spécialement conçus pour contourner les défenses d'un système, y accéder et en extraire des données. Ainsi, l'Arrangement ne comprend pas directement les portes dérobées, les malwares type virus[58] ni les *exploits*[59].

Il ne semble pas y avoir d'évaluation de la mise en œuvre de telles normes. De même, il ne semble pas exister une évaluation

57 : The Wassenaar Arrangement, List of dual-use goods and technologies and munitions list, WA-LIST (15) 1 Corr.1*, 4 avril 2016.
58 : Des approches complémentaires existent, notamment des recours à des normes de comportement responsables des États. On ne s'y arrêtera pas, d'autant plus qu'elles ne sont pas contraignantes, leur portée est donc limitée. Leur but est de sensibiliser à la prolifération d'outils informatiques malveillants et leurs usages.
59 : Encore plus précisément, le contrôle s'applique seulement aux technologies qui permettent la gestion, la création, la délivrance et la communication avec ces logiciels d'intrusion.

de la pertinence d'octroi des licences à l'export de telles technologies. Certains pays, tels que le Canada, publient des statistiques[109], mais le niveau de détail reste insuffisant pour savoir quels outils en particulier ont obtenu des licences ou encore quelles considérations ont été prises en compte pour ce faire. Cela paraît d'autant plus important que, dans le cas canadien pour 2015 par exemple, 2 202 demandes de licences ont été accordées, alors que seulement deux ont été refusées. Si l'on reprend le cas de Procera, un autre point significatif émerge : l'adéquation de la solution technique au problème. Ne serait-on pas face là à l'équivalent numérique de l'utilisation d'un bazooka pour dégommer une mouche. Dans le cadre de l'export d'une technologie pour en faire usage sur le territoire d'un autre pays, le processus d'autorisation doit être correctement calibré pour répondre aux besoins des utilisateurs et aux utilisations finales en prenant en compte les dérives possibles. En effet, les processus d'octroi de licences laissent beaucoup à désirer depuis 2013, que ce soit dans le cas de Procera, de Hacking Team ou de NSO Group. Ainsi par exemple, les autorités italiennes ont approuvé une « *autorisation globale* » à l'export pour les produits logiciels de Hacking Team alors que la participation de l'entreprise à la surveillance et à la répression de journalistes au Maroc était connue[60]. Cette « *autorisation globale* » est pratiquement une carte blanche d'export d'après le même ministère qui l'a délivrée[110], licence qui a permis à Hacking Team d'exporter son *spyware* vers des destinations telles que le Kazakhstan[61]. De même, les autorités israéliennes, et notamment le ministre de la Défense, ont autorisé NSO Group à exporter ses *exploits* 0days pour iPhone sophistiqués aux Émirats arabes unis, où ils ont ensuite été utilisés contre un opposant pacifique[111].

60 : Comme on le voit à partir des e-mails fuités après la compromission de Hacking Team, l'entreprise a obtenu un tel succès suite à un lobbying très intense. https://wikileaks.org/hackingteam/emails/?q=MISE&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult

61 : Cette autorisation a été révoquée en avril 2016 (http://www.ilfattoquotidiano.it/2016/04/06/hacking-team-revocata-lautorizzazione-globale-allexport-del-software-spia-stop-anche-per-legitto-dopo-il-caso-regeni/2610721/).

Beaucoup reste encore à faire pour rétablir et garantir la confiance mais également pour contribuer à endiguer les mésusages de l'outil numérique. Les développements américains abordés le démontrent : promulguer des lois abusives en dilapidant l'argent du contribuable pour un résultat quasi nul n'est pas un exemple à suivre. La prééminence du contrôle sur les libertés n'a pas à être une fatalité.

03

LA QUESTION DE LA CONFIANCE À L'HEURE DU NUMÉRIQUE

LE LOGICIEL LIBRE : UNE NÉCESSITÉ, MAIS PAS UNE PANACÉE

On parlera davantage du logiciel libre et open source dans le chapitre 02 car son émergence participe à celle d'une éthique hacker. Définissons-le brièvement ici, afin de pouvoir discuter sereinement de son impact sur la confiance à l'ère du numérique. Le logiciel libre préserve les quatre libertés fondamentales de son utilisateur : il lui permet de connaître le fonctionnement du code (ouvert), de le modifier, de le partager et d'en faire des dérivés. Cette vision est diamétralement opposée aux logiciels à code fermé, véritables boîtes noires dont le fonctionnement relève de la magie, et qui excluent l'utilisateur de l'équation. Par opposition, ces logiciels sont qualifiés par certains de « privateurs » pour indiquer qu'ils privent l'utilisateur des libertés fondamentales assurées par le logiciel libre. Dans l'esprit du logiciel libre, la règle de base est de toujours pouvoir modifier un logiciel pour en faire un autre. Pour éviter que le nouveau ne se transforme en une boîte noire et que l'éthique soit ainsi pervertie, le projet GNU a défini des règles légales.

En 2017, le logiciel libre est partout. Des langages de programmation, des infrastructures sous-tendant le réseau Internet ou ses couches web à votre téléphone mobile ou votre lave-vaisselle. Alors

qu'il y a dix ans, les défenseurs du logiciel libre et open source faisaient des pieds et des mains pour son adoption large, aujourd'hui c'est chose faite. Mais est-on pour autant un utilisateur plus libre ? Malheureusement, il n'en est rien :

« On brandit en permanence le logiciel libre à bout de bras comme étant THE solution, le Graal, la balle en argent ou le marteau doré. Alors que cette propriété n'apporte en réalité plus aucune protection. […]

Le logiciel libre est mort. Vive la gouvernance éthique.

Le détail qui fait la différence ? La gouvernance et la confiance. Certainement pas la licence libre du logiciel. »[112]

Et cette bataille-là, pour la gouvernance dont le logiciel libre et open source est une composante, sera nettement plus difficile à remporter. Abordons-la à travers deux exemples : le trucage des émissions de polluants par Volkswagen (le fameux #DieselGate) et le vote électronique.

#DIESELGATE : LES YEUX DANS LES YEUX AVEC VOTRE VOITURE

Septembre 2015. Les représentants de Volkswagen, livides, tentent d'étouffer l'un des plus gros scandales industriels du XXIe siècle : l'agence américaine de protection de l'environnement vient d'annoncer que le constructeur automobile allemand a truqué les émissions de polluants de certaines de ses voitures diesel et essence pendant des années[113]. Non seulement les amendes pourraient atteindre des sommes record (18 milliards de dollars) mais le ministère américain de la Justice annonce que certains faits pourraient être qualifiés pénalement[114]. Volkswagen a également confirmé qu'environ 11 millions de voitures diesel vendues majoritairement en Europe sont équipées de logiciels dont le but est de truquer les émissions[115]. L'action dévisse en bourse, le P.-D.G.

démissionne, honteux, le consommateur est en état de choc et le stéréotype allemand de droiture et rigueur est écorné.

Deux questions se posent : d'abord, pourquoi Volkswagen a-t-il eu besoin de mentir ? Et ensuite, comment ces trucages ont-ils passé les commissions d'évaluation de nombreux pays ?

La motivation de ce mensonge à échelle industrielle est relativement simple à comprendre : en 2015, Volkswagen souhaite devenir le premier constructeur automobile mondial de l'année. La société doit donc dépasser Toyota. Pour y arriver, Volkswagen a (entre autres) à s'attaquer au marché américain. Or, le moteur diesel contribue au rejet d'une quantité élevée de NOx (oxydes d'azote), l'un des composants principaux de la pollution de l'air avec les particules fines. Comparé au moteur essence, le diesel est plus polluant en matière d'émission de NOx. En Europe, les réglementations concernant les émissions de NOx ont été assez arrangeantes pendant des années, donc les voitures diesel ont énormément gagné en popularité. (On ne s'étonne guère de constater les épisodes de pollution aux particules fines en France par exemple, où les voitures diesel constituent une proportion importante du parc automobile en activité dans le pays.) Mais les standards relatifs aux émissions de NOx aux États-Unis sont beaucoup plus contraignants[116], ce qui réduit les possibilités d'importation de voitures diesel. L'un des arguments de vente les plus efficaces devient alors le « gasoil propre » (*clean diesel fuel),* un carburant alimentant un moteur plus efficace, le tout étant censé produire moins de CO2 et permettre de faire davantage de kilomètres avec un litre de carburant que le moteur essence. À partir de 2009, la réglementation américaine est assouplie en grande partie en réponse à cette évolution significative de la composition du carburant[117]. Volkswagen est donc en mesure de conquérir le marché américain. Entre 2009 et 2015, ce seront environ 500 000 voitures diesel appartenant à diverses marques du constructeur qui seront vendues aux États-Unis.

Le problème est que le « diesel propre » version Volkswagen n'en est pas un. Des instituts de recherche sur l'environnement ont produit dès 2014 des études très concluantes sur les différences significatives d'émissions NOx entre les voitures Volkswagen testées en laboratoire et les véhicules roulant sur les routes européennes[118]. Des collaborations avec diverses universités américaines ont permis de recueillir des résultats supplémentaires. La conclusion est sans appel : les émissions de NOx des voitures sur la route sont jusqu'à quarante fois supérieures aux tests fournis par Volkswagen en fonction du modèle du véhicule considéré. Face à la menace de l'Agence américaine de protection de l'environnement de mettre un véto à la vente des voitures diesel de Volkswagen en 2016, le constructeur a fini par reconnaître qu'il y avait eu trucage. Des experts supposent que la raison à ce trucage est l'incapacité de Volkswagen à parvenir à un compromis optimal entre basses émissions (nécessaires pour satisfaire aux exigences de la réglementation) et kilomètres parcourus au litre[119].

Quel rapport avec l'informatique, vous demandez-vous ? Les émissions sont le résultat et la partie visible de l'iceberg. Pour savoir comment ces résultats fabriqués ont pu être produits, on devrait s'intéresser à qui – ou plutôt quoi – les a produits. Dans le cas du #DieselGate, le débat s'est majoritairement concentré sur les tests, prévisibles, que les voitures suivent pour établir les niveaux d'émissions. Cependant, c'est bien l'ensemble des logiciels embarqués qui est la vraie cause de ces tricheries. Dans le rapport de l'Agence américaine de protection de l'environnement qui a ébruité le trucage, il est clairement indiqué que Volkswagen introduit de manière systématique des sous-programmes gérant on ne sait comment le frottement et les mouvements des pédales. Ainsi, lorsque les tests « suggèrent » que la voiture est évaluée sur ses émissions de NOx, les programmes en question en changent le comportement pour constater des émissions dans les niveaux requis… Ces mêmes programmes ne semblent pas s'activer le reste du temps. Ces comportements informatiques ont été admis par Volkswagen[120].

LE LOGICIEL LIBRE N'EST PAS UN CAPRICE

La discussion sur la nécessité d'avoir un logiciel dont le code est ouvert s'avère là d'autant plus nécessaire. En effet, aucun des tests sur les émissions n'inclut d'audit logiciel. Le #DieselGate est un exemple flagrant des limites de la confiance octroyée à des boîtes noires sur la simple promesse de bonne foi. Cette question ne se pose pas seulement pour les voitures diesel : on parle presque quotidiennement de la mise en circulation de voitures sans chauffeur. Aucune mesure tangible n'a été proposée, par aucun législateur, quant à un accès ouvert au code et aux algorithmes qui gouvernent le fonctionnement de ces machines. Lors de simulations de gestion de crise pour des entreprises du secteur, crise provoquée par un accident dont le responsable est une voiture autonome, l'un des scénarios impliquait les répercussions d'un accident : la voiture autonome n'a pas de dysfonctionnement logiciel, mais fait un choix d'après son algorithme et percute un bus scolaire pour éviter de tuer ses passagers. Le choix implicite dans ce cas est clair : protéger ses passagers avant tout, quitte à causer davantage de morts ou de blessés. D'autres scénarios impliquent le choix entre le nombre final de morts ou blessés, dont les passagers du véhicule autonome. Chacun de ces cas correspond à une programmation normale de la voiture et non pas à un dysfonctionnement. Alors, vous êtes plutôt pour rester en vie et percuter un bus scolaire ou causer dix blessés et pas douze ?

Ainsi, lorsque de nombreuses personnes se prononcent avec véhémence en faveur du logiciel libre et open source, ce n'est pas par pure lubie ou désir d'embêter leur monde. Au-delà des considérations légales et éthiques (choisir de tricher et empoisonner l'air ou non ; de blesser/tuer certains plutôt que d'autres), la question se pose avec force : dans quelle mesure peut-on avoir confiance en la technologie dans notre quotidien ? Beaucoup ont vu dans le #DieselGate une opportunité de renforcer leur plaidoirie en faveur du logiciel libre et open source dans l'industrie automobile[121].

Les actions n'ont pas été au rendez-vous pour autant. Reste à espérer qu'un jugement futur dans l'affaire en cours avec Volkswagen offrira une motivation suffisante.

Mais la mesure des émissions de polluants n'est pas le seul domaine qui fait pencher la balance en faveur du logiciel libre et open source dans nos objets quotidiens. Vous avez probablement entendu parler de voitures compromises à distance, *via* leurs connexions sans fil comme l'énorme Jeep Cherokee[123] ou l'élégante Tesla[122]. Si vous avez des enfants, vous avez peut-être eu peur à l'annonce que la Barbie connectée au WiFi peut aussi être compromise[124]. Des babyphones connectés à Internet sans fil ne résistent pas non plus à l'intrusion[125]. Votre frigo connecté qui faisait les courses à votre place laissait les identifiants et mots de passe de vos comptes Gmail voyager en clair[126]. Les chercheurs en sécurité informatique Runa Sandvik et Michael Auger ont pu détourner un fusil de précision que quelqu'un avait eu la brillante idée de connecter au WiFi[127] (c'est vrai que c'est primordial pour une arme à feu !). Les « maisons intelligentes » (parce que connectées à Internet) ont aussi été décriées comme un désastre informatique en devenir[128]. Des procédures sont en cours entre une entreprise commercialisant des pacemakers et une société de sécurité informatique ayant démontré de nombreux problèmes sérieux avec la sécurité des implants cardiaques[129]. Et si vous soupirez avec soulagement en pensant à vos sex-toys, détrompez-vous : deux modèles connectés ont déjà été commercialisés… et compromis. Dans un des cas, la compromission a démontré que l'entreprise commercialisant l'objet recueille des données très sensibles grâce à cette connexion (qui remonte les données d'utilisation en temps réel, à l'insu de son utilisateur) ; éthiquement et légalement, c'est discutable, mais rappelons le risque supplémentaire de voir ses données volées. Une utilisatrice du sex-toy connecté incriminé a intenté un procès à l'entreprise suite à ces révélations[130]. De très nombreux problèmes auraient ainsi pu être évités (ainsi que leurs répercussions morales et financières entre autres) si le code avait été ouvert et audité par la majorité.

LE VOTE ÉLECTRONIQUE : UNE FAUSSE SOLUTION À UN PROBLÈME QUI N'EXISTE PAS

Si ouvrir le code de nos voitures et autres objets du quotidien peut être une solution à énormément de problèmes, voici un cas où il est souvent pointé comme tel, à tort : le vote électronique. Nous avons choisi ce cas parce qu'exercer ses droits civiques ne devrait pas être une question de confort ou de compromis douteux.

De temps à autre, une actualité en lien avec le vote électronique apparaît dans les médias et relance le débat sur la pertinence d'une généralisation de celui-ci[131]. Abordons donc la question d'une solution technique à un problème de gouvernance : peut-on faire confiance aux ordinateurs et à l'informatique pour l'élection des représentants du peuple ? Est-ce que le vote électronique généralisé (entraînant la disparition du vote papier) permettra de « débloquer » notre démocratie cahotante ?

Pour pouvoir répondre à ces questions, il faudrait bien comprendre l'impact d'un remplacement du papier par des ordinateurs et Internet. Et en y regardant de plus près, les fondamentaux même du vote s'en retrouvent déstabilisés, voire remis en cause. Ainsi, le vote papier est simple, facile à expliquer à n'importe quel citoyen, difficile à tracer et à corrompre. Il peut paraître à certains que « facile à expliquer à n'importe qui » est secondaire. Bien au contraire ! Comment voulez-vous assurer à toute personne une égale participation à la vie publique et à la gouvernance si certains s'en trouvent écartés par manque de connaissance ou par incapacité technique de voter ? La facilité d'exécution par tout un chacun vient ainsi s'ajouter à la nécessité d'avoir un processus transparent et vérifiable par le citoyen. Dans le cas du vote papier, toutes ces conditions sont réunies : on peut expliquer à un enfant de 5 ans comme à n'importe quel individu qu'il faut entrer dans l'isoloir, choisir son candidat, mettre le bulletin dans l'enveloppe, ressortir, mettre dans l'urne et émarger. Tout le monde peut faire assesseur et s'assurer que les gens qui émargent

sont bien inscrits sur une liste électorale. Et comme l'urne est transparente, on ne peut pas « accidentellement » y mettre plein de bulletins qui viendraient, pur hasard, favoriser largement un candidat plutôt qu'un autre.

Regardons comment ces conditions se vérifient dans le cas du vote électronique. Ce dernier englobe les modalités du vote par ordinateur (appelé machine à voter) et par Internet. Prenons seulement le vote électronique pour l'instant, le vote par Internet est surtout une solution de remplacement mise en place pour les Français à l'étranger mais n'a pas pour vocation à se substituer de façon généralisée au vote papier. Or, en France, il existe de nombreuses communes où le vote électronique est la seule option possible. Donc, afin de pouvoir avoir un système de vote électronique qui soit aussi respectueux des prérequis fondamentaux du vote papier, il nous faudrait pouvoir garantir :

- Que le logiciel fasse ce que l'on attend de lui ;
- Que le logiciel ne soit pas corrompu ;
- Que le matériel fasse ce que l'on attend de lui ;
- Que le matériel ne soit pas corrompu et soit conforme aux exigences légales ;
- Que le logiciel et le matériel soient ceux prévus et audités en amont ;
- Que personne ne soit capable, et à aucun moment avant, pendant ou après le vote, de modifier le système (logiciel et matériel) et les données associées ;
- Que personne ne puisse établir de lien entre les votes exprimés et les personnes ayant voté ;
- Que tout citoyen puisse comprendre chacune des étapes et des technologies mises en jeu dans la procédure de vote.

« Le vote par Internet a ses problématiques propres. »

Benoît Sibaud, expert vote électronique

RS : Qui es-tu et comment es-tu tombé dans le vote électronique ?

BS : J'ai une formation d'ingénieur en informatique. Professionnellement, j'ai été développeur, avant de me tourner vers le domaine de l'intégration et du test de solutions logicielles. Je suis actif dans le milieu associatif et militant dans le domaine du logiciel libre, à la fois d'un point de vue technique mais aussi politique (au sens vie de la cité, indépendamment de la politique mandataire, des partis). Je suis par exemple un des webmestres du site d'actualités LinuxFr.org depuis dix-sept ans et j'ai été administrateur de l'April (association de promotion et de défense du logiciel libre) pendant dix ans (dont cinq ans de présidence). Autrement dit, je baigne dans les questions liées au numérique, aux libertés et à la politique.

Je me suis intéressé au vote électronique via les libristes : l'affaire dite « du 13e bit belge » en 2003 a été évoquée sur une liste de discussion liée au logiciel libre[1]. Il s'agissait d'une erreur de 4096 votants lors d'un vote électronique en Belgique, due a priori à une erreur informatique. C'était au début un simple sujet d'intérêt. Puis la ville où je réside, Issy-les-Moulineaux, a fait le choix en 2006 de passer au 100 % de vote électronique par machines à voter (des ordinateurs de vote) pour les élections institutionnelles. J'ai suivi le sujet depuis, essayant de montrer les limites et les problèmes posés par

1 : http://fsffrance.org/news/article2003-07-11.fr.html

le vote électronique dans ce cadre-là. J'ai écrit à mon maire comme simple citoyen, publié divers documents relatant mon expérience dans les bureaux de vote[2], participé (pour l'April) au sein du Forum des Droits sur Internet à un groupe de travail[3] sur le vote électronique en 2007 et en 2008, collecté les procès-verbaux des différents scrutins de la ville, etc.[4]

En parallèle, j'ai été confronté plusieurs fois à des scrutins non institutionnels en vote par Internet : les élections de conseil de quartiers à Issy-les-Moulineaux, les élections associatives de l'April, des élections professionnelles, des élections d'assemblées générales d'entreprise, etc.

Mes actions précédentes m'ont permis d'être délégué lors du vote par Internet pour les Français de l'étranger lors des élections législatives de 2012 et 2013, donc d'assister aux réunions préparatoires du « bureau de vote électronique (BVE) » au Ministère des Affaires étrangères et européennes et aux dépouillements.

Dans toutes ces actions, j'ai veillé à agir en tant que citoyen, à être assesseur/délégué pour divers partis (MoDem, PS, Parti Pirate) pour ne pas être étiqueté, et à rester dans l'argumentation, la publication d'informations étayées et le partage d'expérience.

RS : De ton expérience en tant qu'assesseur et délégué lors d'un vote par Internet, quels sont tes retours de terrain ?

BS : Les aspects les plus terre à terre sont rapidement apparus. La mise en place du vote par ordinateurs de vote

2 : http://oumph.free.fr/textes/vote_electronique_issy.html
3 : http://www.april.org/groupes/fdi/groupes/fdi/gdt-vote-electronique
4 : https://fr.wikipedia.org/wiki/Vote_électronique (d'ailleurs illustré par une de mes photos)

a été un choix politique mis en place dans la précipitation, sans vrai débat, et malgré les avertissements des experts techniques mais aussi de juristes. On a donc un code électoral bricolé à la va-vite[5] et des solutions techniques souffrant de problèmes basiques[6] : les scrutins n'intéressent le législateur et les vendeurs de solution qu'en période électorale, personne n'investit du temps ou de l'argent en période calme, et de toute façon le marché est petit (les scrutins sont peu nombreux) et fragmenté (chaque pays a son code électoral, sa langue, ses contraintes propres). Rappelons juste que l'évolution électorale est itérative et finalement plutôt lente : pour la France, vote des femmes en 1944, urne transparente en 1988, règles de financement des partis en 1990, prise en compte de la diaspora pour l'Assemblée en 2008 et du vote blanc en 2014.

Mais derrière les basses questions techniques apparaissent des questions bien plus fondamentales, démocratiquement parlant. Un des points essentiels autour du vote électronique, par ordinateurs de vote ou par Internet, est la

5 : Deux exemples :
– Le code électoral exige une urne unique par bureau de vote et un isoloir pour 300 électeurs dans des bureaux de vote d'environ un millier d'électeurs ; or, un ordinateur de vote est une urne et un isoloir.
– Décret n° 2014-290 du 4 mars 2014 portant dispositions électorales relatives à la représentation des Français établis hors de France : les critères pour les délégués pour le vote papier ou pour les ordinateurs de vote (électeur du département, pas de restriction pour le parti) ne sont pas les mêmes que ceux pour le vote par Internet (n'importe qui, mais le parti doit se présenter dans au moins trois circonscriptions), créant ainsi deux classes de citoyens et de partis.

6 : Deux exemples montrent que certains tests simples n'ont pas été faits :
- Les ordinateurs de vote américains ES&S iVotronic utilisés à Issy-les-Moulineaux gèrent mal les accents et la datation d'ouverture/fermeture du bureau de vote (« Ouvert 65516:65525:65502 64800/01/1994 »). Sans parler du fait que les codes de sécurité sont constants et publics (la date du référendum sur le traité de constitution européenne de 2005).
- La solution espagnole Scytl de vote par Internet utilisée pour les législatives en 2012 a été le premier cas de vote nul (jusqu'alors considéré impossible en vote électronique) : un électeur a réussi à voter au second tour pour un candidat éliminé au premier tour, bloquant le décompte du second tour et obligeant à recourir à une seconde procédure (*sic*) de comptage.

fausse impression de simplicité que tout un chacun a initialement sur le sujet. L'Homme est allé sur la Lune, a des distributeurs bancaires et des voitures qui se conduisent toutes seules, ça ne doit pas être bien plus compliqué. Sauf que pour le vote électronique, les contraintes sont nombreuses : il faut assurer le secret du vote, éviter la possibilité de prouver pour qui l'on a voté (et donc de vendre son vote), empêcher de relier l'électeur à son bulletin, respecter la codification du code électoral, permettre de s'assurer de la sincérité du scrutin, être facilement utilisable par l'électeur, etc.

Et ces contraintes vont rendre impossible certaines caractéristiques existant avec le scrutin papier : ce dernier est explicable facilement à un enfant. Bulletin, enveloppe, urne, assesseurs et scrutateurs, décompte, etc. C'est simple à expliquer (pourquoi chaque étape est ainsi) et abordable par les sens (des objets palpables, une enveloppe suivie des yeux dans une urne transparente, etc.). A contrario, le vote électronique est accompagné de la dématérialisation (impossible de voir les électrons migrer dans l'ordinateur ou les photons se déplacer dans la fibre optique, impossible de percevoir ce que fait réellement l'ordinateur, fait-il ce qu'il faut, juste ce qu'il faut ?).

Et il amène aussi une monstrueuse complexité en termes de connaissances, obligeant à faire confiance à des experts (physique des semi-conducteurs, électronique, informatique, cryptologie, télécommunication et réseaux...) pas seulement hors de portée d'un enfant ou d'un électeur, mais aussi de tout expert pris individuellement. Comment l'électeur va-t-il s'assurer de la sincérité du scrutin ? Et l'assesseur ? Et le scrutateur ? Quelle confiance vont-ils avoir dans ce fondement de la démocratie ? Que penser de la citation du rapport d'un

expert observant un vote pour l'Assemblée des Français de l'étranger en 2006 : « [les assesseurs] ont pu voir en permanence, sur un écran, l'image d'une salle informatique dans laquelle des ordinateurs fonctionnaient »[7] ?

De fait les contraintes précédemment évoquées sont contradictoires : il n'est pas possible[8] d'avoir à la fois un scrutin qui soit à bulletin secret, explicable à tous (avec une vraie compréhension) et vérifiable par les électeurs. Le vote électronique impose donc des choix, et actuellement, en France et sur les scrutins institutionnels, il se fait sans être explicable à tous et sans être vérifiable.

RS : On entend beaucoup que le vote électronique, c'est plus moderne et moins cher. Qu'en est-il ? Et quelles évolutions en France ?

BS : Pour mémoire, le vote électronique ne modifie en rien la campagne électorale ou la gestion de la liste électorale, il modifie uniquement la partie scrutin et dépouillement.

Le vote par ordinateurs de vote (institutionnel) est en sursis en France, après un rapport d'information du Sénat en 2014 qui parlait de « régler le sort des machines à voter »[9], un moratoire des agréments pour les machines (toujours les trois mêmes solutions depuis 2007) et pas de nouvelles autorisations pour les communes. Le déclin est perceptible avec un passage de 83 communes et 1,5 million d'électeurs en 2007

7 : http://www.ordinateurs-de-vote.org/IMG/pdf/rapport_pellegrini.pdf
8 : En l'état actuel des connaissances, mais il paraît difficile de voir comment il pourrait en être autrement, sauf à rendre nos sens capables de percer la dématérialisation et à rendre chaque électeur expert multi-domaines. Sans parler du secret industriel commercial opposé par les fabricants.
9 : http://w3.observatoire-du-vote.eu/ressources/Documents%20en%20acc%C3%A8s%20libre/r13-4451.pdf

à 66 communes et 1 million d'électeurs en 2014. Techniquement, la « modernité » évoquée en a pris un coup puisqu'il s'agit de vieux ordinateurs de plus de dix ans, sans mises à jour logicielles ou matérielles, avec des failles connues et publiées, et interdits dans divers pays (dont leurs pays d'origine).

Ils sont aussi générateurs de files d'attente plus longues (interface lente, découverte de la machine, temps de choix et de confirmation sur la seule machine disponible, absence d'isoloir, émargement inchangé, quasi-impossibilité de faire voter 1000 électeurs en 10 heures avec 36 secondes par électeur). Par contre ils accélèrent le dépouillement : le résultat est instantané (mais non vérifiable), ce qui n'est pas forcément indispensable pour des mandats durant des années et pour des scrutins finalement rares, mais permet de passer vite à la télévision[10]. Concernant le coût, il n'y a pas d'informations nationales consolidées sur le sujet. Sur les aspects écologiques, il s'agit d'écrans tactiles à cristaux liquides, d'électronique, de batteries, etc., et il y a toujours les professions de foi papier. Les possibilités de voter plus souvent ou de voter suivant d'autres méthodes de vote (classement, élimination, etc.) ne sont pas utilisées (ni prévues dans le code électoral). Notons enfin que les ordinateurs de vote ont rendu le vote blanc explicite (un bouton ou un choix « vote blanc ») et fait disparaître le vote nul.

Le vote par Internet a ses problématiques propres : des pressions peuvent être exercées sur l'électeur à son domicile, il peut plus facilement vendre son vote, le vote peut être bloqué depuis un pays donné ou perturbé par un pays voyou,

10 : Je ne résiste pas à la tentation de mentionner la ridicule possibilité de recomptage par la machine, qui permet de redemander autant de fois que l'on veut à une machine si son décompte est toujours le même.

l'ordinateur/le mobile de l'électeur peut être mal configuré ou infecté, etc. Il s'adresse surtout à une diaspora qui a des problématiques propres : les urnes physiques (ambassades ou consulats) peuvent être distantes de plusieurs centaines ou milliers de kilomètres, le pays peut être hostile ou dangereux, les services postaux peuvent y être de mauvaise qualité (problématique pour le vote par correspondance), etc. Le vote à l'urne est donc compliqué, le vote avec procuration aussi (il faut aller l'établir), le vote par correspondance est peu fiable (en particulier avec une seule semaine entre deux tours) et le vote par Internet a donc ses propres limites (et notamment le fait d'être interdit pour certaines élections, dont la présidentielle).

Il doit être vu comme un pis-aller suivant les directives du Conseil Constitutionnel mettant la priorité sur le droit de l'électeur de pouvoir exercer sa citoyenneté par le vote, par rapport à son droit à un vote vérifiable par exemple (ou par rapport aux critères internationaux qui préfèrent le vote à l'urne aux méthodes avec intermédiaires comme la procuration ou la correspondance papier ou électronique). Les diverses limitations évoquées ici ont conduit le ministère des Affaires Étrangères et Européennes à considérer que c'était une solution acceptable pour la diaspora, mais à ne pas vouloir la généraliser au reste du corps électoral. Et le 6 mars 2017, le gouvernement a annoncé ne pas recourir au vote par Internet pour les élections législatives de juin 2017, « sur la base des recommandations des experts de l'Agence nationale de la sécurité des systèmes informatiques (Anssi) » : « C'est essentiellement un risque d'image [...]. On ne peut exclure un risque sur la sincérité, mais ce qui est plus probable, en termes de faisabilité, c'est une attaque majeure qui rende

le système indisponible [...] avec un impact important sur l'image du fonctionnement de la démocratie. »[11]

2017 pourrait donc être une année particulièrement marquante pour le vote électronique sous toutes ses formes.

11 : http://www.lemonde.fr/pixels/article/2017/03/07/annulation-du-vote-electronique-des-craintes-d-une-attaque-majeure-rendant-le-systeme-indisponible_5090506_4408996.html

Et là où le bât blesse, c'est qu'aucune de ces exigences n'est possible à satisfaire ni vérifiable par n'importe quel citoyen. D'ailleurs, aucun professionnel ne se risquerait à garantir n'importe laquelle de ces étapes avec une certitude équivalente à celle du vote papier. Rappelons, en parlant de logiciel par exemple, que mettre un bulletin dans une enveloppe, puis une enveloppe dans l'urne et enfin compter les bulletins n'est pas du tout comparable à appuyer sur des boutons et accepter une somme produite par le terminal. Un ordinateur est une machine multifonction : elle sait faire des additions et des soustractions, mais aussi plein d'autres opérations mathématiques. Vu qu'on a affaire à des objets palpables, compter les bulletins dans les enveloppes pour chaque candidat, puis vérifier que le total correspond au total des émargements des électeurs est simple. Il se passe quoi si une machine vous donne un nombre différent de bulletins totaux par rapport aux votants ? On appuie de nouveau sur le bouton et on prie pour que le résultat soit bon ? Et si la machine nous donne un autre résultat, qu'est-ce que cela signifiera ? Qu'on peut appuyer et recompter jusqu'à tomber sur un total (pour un candidat donné par exemple) qui nous satisfasse ? Au final, on ne sait pas quelle option serait la pire : que le nombre de bulletins exprimés ne corresponde pas au nombre d'émargements ou que la machine puisse fournir des résultats différents à la prétendue même opération ?

Si l'on regarde plus loin, on se heurte à des décalages entre les dispositions légales et les exigences de sincérité et vérifiabilité. Ainsi, dans la loi, on lit qu'un ordinateur de vote doit pouvoir résister à une chute d'un mètre de haut (ne pas se casser donc). Mais en quoi est-ce plus pertinent que l'exigence que le matériel fasse ce que l'on attend de lui ? Ne pas se casser suite à une chute n'est aucunement équivalent au cas où le matériel ne modifie pas le comportement des logiciels utilisés. Le problème, plus grave encore, est que rien ne garantit que le résultat du vote corresponde aux intentions des votants ni que les opérations aient été anonymes. C'est plutôt gênant.

Bon, et le logiciel libre et open source, alors ? Comme on le voit et en connaissant son mode de fonctionnement, on peut aisément constater que son utilisation ne résoudra pas les problèmes soulignés plus haut. Oui, on pourra auditer le code, en amont et en aval. Oui, on pourra s'assurer que des traces (des *logs*) sont laissées en bonne et due forme par l'ordinateur où est installé un logiciel libre de vote. Mais la gestion de l'immatériel reste ce qu'elle est. Le pouvoir que certains citoyens auront d'auditer le code ne résout en rien les exigences énoncées plus haut non plus.

Et les exemples de problèmes rencontrés avec les ordinateurs de vote ne manquent pas, aussi bien en France qu'ailleurs : de nombreuses personnes montrent comment modifier la machine dans l'isoloir du bureau de vote, des machines à voter qui donnent plus de votes que d'électeurs, des résultats illisibles parce que la machine ne sait pas gérer l'encodage de caractères, des messages en franglais (en violation avec la loi Toubon)…[132] La nature immatérielle du vote rend énormément de choses plus compliquées. Quant aux erreurs, citons ces observations issues des enquêtes et basées sur l'analyse de procès-verbaux des élections françaises pour la période 2007-2012[133] :

« D'après les remarques portées sur les procès-verbaux de bureaux de vote, nombre de ces disparités sont dues à des votes multiples ou à des impossibilités de voter. Cependant, l'origine endogène de certains écarts ne peut être écartée a priori.

Une machine à voter transforme les votes des électeurs hors de tout contrôle, il n'est donc pas impossible que certaines de ces transformations dénaturent les données sur lesquelles elles opèrent sans que ces dysfonctionnements puissent être constatés. »

Ainsi, si l'on regarde la précision et les écarts (amplitude d'erreur donc) entre vote papier et vote électronique, on constate que, par exemple, pour les élections départementales de 2015, « *il y a en moyenne 3,5 à 4,5 fois plus de différences entre les nombres de votes et les nombres d'émargements lorsque des ordinateurs de vote sont utilisés* ». Ces différences se retrouvent de façon assez systématique dans les élections municipales et européennes de 2014 (« *3 à 4 fois plus de différences* ») et dans les élections présidentielles et législatives de 2012 (« *3,5 à 5,3 fois plus importantes* »).

À l'heure actuelle, les solutions aux exigences listées plus haut ne semblent pas exister. Ou plutôt, elles peuvent être identifiées mais impliquent des compromis (par exemple, mettre à mal le secret du vote). Par ailleurs, un argument souvent évoqué en faveur de la généralisation du vote électronique – le prétendu coût plus bas que le vote papier – est fallacieux. Ou encore, on dira que le vote électronique, c'est beaucoup mieux parce que l'obtention des résultats est beaucoup plus rapide. C'est vrai que quelques heures, c'est dramatique. Mais est-on prêt à mettre en danger nos élections pour ne plus attendre quelques heures une fois par an en moyenne ?

LA VIE PRIVÉE, UNE HISTOIRE DE VIEUX CONS ?[62]

Est-ce pertinent de retomber dans la dénonciation un peu puérile, et surtout stérile, des méchants géants du web qui recueillent des données sur nos vies sans vraiment se soucier de nos états

62 : C'est le titre de l'excellent livre de Jean-Marc Manach, paru chez FYP en 2010. Il pose la question de manière claire (et, selon certains, un peu provocatrice). Le livre – toujours d'actualité – dépasse la pseudo-tension générationnelle et recentre le débat sur nos libertés.

d'âme ? On accepte de donner accès à ces informations, souvent sans faire attention à ce que l'on cède pour de vrai. Ce n'est pas non plus une raison pour entrer dans un cycle de culpabilisation : comme la cigarette, « arrêter Facebook » est difficile en raison de la pression sociale environnante. De nombreuses personnes qui ne l'utilisaient pas ont dû s'y mettre relativement récemment pour éviter d'être oubliés (les anniversaires et invitations que l'on réserve à ses « amis Facebook », les photos de bébé ou les annonces de célibat,…). C'est humain de vouloir rester en contact et injustifié d'aboyer de façon culpabilisante sur les personnes qui estiment que c'est plus important que de refuser les conditions d'utilisation.

Mais si cette présence sur des plates-formes, réseaux sociaux et autres services en ligne qui recueillent nos données est devenue normale, cela ne signifie pas pour autant que l'on doive totalement ouvrir les vannes. Toute considération morale mise de côté, il y a une différence entre avoir « une présence sociale », comme on dit aujourd'hui en (ab)usant d'anglicismes, et avoir la posture « tout ce que vous avez toujours voulu savoir sur moi est sur Internet ». Aujourd'hui, le numérique et notre présence sur le web font partie de notre vie quotidienne. Laissiez-vous la porte grande ouverte nuit et jour, que vous soyez à la maison ou pas ? Très probablement pas. Mais fermer sa porte à clé ne signifie pas pour autant qu'on habite dans une maison avec des miradors, des gardes armés et des chiens. Encore une fois : le modèle de menaces est votre ami et la connaissance des risques aide grandement. Quand on parle de réseaux sociaux, on parle d'écosystèmes où de nombreuses personnes sont impliquées. Si vos mots de passe comportent 10 000 caractères, vous vous sentez sûrement invulnérable, mais pensez à ceux qui sont connectés à vous sur le web et qui, eux, n'ont pas autant de respect pour la complexité des mots de passe. Autrement dit, la sécurité d'un système est celle de son maillon le plus vulnérable.

Intéressons-nous ainsi à deux types d'activités grandement facilitées par l'entrée du numérique dans notre quotidien : le *doxxing* et le *revenge porn*. Les deux activités sont le plus souvent malintentionnées et peuvent prendre des proportions traumatisantes pour leurs victimes.

LE DOXXING

Le *doxxing* est un néologisme de l'argot américain. Il indique la pratique de recherche et de publication d'information personnelles. Le plus souvent, la motivation d'une telle démarche est l'humiliation publique d'une personne ou, plus largement, un règlement de comptes. Les informations personnelles peuvent être de tout genre : des photos, le numéro de téléphone, l'adresse personnelle postale ou e-mail, des commentaires ou propos désobligeants, etc. Ces éléments constituent un « dossier » que l'auteur peut utiliser pour discréditer ou compromettre sa cible. Il y a des cas où l'approche est utilisée pour traquer et démasquer les auteurs de commentaires haineux par des gens bienveillants qui peuvent par la suite tenter de faire peur aux commentateurs pour les pousser à arrêter leurs déclarations[134]. Le problème de cette dernière approche, même si elle part d'une bonne intention, est le recours occasionnel à des moyens de recherche aux limites du légal ou au-delà : on peut obtenir beaucoup d'informations personnelles sur quelqu'un qui tient des propos haineux en se servant de *spearphishing,* mais cette technique n'est pas légale. Si l'on peut collecter beaucoup d'informations sur les gens parce que leur ego les pousse à faire la démonstration de leurs dîners, fêtes et nouvelles acquisitions, les harponner et se faire passer pour un fournisseur d'accès à Internet pour obtenir des détails supplémentaires n'est pas acceptable, même si on a de très bonnes intentions au départ.

Comment s'exprime la « revanche par *doxxing* » ? De plein de façons : menaces, pizzas commandées pour vous et non payées

(voir chapitre 02), harcèlement en ligne, *swatting*[63]. Des cas de *swatting* sont connus en France, que ce soit à l'encontre de journalistes[135], d'élus[136] ou encore d'associations[137]. D'après la loi française, le *doxxing* relève du Code pénal (atteintes à la personnalité) pour atteinte à la vie privée, dénonciation calomnieuse et atteinte au secret (par exemple en cas de violation du secret des correspondances si quelqu'un s'introduit dans votre boîte e-mail et en publie des extraits choisis).

LE REVENGE PORN

Le *revenge porn* relève également de la diffusion d'information personnelle mais est différent du *doxxing*. Dans un cas de *revenge porn*, un proche, généralement un ex-compagnon ou ex-amoureux éconduit, dissémine des contenus multimédias de son ex-partenaire (féminine le plus souvent). Le côté « *revenge* » (vengeance) est très clair dans ces agissements. Ces contenus peuvent être des images dénudées, des vidéos d'ébats, etc. que les deux ont pris ou échangés lorsque les choses allaient à merveille entre eux. La personne publie ainsi les contenus, sans le consentement préalable de celle dont elle veut se venger, sur autant de sites web que possible, de façon qu'ils soient vus par le plus grand nombre. Les publications peuvent être faites de manière à donner l'impression d'émaner de la personne cible, comme si elle publiait une invitation à la rejoindre... Et souvent, ces « annonces » contiennent également l'adresse personnelle et le numéro de téléphone de la victime. Lorsque cette machine se déchaîne, il est difficile de l'enrayer. Les personnes victimes de *revenge porn* essaient de se protéger en prenant des chemins différents pour leurs déplacements, en changeant de numéro de téléphone, de domicile, etc. Comme le précise la députée et présidente de la délégation de l'Assemblée

63 : Il s'agit d'un canular téléphonique anonyme : on appelle les autorités pour faire croire au besoin d'une intervention d'urgence chez un particulier en prétextant une prise d'otage ou autre situation d'extrême gravité. Le but est de nuire à la personne (imaginez le GIGN qui rentre en défonçant votre porte...).

nationale aux droits des femmes, Mme Catherine Courtelle, lors des débats parlementaires autour du *revenge porn* :

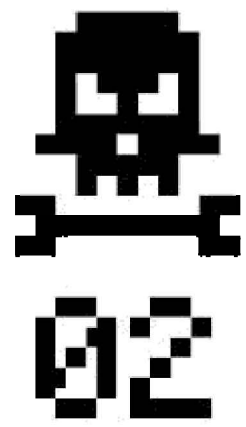
« *Les conséquences de ces violences virtuelles sont, elles, bien réelles : souffrances, anxiété, perte d'estime, isolement, décrochage scolaire, automutilation, voire actes suicidaires. Elles sont amplifiées par la diffusion massive que permet le numérique.* »

De plus en plus de pays introduisent des sanctions pénales pour les personnes coupables de *revenge porn* : ainsi, en janvier 2016, le Code pénal a été modifié pour porter à deux ans de prison et 60 000 euros d'amende les peines encourues par ces individus qui se vengent de leurs anciennes conquêtes en mettant en ligne des images sexuellement explicites[138]. Suite à deux cas de *revenge porn,* dont l'un a mené la victime au suicide et l'autre montrant un viol, l'Italie s'est également saisie de la question[139]. Le problème n'est pas vraiment répandu en France, contrairement aux États-Unis, où des sites dédiés existent où on poste du *revenge porn* en masse[64]. Le cadre légal étant assez inégal (seulement vingt-six des cinquante et un États ont une législation pénalisant la pratique), certains de ces sites en tirent un bénéfice sonnant et trébuchant : ainsi, si vous souhaitez que les opérateurs du site enlèvent les contenus vous concernant, il faut vous acquitter d'une somme qui varie de site en site. Pour les contrecarrer, des personnes – journalistes, chercheurs ou encore activistes – traquent les sites publiant ce genre de contenus et émettent des attaques (avec des DDoS le plus souvent)[65].

64 : Un documentaire de Vice (sous-titré en français) permet de rencontrer certaines des victimes aussi bien que des opérateurs de sites où ce genre de contenus est diffusé https://www.vice.com/fr/article/le-revenge-porn-et-ses-degats-broadly-758

65 : Les Anonymous, dont on parlera au chapitre 02, ont fait ce genre de choses. La pratique est tellement répandue à tous les coins du monde que ce genre d'activistes existent même en Corée du Sud (https://twitter.com/soraeliminate). Le nom du compte Twitter vient du plus important « fait d'armes » de ces féministes sud-coréennes : la fermeture du site sora.net, connu pour non seulement publier des contenus *revenge porn* mais également héberger des forums d'« échange de bons procédés » sur les manières d'abuser des victimes hors du web.

On s'attendrait à une conclusion de chapitre qui claque… Ce n'est pas évident. Ce qui l'est cependant, c'est la ribambelle d'enjeux qui constituent et façonnent notre quotidien, leur imbrication et impact sur notre vie. Si vous ne retenez qu'une chose, on espère qu'elle soit une compréhension plus riche et critique du numérique : le « quoi » de ce livre fait ainsi place au « qui ».



02

LA FIGURE DU HACKER : LES BONS, LES BRUTES ET LES ANONYMOUS

× × ×

01

....

50 NUANCES DE HACKER

Leur relation au pouvoir étatique, centralisé, a de multiples facettes : prise de contrôle abusive de systèmes d'information, publication non autorisée de contenus sous droits d'auteur pour « *libérer* » les œuvres, publication de vidéos classées « secret-défense », adoption de monnaies parallèles, etc. Nous le voyons bien : les hackers d'Anonymous et autres groupes dissidents rejoignent l'armée des empêcheurs de tourner en rond. Pousser les frontières, questionner la propriété et l'autorité, voilà ce que font ces internautes. La notion de valeurs culturelles associées à la technologie devient alors prégnante. Une réflexion s'impose. En effet, la plupart d'entre nous ne supportons pas les défaillances d'un téléphone ou le moindre dysfonctionnement d'un ordinateur. Mais *quid* de la perception finalement positive de ces couacs qui nous permettent de « mettre les mains dans le cambouis » et d'établir une autre interaction avec l'objet ? Essayez un jour de réparer votre ordinateur, vous verrez que votre rapport à la machine change.

Un hacker est donc un bricoleur et un explorateur qui ne se contente pas de constater que « mince alors, ça marche pas ». En questionnant le statu quo (certes, en des termes peu châtiés, voire cryptiques[1] ou dramatiques[2]), les hackers recréent des normes sociales. Cependant, la moralité des actions n'est pas le sujet ici. Pour reprendre Léo Ferré : « *Ce qu'il y a d'encombrant avec la morale, c'est que c'est toujours celle des autres.* » Il ne s'agit

donc pas, chers lecteurs, de faire insulte à votre intelligence en me positionnant en donneuse de leçon sur le bien et le mal, mais de clarifier et de contextualiser des agissements.

Il est souvent difficile de bien distinguer les bons et les brutes, les Anonymous et lanceurs d'alerte, les « chapeaux blancs », les « chapeaux noirs » et toutes les nuances de gris qui façonnent le paysage numérique toujours mouvant. Essayons donc d'y voir plus clair.

« RAPIDE ET SALE »

Avec les premiers ordinateurs apparaissent les premiers experts informatiques. Dans les années cinquante, le prestigieux MIT[1] voit ainsi naître en son sein des « hackers ». En anglais, *to hack* (d'où l'anglicisme « hacker ») est un mot générique qui traduit surtout, dans ce contexte, l'idée de trouver un moyen autre, alternatif, de faire faire quelque chose à la machine.

Ces personnes cherchent donc à comprendre le fonctionnement de la machine, à l'améliorer et à innover. Elles corrigent des erreurs dans les programmes informatiques ou trouvent des moyens d'optimiser l'exécution d'un programme, en réécrivant par exemple certaines étapes d'un processus. Le mot a évolué pour également indiquer une manière peu conventionnelle, mais fonctionnelle, de corriger un dysfonctionnement : c'est pourquoi le mot français que l'on a trouvé pour traduire « hacker » est « bidouilleur ». On entendra ainsi souvent des gens qui « bidouillent » dire : « *Bon, mon script tient avec des bouts de scotch mais osef* [abréviation de « on s'en fout »], *ça fait le truc.* » L'idée d'un hack est donc de faire en sorte que ce soit fonctionnel sans pour autant en faire quelque chose de fini, perfectionné, joli… Les « bouts de scotch » sont bien sûr une image, pour exprimer le côté artisanal et « vite fait » du correctif. L'abréviation anglaise Q&D (*quick and dirty*, soit « rapide et sale ») traduit bien l'esprit du hack.

1 : Massachusetts Institute of Technology à Cambridge.

C'EST BEAU COMME UNE SERRURE CROCHETÉE

Il est évident que cette approche de la technologie façonne les interactions entre celles et ceux qui la pratiquent. S'échanger des programmes, réfléchir ensemble à comment aller encore plus loin, comparer ses solutions à un même problème, etc., sont des activités fondamentales et naturelles. Au MIT d'autrefois, accéder aux machines, normalement réservées à certains scientifiques seulement, devient donc un défi. Et le fait qu'il y ait un obstacle à franchir rend la perception de l'accès à la technologie et à la connaissance bien plus savoureuse. On comprend mieux pourquoi l'accès libre et ouvert à la connaissance constitue un fondement de la culture hacker et de ce qui est devenu aujourd'hui le numérique.

Ce rapport à l'interdit, à ce qui n'est réservé qu'à une élite façonne forcément le rapport à l'autorité centrale des hackers. S'introduire dans une pièce fermée à clé est un défi symbolique autant que physique. Si vous vous demandez pourquoi les protagonistes de la série culte *Mr Robot* savent aussi bien crocheter des serrures, vous avez là un élément substantiel de réponse. Le seul fait de crocheter une serrure est un petit défi en soi. Si vous aimez vous faire des nœuds au cerveau et résoudre des énigmes, alors vous aimerez crocheter une serrure ! Le festival Chaos Communication Congress (le CCC)[3], le plus grand festival de culture hacker et alternatives, propose tous les ans des stands où on peut acheter des kits de crochetage et apprendre à s'en servir. Plus encore, aux États-Unis, le crochetage de serrure est un « *locksport* ». Et comme tout sport, il a ses règles : on ne crochète pas des serrures qui ne nous appartiennent pas ; on ne crochète pas des serrures dont on se sert. Les limites de la pratique de ce sport sont donc claires : on ne vole pas et on ne coupe pas la branche sur laquelle on est assis.

Une association appelée Toool (pour *The Open Organisation of Lockpickers*, l'organisation ouverte des crocheteurs de serrures), en Europe et aux États-Unis réunit des hackers de tous bords qui aiment à résoudre des énigmes complexes[4]. Et c'est là où le fait

d'ouvrir des portes closes représente une superbe métaphore du hacking : y parvenir requiert de la patience. Comprendre comment le système fonctionne, quels sont ses rouages et comment on peut intervenir sur ces mécanismes.

Avec le temps, le verbe *to hack* a évolué en fonction des pratiques[2]. L'introduction dans des systèmes informatiques est devenue un véritable métier et, logiquement, la défense contre les intrusions aussi. La métaphore du crochetage de serrure persiste : l'une des pratiques les plus fondamentales de l'audit de sécurité est le « *pen test* », abréviation de « *penetration test* », ou, la découverte ou l'exploration des brèches et trous susceptibles d'être des portes d'entrée chez autrui.

On se retrouve dès lors dans *Alice au Pays des merveilles*... version hacker : lorsque Alice rencontre la Reine Rouge, toutes deux se lancent dans une course. Alice demande alors : « *Mais, Reine Rouge, c'est étrange, nous courons vite et le paysage autour de nous ne change pas ?* », ce à quoi la Reine répond : « *Nous courons pour rester à la même place.* » La métaphore est connue comme une illustration de la course aux armements, que ce soit entre États-nations ou entre espèces. Chez les hackers, une course permanente existe aussi : on s'y donne des défis toujours plus complexes à résoudre.

L'ÉTHIQUE HACKER

En 1984, Steven Levy[5], un journaliste tech américain ayant grandi avec l'émergence de l'informatique et de la culture hacker, définit « l'éthique hacker » en quelques points :

- Toute information est par nature libre.
- La décentralisation doit être promue, l'autorité n'étant pas digne de confiance.

2 : Pour la postérité, notons ce glossaire collector de 1993 qui introduit le lexique : https://www.ietf.org/rfc/rfc1392.txt

- Parmi les hackers, ce qui compte, ce sont les prouesses et non les hiérarchies sociales. On retrouvera cette notion de « *do*-ocratie », soit le pouvoir par ceux qui font (*to do*), chez Anonymous par exemple.
- De l'art et, plus largement, de la beauté peuvent être créés avec un ordinateur.
- Les ordinateurs peuvent changer la vie, voire l'améliorer.

Cette éthique a énormément de déclinaisons. Le MIT a donné Richard Stallman, le fondateur du projet GNU, que l'on connaît aujourd'hui comme le père de la formalisation du logiciel libre. Ce dernier préserve les quatre libertés fondamentales de son utilisateur : il lui permet de connaître le fonctionnement du code (ouvert), de le modifier, de le partager et d'en faire des dérivés. Cette vision est diamétralement opposée aux logiciels à code fermé, véritables boîtes noires dont le fonctionnement relève de la magie, et qui excluent l'utilisateur de l'équation. Stallman qualifie ces logiciels de « privateurs » pour indiquer qu'ils privent l'utilisateur des libertés fondamentales assurées par le logiciel libre. Dans l'esprit du logiciel libre, la règle de base est de toujours pouvoir modifier un logiciel pour en faire un autre. Pour éviter que le nouveau ne se transforme en une boîte noire et que l'éthique soit ainsi pervertie, le projet GNU a défini des règles légales. Ces dernières sont les licences de la famille GPL (*General Public Licence*) ; elles sont qualifiées de « héréditaires » ou « virales » parce qu'elles obligent à conserver les libertés fondamentales du logiciel libre dans chaque dérivation qui en est faite. Ainsi, lorsque la série bureautique Open Office s'est retrouvée en difficulté de gouvernance il y a quelques années, la partie de la communauté de développeurs qui souhaitait continuer le projet en accord avec leur vision a pu faire un *fork* (un dérivé ou une scission en français) que l'on connaît aujourd'hui comme la suite bureautique Libre Office. Cette dernière continue à être un logiciel libre. En cohérence avec l'éthique du logiciel libre, un mouvement a dérivé, connu sous le

nom d'*open source* (code source ouvert), dont la préoccupation est surtout technique. Mais, laissons là les divergences philosophiques, il faudrait un second livre pour en narrer les détails !

En 2017, le logiciel libre est partout. Des langages de programmation, des infrastructures sous-tendant le réseau Internet ou ses couches web à votre téléphone mobile ou votre lave-vaisselle. Par exemple Linux, le nom un peu réducteur de certains logiciels libres et open source formant un système d'exploitation a pénétré chaque parcelle informatique de notre vie. Un logiciel libre peut être gratuit, mais l'inverse n'est pas vrai. L'éthique qu'il porte est fascinante et toujours d'actualité : qu'est-ce qui pousse quelqu'un (ou un groupe de personnes) ayant une expertise certaine à passer ses soirées et même ses journées à créer quelque chose qui ne lui rapportera pas d'argent ? Plus encore, dans un environnement socio-économique où « faire » et « bidouiller » sont vus comme des activités subalternes, « col-bleu » et peu gratifiantes, qu'est-ce qui motive des gens à persévérer et créer de l'abondance qui ne leur rapporte (presque) rien ?

Gabriella Coleman, une anthropologue dont on reparlera, a raconté son immersion dans le monde des « hackers » en général et des communautés de logiciels libres et open source en particulier. Son livre[3] rend compte de l'attachement que portent nombre de ces communautés aux principes de « *protection de la propriété et des libertés civiles, promotion de la tolérance et de l'autonomie individuelle, sécurisation d'une presse libre, direction via un gouvernement aux pouvoirs limités et des lois universelles, et préservation du principe d'opportunité équitable et de méritocratie* ».

Les personnes présentes dans ce livre évoluent pour beaucoup avec ces valeurs ; elles font leur promotion *via* le numérique, et ce sans même y penser. Les actions et principes évoluent avec le temps, bien sûr, mais l'étoile de Nord de cette éthique reste inchangée.

3 : *Coding Freedom – The Ethics and Aesthetics of Hacking*, E. Gabriella Coleman, Princeton University Press, 2013.

Ce côté « Bisounours » peut faire sourire, attendrir ou, au contraire, agacer. Il n'en reste pas moins que ces valeurs universalistes se sont étendues bien au-delà des communautés où elles sont nées. Cette approche sous-jacente a non seulement permis de créer des systèmes plus performants et plus sécurisés mais a également initié des modèles d'affaires (les *business models)* et d'innovation qui permettent de faire des bénéfices financiers avec de l'abondance et non plus avec de la rareté. La récente mode des fablabs[4] et autres hackerspaces[5] constitue ainsi une réflexion pratique sur le futur de la notion de travail et revalorise *Homo faber*[6]. On connaît aujourd'hui les modèles d'affaires basés sur le service autour d'un logiciel et non sur le droit de s'en servir pour un temps limité contre paiement ; de plus, des entreprises de conseil et accompagnement se revendiquant de l'innovation ouverte (*open innovation*) ont également vu le jour, proposant une méthodologie différente du R&D cloisonné classique impliquant des échanges et des communautés de pratiques lors de la création d'un nouveau produit.

LES BONS, LES BRUTES ET LES GRIS

Parler de l'éthique du crochetage de serrure et du partage de code source est impossible sans aborder le rapport à la sécurité des systèmes informatiques et des logiciels. Comme de ceux qui ne respectent pas les règles du jeu. Car il est évident que ceux-là existent et existeront toujours, quel que soit le contexte.

Le mot « hacker » est francisé en « hackeur »[7], mais quelle que soit son orthographe, le sens qui lui est donné en français

4 : Lieu ouvert au public où sont mis à disposition toutes sortes d'outils, notamment des machines-outils pilotées par ordinateur, pour la conception et la réalisation d'objets. La caractéristique principale des fablabs est leur « ouverture ». Ils s'adressent aux entrepreneurs, aux designers, aux artistes, aux bricoleurs, aux étudiants ou aux hackers en tout genre... Pour se tenir au courant de leur actualité, lire makery.info.
5 : Sortes de laboratoires communautaires/tiers-lieux ouverts où des hackers peuvent partager ressources et savoirs.
6 : Pour une plongée en français, *L'Âge du faire. Hacking*, travail, anarchie, Michel Lallement, Paris, Seuil, 2015.
7 : Nous conserverons ici l'orthographe anglo-saxonne.

dans l'imaginaire collectif, c'est celui du pirate (donc méchant) informatique ; celui qui veut absolument se saisir de nos numéros de carte bancaire pour s'acheter des drogues ou faire exploser une centrale nucléaire. L'imagerie invariablement associée est aussi ridicule que risible : le hacker est toujours un mâle dont on ne distingue pas bien le visage, dissimulé dans un *hoodie* noir avec une capuche et qui tape des trucs cabalistiques devant un écran noir avec des chiffres et des lettres. Plusieurs variations de cette image existent, où la capuche semble être un incontournable, sans que l'on sache très bien pourquoi.

La terminologie introduite (le plus souvent par ceux qui étaient concernés) dès les années quatre-vingt, lorsque « hacker » était de plus en plus exclusivement associé à une activité criminelle, fait surtout référence aux couleurs. Celles-là sont un peu trop manichéennes : les nombreuses exceptions montrent surtout que la réalité est en nuances de gris. Ainsi, les *white hats* (« chapeaux blancs ») sont les bons, les *black hats* (« chapeaux noirs »), les brutes, et les *grey hats* (« chapeaux gris ») représentent le plus souvent ceux qui utilisent des moyens illégaux pour accomplir de bonnes actions. Ce que l'on est venu à appeler les hacktivistes sont donc en nuances de gris. Ceux-ci défendent une cause humaniste ou humanitaire en se servant de la technologie, même si cela implique le recours à des activités interdites par la loi. Mot un peu barbare, il est formé d'une contraction entre « hack » et « activist », ce dernier traduisant en anglais une activité militante[8].

Trouver des failles n'est ni un problème ni un avantage ; c'est ce que l'on fait avec les brèches qui peut être l'un ou l'autre. En pharmacologie, c'est la dose qui fait le poison. En informatique, c'est l'usage de la vulnérabilité qui fait la couleur du hacker. Éprouver la sécurité d'un logiciel qui sera diffusé à grande échelle, c'est plutôt positif : nous préférons toutes et tous utiliser des outils sécurisés.

8 : Le mot « activiste » est connoté négativement en français. En anglais, c'est le contraire : un « militant » est le plus souvent quelqu'un participant à une organisation illégale ou terroriste, contrairement à l'*activist*.

Un expert en sécurité peut ainsi par exemple (et en le disant très vite) être assimilé à un *white hat* : il fera les tests nécessaires pour répertorier et corriger toutes les brèches et failles d'un produit informatique. C'est ce que proposent les entreprises de sécurité informatique aux développeurs de logiciels et aux sociétés qui déploient des solutions techniques extérieures au sein de leur infrastructure. Un expert de ce genre peut également être expert judiciaire ; dans ce cas, il réceptionne des machines (ordinateurs, téléphones, etc.) sous scellés, saisies dans le cadre de perquisitions, et s'emploie à casser la sécurité imposée par le suspect ou la victime. Les *white hats* peuvent également s'introduire dans des systèmes pour le goût du défi, sans intention malveillante ; le plus souvent, s'ils y arrivent, ils préviennent les gestionnaires desdits systèmes du point vulnérable.

Dans notre classification, les brutes, les « chapeaux noirs », ou « black hats », sont toutes les sortes de personnes malveillantes. Mais il est très difficile de définir ce qu'est la malveillance : comme tout qualificatif ayant trait à la morale, le bien et le mal dépendent de qui en parle. Un *black hat* peut être un escroc qui se débrouille pour vous piéger et obtenir le numéro de votre carte bancaire. Un escroc peut également prendre vos données en otage et vous demander une rançon pour vous les rendre (cf. le *ransomware* dans le chapitre précédent). Il peut encore dérober les identifiants et mots de passe d'un milliard de comptes e-mails Yahoo! et les vendre sur le darkweb (cf. chapitre 03). Un *black hat* peut également faire des recherches de failles, mais, plutôt que d'en avertir les administrateurs, il les vendra au plus offrant. Il s'agit des vulnérabilités 0day (zero day ou jour zéro) que l'on a déjà évoquées (voir chapitre 01). Ces cas sont relativement simples à classer dans la catégorie « méchants ».

Mais *quid* des hackers mercenaires ou de ceux qui exposent les secrets d'entreprises ayant des pratiques contestables voire illégales ? Un hacker peut encore être un « cybermilitant » : au service d'un gouvernement, il peut créer des logiciels espions

dirigés contre ses concitoyens ou contre les services d'un autre gouvernement. Si une entreprise viole la loi et les conventions internationales en faisant travailler des enfants, en nourrissant des conflits armés pour se faciliter l'accès à des ressources rares, en empêchant l'accès à la connaissance, etc., peut-on qualifier un de ses employés de « méchant » parce que la personne aura fait fuiter des informations sur ces pratiques ? Ou peut-on traiter de « brute » un hacktiviste qui s'introduit par un moyen illégal dans les systèmes informatiques d'une société qui vend du logiciel espion à des gouvernements qui emprisonnent et torturent leurs opposants ? Dans chaque cas, décider de la moralité de l'action n'est pas chose aisée.

02

DU TROLL À L'HACKTIVISTE

En parlant de moralité… Qui sont les Anonymous ? Des trolls[9] ou des hackers ? Ou peut-être des lanceurs d'alerte ? Qu'est-ce que le « lulz », plaisanterie plus ou moins drôle mais toujours aux dépens d'autrui, et pourquoi est-il si important pour saisir l'évolution de ces plaisantins ? Comment un site de trolls tel que 4chan a-t-il pu produire des blagues potaches et de mauvais goût, et donner naissance à un activisme politique défendant, à sa manière, la veuve et l'orphelin ?

Le rire, ce lulz (dérivé du « LOL » connu comme « mdr » en français), est grinçant et quelque peu transgressif, voire déviant, mais en quelques années sa motivation a changé. Comment cela s'est-il produit ? Il est important de comprendre que lorsque l'on parle de *trolling*, d'Anonymous et de hackers, il est impossible de créer une filiation précise des phénomènes ; comme tout processus social, ceux-là sont un ensemble intimement entremêlé de contextes, d'acteurs et d'évènements. La catégorisation stricte, le leadership et la stratification horizontale sont antinomiques du mouvement multiforme, vibrionnant et en constante évolution qui nous occupe ici. Tentons d'en comprendre les caractéristiques fondamentales et retraçons ensemble une (très) brève histoire d'Anonymous.

9 : Personnage dont le but est de perturber, sur les réseaux sociaux, une discussion en multipliant les messages sans intérêt ou virulents…

GÉNÉALOGIE DU TROLL

Le *trolling* est une vieille tradition : qui ne connaît pas le principe du canular téléphonique ? Qui n'a pas, petit, appelé un numéro de téléphone inconnu pris au hasard dans l'annuaire et raconté une blague (pas toujours très drôle !) avant de raccrocher, tout rouge et hilare ?

Le *phreaking* est le piratage téléphonique et date des années soixante : un jour, aux États-Unis, quelqu'un découvre qu'un son de fréquence 2 600 Hertz permet, lorsqu'il est émis sur des appels longue distance, d'avoir accès à des options d'administration avancées (mode opérateur). Or un tel bip pouvait être produit à l'aide d'un sifflet distribué gratuitement dans des boîtes de céréales Cap'n Crunch. L'âge d'or du *phreaking* est le début des années soixante-dix, période foisonnante d'avancées technologiques importantes pour les réseaux et les communications téléphoniques[6]. Ces explorations sont documentées ; des *phreaks* lancent en 1984 le magazine *2600: The Hacker Quaterly*. Les fondateurs en sont Eric Corley, alias Emmanuel Goldstein, et David Ruderman. La revue existe toujours d'ailleurs, son site web est resté fidèle au design des années 1990[7]. Une grande partie de ces exploits violent cependant les lois en vigueur : on a déjà entendu parler de personnes se retrouvant avec des factures exorbitantes de téléphone fixe à régler, jurant de ne jamais avoir appelé le(s) numéro(s) en question. Le *phreaking* fait aussi partie de la culture populaire : si vous regardez le film culte *Hackers* de Iain Softley avec Angelina Jolie[8], vous y reconnaîtrez l'un des protagonistes, Emmanuel Goldstein, dont le pseudonyme dans le groupe de hackers est Cereal Killer ; divers cas de *phreaking* sont également évoqués.

Avec l'avènement du web grand public dans les années quatre-vingt-dix, le trolling a également changé de visage. Les *flame wars*, ou « discussions au lance-flammes », voyaient s'affronter des utilisateurs de Usenet, l'ancêtre des forums web. Ces activités sont décrites en détail dans le *Big Dummy's Guide to the Internet*[9]

« France Télécom ne s'est aperçu de rien, même pas de la surconsommation. »

Anonyme, expert réseaux et télécommunications dans un grand groupe

Dans les années quatre-vingt-dix, alors que j'étais collégien puis lycéen en Île-de-France, j'ai eu pas mal d'occasions de me frotter aux infrastructures telco *[télécommunications, NdR]* de l'époque.

Fin 1996, alors que je renégociais ma transfix *[une liaison Internet dédiée, NdR]* personnelle (j'avais une NextStation pour héberger quelques sites web faits au black, au cul d'une ligne 32kbps), j'ai fait pas mal de confcall avec Transpac/France Télécom Entreprise de l'époque. C'était fun parce que j'avais à peine mué, donc ils ne comprenaient pas à qui ils parlaient… j'avais fini par bricoler un « vocoder »[1] assez primitif pour vieillir ma voix.

Donc, à force de confcalls, de commerciaux à la bourre, d'interruption d'appels, etc. j'ai fini par passer pas mal de temps à explorer le « menu interactif » de l'agence France Télécom Entreprise (FTE), pour finir par me rendre compte de la connexion entre les numéros de l'agence « pro » et de l'agence « commerce/acquisition », un numéro vert en 05 à l'époque.

Leur standard était un truc assez évolué, à base de cartes de fonctions complémentaires sur un Alcatel de la gamme

1 : Vocoder : remodulation/repitching dynamique pour décaler un son de quelques notes, voire octaves. L'interviewé précise : « Je l'avais fait avec des LAR et un 6502, en fait un circuit que j'utilisais pour les décodeurs pirate de Canal+ et les chaînes FT câble, juste pas sur les mêmes modules d'entrée/sortie. »

4400 (dont tout fonctionnait en DTMF[2]). J'avais eu l'occasion d'en consulter la notice détaillée lors de mon stage de découverte en entreprise (où j'avais – entre autres – dû reprogrammer celui d'une collectivité parce que le changement de téléphoniste sur marché public s'était mal passé et que les services municipaux n'étaient plus joignables).

Bref, le standard de l'agence FTE Île-de-France nord-ouest (en fait, départements 92, 78, 95) avait une sacrée PABX[3] quasiment aussi riche qu'un CO régional, et j'ai commencé à en explorer les menus en dehors des quarts d'heure d'attente des rendez-vous commerciaux. Ce que j'ai fini par trouver, en gros, c'est qu'on pouvait appeler un numéro vert, depuis n'importe quelle ligne fixe (ou cabine), et avec moins de six touches, arriver sur un des soixante salons de conférences que le PABX était capable de gérer.

L'info a un peu tourné sur les fils de discussion Usenet et quelques BBS[4] locaux, jusqu'à ce que je l'oublie. On devait être en 1996. Mais on s'en servait surtout entre copains du collège, j'avais même monté un modem en attente sur un des salons pour que mes copains de collège/lycée – qui n'avaient pas de connexion illimitée – puissent se connecter gratos pour synchroniser leurs discussions Usenet *via* ma transfix.

En 1998, je reçois un e-mail bizarre qui me demande de détailler la hiérarchie de l'ISV du PABX. J'ai vite compris que c'était un autre phreaker, donc j'ai expliqué un peu, et il a donné plus d'écho au truc. On s'est retrouvé pendant l'été

2 : Cela correspond à l'appui d'une touche sur les téléphones (vous savez, quand on entend les instructions du genre « appuyez sur 1 pour réécouter votre message », etc.).
3 : Central téléphonique privé d'entreprise.
4 : L'ancêtre des forums web.

1998 à plus de quatre cents, connectés tous les soirs sur le PABX, avec des salons « Trivial Pursuit », d'autres « chat sexy » et quelques-uns « privés » ou régionaux. Un de mes potes a rencontré la mère de ses trois gosses sur un des salons « Trivial Pursuit » de l'époque.

France Télécom ne s'est aperçu de rien, même pas de la surconsommation (ils ne se facturaient pas en interne), donc ça a tourné peinard pendant pas loin de deux ans. Et ça s'est arrêté un jour, sans qu'on sache pourquoi exactement. Bref, un PABX pas sécurisé, une gestion laxiste des routages de SDA[5], et on avait créé une petite communauté qui a tenu presque trois ans... Sans finalement faire de tort à personne. C'était cool, le phreaking dans les années quatre-vingt-dix.

Bon, en marge de ça, j'ai pas mal de contacts de l'époque qui phreakaient avec préjudice pour les abonnés, et je n'ai jamais vraiment cautionné. Mais c'était une partie du sport : repérer les infras, comprendre le brassage des lignes, savoir repérer les plus « safe » et se brancher dessus pour emmerder les services d'hôtesses X...

Je connais au moins deux mecs qui phreakaient à l'époque et qui sont maintenant des tauliers incontournables sur les grosses infras telco. Enfin, un peu comme moi. Finalement c'est en « piratant » les réseaux voix qu'on a acquis les logiques requises pour faire marcher les réseaux d'aujourd'hui... Et, globalement, on n'a embêté presque personne, pour faire ce qui nous permet aujourd'hui d'assurer une sorte de service public.

Vive les telcos !

5 : Un numéro direct externe.

datant de 1993. Ces échanges inflammatoires sont des *trollings* en règle : quelqu'un de désobligeant vous invective et se positionne en empêcheur de discuter en rond. À l'époque, ces « net.weenie » ont pour but principal de mettre le boxon dans les discussions[10]. L'association EFF (Electronic Frontier Foundation) reconnaît même alors l'existence des net.weenies et précise, dans un guide d'utilisation de listes de diffusion, que celles-ci ont un caractère plus privé et souffrent moins de la présence désagréable de net.weenies que les forums Usenet publics[11]. Mais ces trolls des temps anciens n'étaient pas nécessairement aussi malveillants que peuvent l'être d'autres, plus contemporains ; par exemple, les Warlords faisaient du très beau *trolling*. Ils étaient surtout présents dans le sous-forum « alt.fan.warlord »[12] et se distinguaient par leur désaccord avec la netiquette (les règles de fonctionnement instaurées sur le forum). Ainsi, au lieu d'avoir une signature électronique de quatre lignes maximum, les leurs étaient des chefs-d'œuvre d'art ASCII[10].

D'autres utilisateurs se sont rendus célèbres par leurs comportements disruptifs : Netochka Nezvanova (un pseudonyme reprenant le nom du personnage principal du tout premier livre de Dostoïevski)[13] ou encore Brice Wellington[14]. Le troll ayant le plus d'impact aujourd'hui est BIFF, aussi connu comme B1FF : créé par Joe Talmadge de HP[15], il est l'archétype du novice, ou *newbie*. Ses interventions sont toujours en MAJUSCULES, contiennent des fautes d'orthographe ou des détournements de mots : une expression satirique et hétérogène dans un espace d'expression homogène. BIFF est aussi considéré comme étant à l'origine du langage alternatif *leet* (1337) : les lettres d'un mot sont remplacées par des chiffres ayant une apparence similaire. Le *leet* comprend non seulement les substitutions de lettres par des chiffres, mais aussi le mélange de lettres au sein d'un mot (« pr0n »), des substitutions

10 : L'art ASCII consiste à réaliser des images uniquement à l'aide des lettres et caractères spéciaux contenus dans le code ASCII. Par exemple, :-) est un émoticône en ASCII représentant un sourire ; _/o< est un canard ; \o/ signifie victoire et /o\ est signe de consternation (c'est l'image de quelqu'un qui se prend la tête dans les mains). Voir par exemple http://www.ascii-fr.com/ pour une jolie collection.

de lettres par d'autres avec une sonorité proche (« h4xx » pour « hack »), la création d'une lettre à partir de signes (« x » à partir de ><), etc.

La création de sous-forums Usenet tels que les (pas toujours) fameux alt.sex et alt.tasteless est notable. Ainsi, alt.tasteless, l'ancêtre de 4chan, est un endroit où « *on garde les malades loin* » des autres forums, comme l'explique un de ses « habitants » principaux[16] Comme ce livre est susceptible d'être lu par des personnes sensibles, nous ne citerons pas d'exemples de commentaires issus d'alt.tasteless.

ANONYMOUS : DERRIÈRE LE MASQUE

Ainsi la création de 4chan en 2003 est-elle le prolongement de ces comportements en ligne. La partie de 4chan connu comme « /b/ » était l'agora des trolls en tous genres, du porno jusqu'à des choses qu'on préfère ne pas revoir, même si on n'a pas nécessairement une âme trop sensible. Les utilisateurs de /b/, appelés des « /b/tards », s'appellent tous avec des mots composites finissant par le suffixe « -fag » ; ainsi par exemple, un novice est un « *newfag* ». Une autre caractéristique très forte de 4chan est que ses utilisateurs ne s'identifient pas : ainsi, les auteurs d'un grand nombre de messages sont listés comme « Anonymous ». Les utilisateurs créent des mèmes[11] et se trollent mutuellement, même si des situations de bienveillance exceptionnelle existent également lorsqu'un utilisateur a des problèmes de cœur par exemple ou si quelqu'un publie une vidéo de chat en train d'être maltraité. Contrairement à beaucoup de listes de diffusion et forums web, ces échanges sont assez éphémères et ne sont pas archivés.

Les utilisateurs étant anonymes, il se crée un environnement interactif assez particulier. Le capital social (tel que la réputation ailleurs ou sur le site en question) d'un utilisateur n'a aucune valeur ;

11 : Dans sa forme la plus sommaire, un mème est une idée simple propagée à travers le web. Elle peut prendre la forme d'un hyperlien, d'une vidéo, d'un site internet, d'une image, d'un hashtag...

la fonction de l'anonymat est donc de mettre tous les utilisateurs sur un pied d'égalité. Ce fonctionnement permet par conséquent des agissements collectifs absolvant les participants d'une responsabilité individuelle, sans pour autant supprimer la responsabilité collective.

Pendant quelques années, c'est cet idéal d'action individuellement anonyme et collectivement revendiquée qui prévaut. C'est ce qui rend la réalité et le fonctionnement d'Anonymous très difficiles à saisir. Pour les gens qui n'ont pas suivi le développement du groupe ou qui y ont encore moins pris part, cette culture de l'anonymat qui ne tolère pas de mise en avant personnelle est compliquée à appréhender. Cette difficulté a été très clairement perçue lors de l'émergence du mouvement Nuit debout[12] qui n'avait pas de leader identifié. Les médias, dont les contraintes sont différentes, ont tendance à vouloir personnifier, identifier un leader. La contextualisation est souvent omise, au profit de ce qui est susceptible d'attirer l'audimat, aux dépens de la complexité inhérente aux interactions et mouvements techno-politiques.

DES « HACKERS SOUS STÉROÏDES »

C'est ainsi que Fox News, la chaîne télé américaine conservatrice, appelle les Anonymous vers 2007. En réponse, une vidéo[17] est publiée sur YouTube ; une voix métallique derrière un simple costume sans visage y proclame :

« Le nom et la nature des Anonymous ont été ravagés, comme s'il s'agissait d'une pute dans une allée sombre, et ensuite donnés en pâture au public. Permettez-moi de le dire simplement : vous avez

12 : En 2016, en réponse à la très controversée loi El-Khomry (dite aussi loi Travail), des manifestants se rassemblent place de la République à Paris revendiquant une « nuit debout » contre la loi Travail. Le lendemain, suite à une excellente couverture média, les manifestants retournent passer la nuit place de la République. En quelques jours, le mouvement grossit ostensiblement et s'installe plus durablement. Plusieurs « commissions » sont créées, chacune en charge d'une thématique particulière. Après l'été, le mouvement s'essouffle et diminue en intensité jusqu'à se dissoudre presque complètement.

totalement loupé le coche quant à qui et ce que nous sommes. Nous sommes tout le monde et personne. Nous sommes le visage du chaos et les messagers du Jugement. Nous rions au visage de la tragédie. Nous nous moquons de ceux qui souffrent. Nous ruinons les vies d'autres personnes simplement parce que nous le pouvons. […] Nous sommes l'incarnation de cette humanité qui n'a ni remords, ni attention, ni amour, ni sens moral. […] VOUS… AVEZ MAINTENANT… NOTRE ATTENTION. »

La grandiloquence de la vidéo se moque en réalité du style de Fox News qui, dans un bref et kitschissime reportage, avait décrit le groupe comme des « *hackers sous stéroïdes* »[18]. Les Anonymous y sont présentés comme une « *machine de propagande haineuse sur Internet* », composée de pirates informatiques vivant dans la clandestinité et les bas-fonds de l'Internet, attaquant les Américains innocents, causant des ravages et allant jusqu'à menacer de bombarder les stades. Une femme, dont le visage est caché pour protéger son identité, assise dans ce qui semble être une maison de banlieue, les qualifie de « terroristes domestiques ». La caméra coupe alors brusquement pour montrer une camionnette beige qui explose. Une bande-son sinistre souligne le dialogue et accompagne ces visuels. Quand on veut être poli, on dit que « ça a mal vieilli »… Fox News, comme une bonne partie des médias traditionnels et grand public, tentait en fait d'expliquer à son public ce que sont les Anonymous.

Le lulz de la vidéo-réponse d'Anonymous illustre l'image ambivalente du groupe et du hacker. Revendiquée d'abord par les trolls et les hackers, elle évolue avec les Anonymous. Le sociologue Antonio Casilli « *explique ces comportements en termes de processus social. On est troll pour provoquer des changements dans le positionnement des individus dans les réseaux. Parfois, il s'agit de contester certaines autorités et hiérarchies qui se créent dans les forums de discussion ou dans les communautés en ligne – ces trolls sont là pour faire émerger de nouveaux contenus* »[19]. Le troll

est donc surtout un processus social, un agencement d'acteurs et de ressources (linguistiques, matérielles ou de capital social). Cela ressemble fort au hacker…

DU TROLL À L'(H)ACTIVISTE : LA GUERRE CONTRE LA SCIENTOLOGIE

Comment des gens sensiblement immatures et outranciers, des trolls nuisibles et souvent dangereux, sont-ils devenus un collectif d'un type nouveau, défendant activement des valeurs humanistes ?

On considère aujourd'hui que l'évènement significatif dans le faisceau menant à ce mouvement est la publication fuitée d'une vidéo de propagande assez déplaisante où l'acteur Tom Cruise, M. « Mission impossible » et célébrité en chef de l'Église de Scientologie, tient le rôle principal. Le contexte socio-culturel est essentiel ici : contrairement à la France, la Scientologie est très présente en Amérique du Nord où elle est également très puissante et où elle persécute ses membres qui tentent de fuir. La secte a par ailleurs un passif connu de censure, harcèlement et intimidation judiciaire. En 1995 déjà, la Scientologie tente de fermer certains forums Usenet. Cette tentative de censure par la secte et la « *guerre à la Scientologie* » déclarée par le collectif Cult of the Dead Cow la même année, ainsi que les procès faits à des journalistes danois durant dix ans, ont forgé une identité : « la Scientologie vs. Internet »[20].

Donc, une fois la vidéo de Tom Cruise publiée, l'Église de Scientologie fait comme d'habitude : des lettres de mise en demeure sont envoyées à divers sites web et la plupart obtempèrent. La vidéo est cependant gardée accessible sur d'autres sites tels que Gawker. Côté 4chan, c'est la goutte qui fait déborder le vase. Les agissements de la Scientologie sont perçus comme une violation de la liberté de penser et de la libre circulation de l'information. C'est ce qui donne naissance au Project Chanology[21], le premier

projet à visée politique issu de 4chan : *Chanology* est une contraction de « chan » (de 4chan) et « -ology » (de Scientology).

Ainsi, durant la semaine du 15 au 23 janvier 2008, le lulz se déchaîne contre la Scientologie : des sites web lui appartenant sont attaqués, la hotline est inondée de faux appels et de canulars, les fax sont saturés de fac-similés tout noirs ou montrant les fesses de certains Anonymous, des quantités invraisemblables de pizzas (non payées bien sûr !) sont livrées dans divers centres de l'Église de Scientologie…

La coordination des attaques se fait *via* IRC (*Internet Relay Chat*, un type de chat en mode texte). Les fameuses vidéos[22] d'Anonymous qui les font vraiment connaître sont créées sur le canal #press. Lequel fera plus tard sécession et sera nommé #marblecake (« gâteau marbré », d'après le goûter de son créateur ce jour-là). Le message est clair :

"We shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form […]. We recognize you as serious opponents, and do not expect our campaign to be completed in a short time frame. However, you will not prevail forever against the angry masses of the body politic. Your choice of methods, your hypocrisy, and the general artlessness of your organization have sounded its death knell. You have nowhere to hide because we are everywhere… We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

« Nous allons vous expulser de l'internet et nous appliquer à systématiquement défaire l'Église de la Scientologie en sa forme actuelle […]. Nous reconnaissons que vous êtes un adversaire sérieux et ne nous attendons pas à ce que notre campagne soit de courte durée. Cependant, vous n'allez pas sortir vainqueurs [de votre bataille] contre les masses en colère. Vos méthodes, votre hypocrisie et le manque généralisé d'élégance de votre organisation en ont sonné le glas. Vous n'avez nulle part où vous cacher

parce que nous sommes partout. Nous sommes Anonymous. Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Préparez-vous. »

LE LULZ SE POLITISE

Au début du mois de février 2008, les geeks se reconnaissant dans les missions du Project Chanology manifestent dans la rue. Un code de conduite publié le 1er février entre dans le détail. La règle n° 17 recommande de se couvrir le visage ; même si aucune invitation particulière à porter un masque n'y figure, on voit de nombreux manifestants sortir affublés du masque de Guy Fawkes, popularisé par le film culte *V pour Vendetta*. Six mois seulement se sont écoulés depuis le reportage de Fox News qui traitait les Anonymous de « *machine de propagande haineuse sur Internet* ».

L'inspiration politique est de plus en plus présente dans les actions du collectif, même si l'angle reste relativement américain. À quelques mois des élections présidentielles de 2008 éclate le scandale des e-mails hackés de Sarah Palin, la colistière de John McCain (parti Républicain). L'histoire prend rapidement une dimension politique et continue de résonner dans le paysage politique américain depuis 2008. Pourquoi un tel impact ? Sarah Palin passe sur le devant de la scène politique en 2008, lorsque le candidat républicain à la présidentielle la choisit en tant que colistière : le parti Républicain fait ainsi la place belle au Tea Party. Mme Palin est à l'époque gouverneure de l'État d'Alaska ; sa manière de gérer les affaires du département ne fait pas l'unanimité. Une représentante du parti Républicain, suspectant des conflits d'intérêts et des activités à l'éthique douteuse dans l'équipe de Palin, dépose une requête pour avoir accès à leurs échanges par e-mails. Les messages communiqués suite à cette requête ne montrent rien de concluant. Cependant, certains messages électroniques, retenus par l'administration

parce qu'ils contiendraient des « secrets administratifs », suscitent la curiosité : certains mentionnent en objet un journaliste d'investigation peu accommodant, d'autres, le candidat au poste de Palin, etc[23].

On est à l'été 2008. La course à la présidentielle bat son plein. Divers médias commencent à faire des requêtes similaires dans le cadre du droit à l'information inscrit dans la législation américaine[24]. Il apparaît alors que la gouverneure Palin a également une adresse e-mail privée, chez Yahoo!. Cela en a fait hurler plus d'un car, en tant que gouverneure de l'État d'Alaska, Madame Palin et son équipe ont des e-mails gérés par l'administration publique. Or, si ces moyens de correspondance peuvent être retenus, archivés et, si besoin, utilisés dans le cas de poursuites judiciaires, ce n'est pas le cas des adresses privées. Le fait d'utiliser une adresse e-mail privée et un téléphone personnel non homologué par l'administration publique est donc le moyen le plus simple de se dérober en cas de couac[25]. C'est une tactique connue, déjà utilisée par des cadres de l'administration Bush[26]. Pour couronner le tout, on est au beau milieu d'un scandale : Madame Palin aurait fait pression pour que son ex-beau-frère, officier de la police d'État d'Alaska, soit remercié rapidement. Apparemment, le divorce de la sœur de Madame Palin a été houleux. Cette histoire éclabousse la campagne présidentielle et le camp républicain.

Ainsi, non seulement certains des e-mails officiels de la gouverneure ne sont-ils pas communiqués aux citoyens et journalistes qui voudraient les analyser, mais, en plus, il y a des e-mails sur lesquels l'administration publique n'a aucune prise[27]. C'est dans ce contexte qu'un étudiant de 20 ans, fils d'un élu du parti Démocrate de l'État du Tennessee, et par ailleurs adepte de 4chan, réussit à s'introduire dans la boîte e-mail privée de Sarah Palin. À le lire d'ailleurs[28], cela n'aurait pas été compliqué ! Et, en effet, avec toutes les traces que l'on laisse en ligne *via* les différents réseaux sociaux, trouver les dates de naissance (disponibles sur Wikipédia),

le code postal et l'endroit où Madame Palin a rencontré son mari n'est pas difficile. Le hacker estime qu'il lui a fallu 45 minutes au total pour trouver le mot de passe. Une fois entré dans la boîte e-mail, il récupère donc une archive, fait des captures d'écran et les publie sur 4chan. Plusieurs personnes, des médias connus et indépendants tels que Gawker[29] ou bien WikiLeaks[30] se saisissent de l'histoire. La compromission prend de l'ampleur, plus à cause de la simple existence d'une messagerie privée permettant de contourner la législation, alors que des accusations pèsent sur la gouverneure, que pour son contenu. À cela s'ajoute le fait que ce compte n'est pas aussi sécurisé que les comptes gérés par l'administration, ce qui peut poser problème en cas d'échange d'informations sensibles. D'autant plus que l'époque est aux tentatives (assez souvent réussies) de compromission de comptes e-mails de peoples[31].

N'empêche, l'introduction abusive dans les correspondances privées d'autrui est un délit. L'étudiant s'y étant introduit a fait preuve de négligence en laissant de nombreuses traces. Lorsque le FBI se saisit de l'affaire, remonter jusqu'à lui se révèle relativement simple. Il est arrêté un mois après les faits et jugé. Il se défend en parlant de son action comme d'une blague potache, il avait d'ailleurs effacé de son ordinateur les contenus récupérés peu après l'intrusion dans la messagerie. Mais les juges ne voient pas l'affaire de cet œil : en s'introduisant abusivement dans le compte e-mail et en en publiant des messages, il aurait tenté d'influencer le cours de la campagne présidentielle. Le fait d'effacer les contenus récupérés est considéré comme une tentative d'obstruction à la justice. Condamné à une peine de prison, il est libéré en 2013[32].

« JE L'AI FAIT POUR LE LULZ »

Nous l'avons déjà vu, le lulz, humour agaçant, noir et quelque peu grinçant, fait partie de l'identité des Anonymous (par exemple, la manifestation anti-Scientologie d'Anonymous déguisés en zombies[33]). Il en est de même avec la nature décentralisée et

multifacettes du collectif. C'est dans ce rapport à la communauté que les agissements perturbateurs de quelques aigris du clavier deviennent intéressants. Antonio Casilli dit des trolls qu'ils « *ont un véritable rôle structurant au sein de chaque communauté – et qui plus est sur Internet, où leur présence est permanente et démultipliée. En effet, l'identification négative dont ils font l'objet permet aux autres membres de la communauté de s'identifier positivement entre eux : en faisant front contre un adversaire commun, ils font corps : "Face aux trolls, les autres sont porteurs de la norme sociale."* »[34]

Prenons un exemple concret : Oprah Winfrey, présentatrice vedette américaine. Après la vidéo grandiloquente en réponse à Fox News évoquée plus haut et la compromission des e-mails de Sarah Palin, c'est à son tour de se « faire avoir »[13].

Cela tourne autour du mème trollesque « *It's over 9000!* » qui se lisait également écrit ainsi : « It's over *NINE THOUSAAAAAAAAAAAAAAND!* » Le mème vient de la série animée populaire *Dragon Ball Z* et exprime un très grand niveau de puissance. Au départ, l'extrait vidéo se retrouve sur 4chan : c'est une private joke ; mais il gagne tellement en popularité qu'il devient un mème[14] célèbre[35]. Dans un de ses shows, la présentatrice parle des « *prédateurs sexuels* » (pédophiles)[36] et explique à ses auditeurs que ces gens-là font ce qu'ils font à cause d'Internet. Cette affirmation péremptoire et fausse agace toujours car elle est trop souvent instrumentalisée pour justifier une vision conservatrice, parfois réactionnaire et souvent répressive du numérique. Des membres de 4chan décident alors de faire du lulz : sur le forum web d'Oprah apparaît ainsi le message suivant, signé Anonymous :

13 : Ce que nous allons faire est la pire des choses à faire : expliquer une blague…
14 : Un autre mème notable dans l'histoire est Pedobear : il s'agit d'une mascotte, un ours dessiné, utilisée sur 4chan pour signaler du contenu pédopornographique. Ce dernier y est explicitement interdit, mais il arrive que des gens en publient ; l'image de Pedobear sert alors à signaler ce contenu à la modération. Le mème a longtemps été confondu avec un appel à la diffusion de contenus pédopornographiques.

"I don't forgive. I don't forget. My group has over 9000 penises and they are all raping children."

« Je n'oublie pas. Je ne pardonne pas. Mon groupe a plus de 9 000 pénis et ils sont tous en train de violer des enfants. »

Quelques jours plus tard, Oprah apparaît dans un de ses shows et lit ce message… Internet explose de rire : « *epic win* » pour 4chan, « *pwn* » pour Oprah[37]. Une blague de mauvais goût ? Oui. Une blague de mauvais goût ET qui dérange ?[38] Oui.

L'histoire devient cependant exemplaire[39] car elle met le doigt sur une idée fort populaire : « Internet = criminalité ». La dénonciation se fait entre initiés, certes, mais le sens politique n'en reste pas moins pertinent et la régulation des sites effective. On ne peut pas décider du blocage d'un site web entier uniquement parce que certains y publient du contenu manifestement illégal, même si cette fermeture est réclamée par divers partisans du tout répressif. Si le combat contre la pédopornographie est tout à fait nécessaire et légitime, il ne doit pas pour autant être instrumentalisé dans un débat public ni servir l'agenda politique d'un gouvernement[40].

Ce que montre cette anecdote, c'est la complexité des interactions et des agissements de ceux que l'on tend trop souvent à reléguer dans la catégorie « relou irrécupérable des internets ». On est loin ici de la psychologie de comptoir qui veut que l'anonymat des internautes soit à l'origine de leur comportement pénible. De même que la légende urbaine selon laquelle les jeux vidéo poussent à commettre des crimes violents, on peut entendre régulièrement quelque psychanalyste pérorer sur le prétendu « *effet désinhibant* » d'Internet[15], usant de moult qualificatifs tels que « *pervers* », « *narcissique* », etc. S'il est vrai que l'anonymat (réel ou perçu par l'internaute) permet

15 : Attention, être docteur en quelque chose ne signifie pas seulement être médecin. Cela veut dire avoir soutenu une thèse de doctorat. Exemples : http://www.liberation.fr/france/2012/06/12/twitter-a-un-effet-desinhibant_825882 ou https://www.cairn.info/load_pdf.php?download=1&ID_ARTICLE=JDP_301_0034

une hardiesse supplémentaire[16], le contexte et la permissivité des propos n'en sont pas moins importants. Des recherches récentes en sciences sociales tendent même à démontrer que nous avons tort de croire que les gens seraient moins aggressifs s'ils s'exprimaient sous leur vrai nom[17]. On est également loin des poncifs comme « *l'ère de l'anonymat en ligne est sans doute bientôt terminée* »[41] et autres stéréotypes outranciers selon lesquels il s'agit forcément d'un homme blanc, moche, à grosses lunettes. Lorsque l'on questionne les normes établies – qui plus est, avec véhémence et force rhétorique – on indispose forcément. Cette approche conflictuelle peut cependant être un outil puissant pour remodeler les espaces d'interactions entre les internautes. Au lieu de se soumettre aux règles dictées par une autorité (souvent centrale et centralisée), on les interroge et les remet en cause pour les repenser et les faire évoluer[18].

L'HACKTIVISME FACE AUX LIMITES DE LA LOI

Ce qui était un projet politique quelque peu unidimensionnel – Project Chanology – se transforme progressivement en *Anonymous Everywhere*. Ainsi, en 2009, les Anonymous soutiennent-ils

16 : Il faut distinguer le sentiment d'impunité reflété par la notion de désinhibition totale, de la propension à se laisser aller à dire des choses qu'on ne dirait pas face à des personnes nous connaissant. Ce sentiment permet une hardiesse qui peut, par exemple, autoriser à entrer en contact directement avec des personnes qu'on aurait approché difficilement physiquement (les enfants ou adolescents), parmi d'autres facteurs qui font tomber les barrières. De façon encore plus générale, comme le soulignait une personne des forces de l'ordre lors des échanges que nous avons eus, il s'agit « d'une excuse très courante des délinquants sur Internet qui ne se rendent pas totalement compte des conséquences de leurs actes. Ça n'est pas très différent du sentiment de toute puissance au volant d'une voiture ». Voir également : https://www.cairn.info/resume.php?ID_ARTICLE=JDP_301_0034.

17 : Un excellent billet de Nate Mathias, chercheur au MIT, revient sur les débuts de l'idée préconçue que l'anonymat serait la cause d'attitudes virulentes et irrespectueuses en ligne. Elle fait une analyse détaillée et accessible : https://blog.coralpriject.net/the-real-name-fallacy

18 : L'anthropologue canadienne Biella Coleman défend par exemple la thèse selon laquelle les trolls d'aujourd'hui sont les tricksters d'hier. Le trickster, que l'on peut traduire par « fripon », est une figure divine comparable à Hermès dans la mythologie grecque. Il s'agit de figures ambivalentes, porteuses de bruit, de désordre, de mouvement. Dotés du pouvoir de la communication mais le détournant en un éternel malentendu, les tricksters d'autrefois semblent en effet réincarnés dans les trolls du web d'aujourd'hui. Lire gabriellacoleman.org/blog/?p=1902.

les manifestations post-électorales en Iran, appelées « le Mouvement Vert »[42]. Toujours en 2009, ils s'attaquent aux sites web du gouvernement australien[43] après que celui-ci a pris des engagements forts en faveur de la surveillance nationale par les FAI (fournisseurs d'accès à Internet).

De nombreuses autres actions visant à protéger la liberté d'expression, notamment celle sur Internet, se multiplient. On note ainsi la publication d'un grand nombre de films pornographiques sur YouTube[44] pour protester contre la décision de l'opérateur du site d'enlever certaines vidéos. Cependant, ces actions restent épisodiques, et ne font pas les gros titres.

Pour bien comprendre ce qui va suivre, il est primordial de saisir d'abord le contexte. Permettons-nous donc une parenthèse sur les dispositifs légaux protégeant la création culturelle au sens large. La problématique posée par le droit d'auteur à l'ère d'Internet est un véritable nœud gordien et a causé une guerre juridico-politique pour le contrôle du domaine de l'immatériel. L'évolution fulgurante du numérique (Internet, matériel, moyens de création) a multiplié et amplifié les outils permettant à tout un chacun de créer et de diffuser des œuvres. Le système traditionnel de gestion de la diffusion des créations, connu également sous le nom symptomatique d'« industries culturelles », repose précisément sur la capacité d'un système à assurer la multiplication et la distribution des œuvres. Dans le jargon du domaine, on les appelle les ayants droit : les créateurs cèdent les droits d'exploitation à des organisations, privées et publiques, qui gèrent ainsi la diffusion des contenus, en échange de quoi les auteurs reçoivent des royalties.

Les tentatives d'encadrer et de limiter la distribution d'œuvres en ligne apparaissent donc avec le développement d'Internet grand public. Une quantité invraisemblable de textes législatifs, aussi bien nationaux (DMCA aux États-Unis, lois DADVSI et Hadopi en France, etc.) que supranationaux (Office mondial de la propriété intellectuelle, directives EUCD et IPRED en UE, entre autres), sont

élaborés. Suite à un lobbying intense pour le compte des ayants droit des industries culturelles, en 2009, la loi Hadopi passe en force[45] et l'entité publique du même nom est créée. Cette institution, répondant au doux nom de « Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet » a pour objectif affiché la pédagogie et l'encouragement de l'offre légale de diffusion d'œuvres sur Internet. En pratique, le travail de l'Autorité concerne principalement la poursuite des internautes mettant à disposition sans autorisation des contenus *via* des logiciels de pair-à-pair.

La loi Hadopi provoque donc une importante levée de boucliers de toutes parts accompagnée d'épisodes comiques tels que la ruse des députés PS (alors dans l'opposition) se cachant derrière les rideaux de l'Assemblée nationale pour créer un surnombre au moment du vote afin de l'empêcher[46]. Cette loi, et l'institution idoine, est, pour la France, un tournant décisif : non seulement parce qu'un nombre important de geeks s'est politisé et a commencé à s'intéresser à la manière dont le législateur se saisit de l'internet. Mais aussi parce que l'accès toujours plus facile à celui-ci a élargi l'auditoire et l'a ouvert à un public moins spécialisé. S'ensuit un jeu du chat et de la souris entre ayants droit et utilisateurs. En effet, de nombreuses études montrent que les créateurs au nom desquels ces lois sont prétendument votées ne touchent qu'une petite partie des bénéfices engrangés[19]. En face, les utilisateurs souhaitent avoir accès aux contenus quasi illimités qui se diffusent grâce à Internet. La bataille prend une autre dimension lorsque l'on comprend que les livres d'école, les supports d'apprentissage des langues, etc. sont fréquemment protégés par des régimes de droits d'auteur restrictifs. On peut donc dire qu'en pénalisant les utilisateurs qui se les procurent gratuitement, on pénalise l'accès à la connaissance.

19 : https://lesjours.fr/obsessions/la-fete-du-stream/ ; Le dernier bilan de l'action de l'Autorité est disponible : https://www.nextinpact.com/news/103307-hadopi-pres-9-millions-d-avertissements-99-condamnations-connues.htm Pour toute personne souhaitant suivre l'actualité de la question et/ou en connaître le passé animé, voir les articles de Marc Rees sur NextInpact.

On voit qu'il existe une tension réelle entre le système traditionnel de gestion des droits des auteurs et créateurs, et la diffusion de contenus à l'ère d'Internet. En effet, l'usage le plus courant, comme la consultation d'une page web, pose déjà un problème de taille : lorsque l'on charge une page web, souvent on la copie[20]. En effet, si nous regardons dans les paramètres de notre navigateur et fouillons un peu, nous pouvons par exemple constater que les médias (photos, vidéos, etc.) restent sur notre ordinateur. Il en est de même avec le streaming : il s'agit d'un téléchargement certes rapide et qui s'efface au fur et à mesure que l'on progresse dans le contenu, mais un téléchargement tout de même.

C'est dans cette optique de partage et de décentralisation et de diffusion de fichiers pair-à-pair qu'existent les torrents ; il s'agit de moyen de dissémination de contenus où chacun est aussi bien distributeur que consommateur[21]. Ce sont des logiciels tels qu'eMule, Kazaa, ou des sites tels que The Pirate Bay et MegaUpload. L'idée est simple : vous avez un contenu que vous voulez partager, vous le mettez en distribution *via* un outil dédié et tout le monde peut le télécharger. Vous bénéficiez d'une manière identique de la mise à disposition de contenus de la part des autres. Simple et rapide. Et comme plusieurs personnes peuvent être sources d'un même contenu (c'est l'aspect décentralisé), bon courage pour couper les vannes !

Ces quelques éléments remettent les choses en perspective. Au XXI^e siècle, vouloir limiter la dissémination de contenus immatériels, alors qu'Internet – et donc le domaine de l'immatériel – est omniprésent, est une véritable contradiction. Contrairement à une époque où la rareté d'un objet lui conférait sa valeur, la nôtre est celle de l'abondance. Ce glissement change fondamentalement la façon d'appréhender le monde, les règles juridico-politiques

20 : L'évolution des technologies web fait que le contenu d'une page web aujourd'hui est de plus en plus souvent généré dynamiquement en fonction d'interactions avec le serveur. Ainsi, elle n'est plus « copiée » sur un ordinateur.
21 : Souvent, BitTorrent et torrent sont utilisés de façon interchangeable. BitTorrent est, en réalité, un protocole d'échange de fichiers ; un torrent est un fichier de métadonnées utilisé par les logiciels qui le lisent.

qui souhaitent le gouverner et notre place dans cette vastitude. Les modèles économiques (*business models*) changent également pour prendre la mesure de cette abondance. Le rôle dans ce paysage d'Internet, et du numérique au sens large, est central. De plus en plus de prises de position émergent, et pas seulement de la part d'opposants farouches au droit d'auteur le plus restrictif, pour défendre une nouvelle manière de penser et de rémunérer les échanges, marchands ou non, de contenus[22].

La politisation des geeks et autres trolls révèle la tension entre une vision sclérosée du partage de créations et la manière tout à fait naturelle dont cela se fait sur Internet. Pour des gens qui savent qu'une page web est en fait copiée sur un ordinateur lorsqu'elle est consultée, il est tout simplement aberrant de vouloir limiter le partage de contenus en ligne. L'instrumentalisation de lois anti-terroristes (telles que le *Patriot Act*) pour lutter contre ce qui est considéré comme des violations des droits d'auteur est dénoncée par nombre d'internautes[47]. Le rôle des hébergeurs centralisés qui se plient aux injonctions des ayants droit et suppriment unilatéralement des contenus est décrié.

PIRATE !

C'est dans ce contexte que se propage en 2009 comme une traînée de poudre un article faisant la part belle à Aiplex Software[48], une société indienne dont le fonds de commerce est l'attaque DDoS (attaque par déni de service) contre des sites web hébergeant du contenu multimédia sous droit d'auteur[49]. Ainsi, si l'hébergeur refuse d'obtempérer et de supprimer un contenu sur demande des ayants droit, une société tierce peut recourir à des moyens illégaux pour l'accomplir. C'est comme la piraterie d'État d'autrefois, quand les pirates attaquaient les navires d'autres puissances. Le lien entre

22 : Ce livre n'étant pas l'endroit pour en parler, se référer à la bibliographie (http://www.liberation.fr/medias/2013/05/13/rapport-lescure-grand-flou-va_902650) pour trouver des ressources en français. La plupart de ces contenus sont accessibles à des personnes sans formation en droit.

ceux-ci et les États était de notoriété publique, même si, officiellement, les bateaux battaient pavillon pirate. Aiplex a été missionnée par diverses sociétés cinématographiques de Bollywood[50], mais la rumeur veut que des mastodontes américains tels que la Motion Picture Association of America (MPAA) aurait également bénéficié de ses services. Toutefois, la preuve n'en a pas été rapportée.

C'est un moment charnière pour Anonymous. Le Project Chanology a été un désaveu public mais n'a jamais eu recours à des pratiques illégales. Les manifestations physiques ont toujours été autorisées par les préfectures et autres administrations concernées. Les blagues potaches contre la Scientologie n'étaient rien de plus : pénibles, mais légales. Avec l'article sur Aiplex, la discussion change : « Puisque les grands et riches ennemis peuvent utiliser des moyens illégaux, pourquoi pas nous ? » Ce serait répondre d'égal à égal. Sur IRC[23], la proposition de riposter est rejetée avec véhémence.

Par nature décentralisés et libertaires, les Anonymous fonctionnent selon les règles de la « *do*-ocratie ». Le pouvoir décisionnaire revient à celles et ceux qui « font ». Bien sûr, toute personne qui le souhaite peut se revendiquer des Anonymous. Ainsi, même si l'opposition est forte contre l'usage de DDoS, une minorité se retrouve dans l'usage d'une tactique certes illégale mais radicale et puissante. Cette minorité, bannie des canaux IRC liés aux Project Chanology et autres projets se revendiquant de l'action dans les limites de la loi, est devenue le collectif AnonOps.

OPERATION PAYBACK : LA DÉSOBÉISSANCE CIVILE VERSION GEEK

Ne craignant pas l'illégalité, les AnonOps jouent également sur l'engouement médiatique que suscite l'annonce de l'attaque d'un site web[51]. Lorsque le jour dit, le site web est en effet inaccessible, l'effet médiatique est au bas mot décuplé[52].

23 : Voir p. 157.

Le site web d'AiPlex ne sera pas épargné. Un individu, non identifié à ce jour, s'en charge avant que les AnonOps se tournent vers de plus gros acteurs des industries culturelles. Parmi les victimes notables[53] d'Operation Payback sont la MPAA, la Recording Industry Association of America, l'étude d'avocats britannique ACS:Law, la Fédération contre le vol de droits d'auteur australienne, la boîte de nuit britannique Ministry of Sound, l'équivalent espagnol de la SACEM, le site web de l'équivalent américain de l'INPI.

La mission est simple et claire[54] :

"Anonymous is tired of corporate interests controlling the internet and silencing the people's rights to spread information, but more importantly, the right to SHARE with one another. The RIAA and the MPAA feign to aid the artists and their cause; yet they do no such thing. In their eyes is not hope, only dollar signs. Anonymous will not stand this any longer."

« Anonymous est fatigué des intérêts corporatistes qui contrôlent l'internet et réduisent au silence le droit des gens de partager l'information et même, plus significativement, le droit de PARTAGER avec autrui. La RIAA et la MPAA feignent d'aider les créateurs et leur cause ; cependant, il n'en est rien. Dans leurs yeux, on ne lit pas d'espoir, seulement des dollars. Anonymous ne supportera plus cet état de fait. »

L'action militante change et on peut se demander quel sera l'impact de ces « armes du geek », comme les appelle l'anthropologue Biella Coleman. En effet, comment se prémunir contre un collectif d'anonymes qui déploient leurs propres outils et agissent selon un consensus plus ou moins clair sur un obscur site web tel que 4chan ? Est-ce qu'une manifestation de désobéissance de ce genre pourrait évoluer et devenir « *the protest of the future* » (« *la contestation du futur* »)[55] ? Voici un intéressant retournement de situation ! Les MPAA, RIAA et autres sociétés de gestion de

droits d'auteur sont connues pour avoir fermé des sites web pour violation de droits d'auteur (partage de fichiers, donc) ; pire, des études d'avocats tels qu'ACS:Law au Royaume-Uni et d'autres aux États-Unis se sont spécialisées dans les mises en demeure d'internautes et la réclamation de sommes exorbitantes[56].

Dans ce débat, le cas d'ACS:Law est intéressant puisqu'il montre l'évolution d'Anonymous et leur impact dans le domaine techno-politique. C'est en mai 2009[57] que leur fonds de commerce principal devient la poursuite d'internautes téléchargeant des contenus à partir de sites web de partage (torrents, etc.). Il n'est pas question de quelques dizaines de lettres de mise en demeure, mais de plus de 25 000 injonctions en moins d'un an[58]. L'étude attire l'attention des autorités. ACS:Law prétend[59] que la majorité des mises en demeure n'arrivent jamais au tribunal (elles sont donc réglées à l'amiable). Pour d'autres, jusqu'à 40 % des personnes ayant reçu les injonctions ont payé[60] pour éviter les poursuites. D'après le directeur d'ACS:Law, l'étude aurait encaissé plus de 1 million de livres sterling entre mars 2009 et avril 2010[61] ; mais les deux tiers de ce montant seraient allés dans la poche du directeur, et les ayants droit n'auraient récupéré que la petite part du gâteau[62]. Des poursuites ont donc été engagées contre ACS:Law au Royaume-Uni dès l'été 2010.

Dans le cadre de ces poursuites, des éléments troublants semblent montrer que l'étude d'avocats s'est fait une spécialité du harcèlement des internautes[63]. Pour se défendre, ACS:Law engage un avocat connu pour organiser la riposte de vendeurs d'armes, de producteurs d'OGM et autres organismes de recherche peu scrupuleux. Pour ses adversaires, les agissements d'ACS:Law s'apparentaient à des campagnes de sabotage du droit de protester et du droit d'association. Ses méthodes avaient par ailleurs été décriées par des parlementaires britanniques lors des débats sur les amendements de leur loi Création et Internet. Des Lords avaient dénoncé le coût exorbitant de poursuites en violation de droit d'auteur, qualifiant ces procédés de « *chantage* »[64], et

l'engorgement du système judiciaire que la proportion d'accusations injustifiées avait provoqué[24].

Comment la décision d'attaquer ACS:Law avec des DDoS lors d'Operation Payback a-t-elle été prise ? Ce n'est pas clair. Il ne semble pas pour autant que ce choix soit le fait du hasard. Ainsi, le 20 septembre 2010, le site web de l'étude est attaqué et reste inaccessible pendant quelques heures. Le directeur de l'entreprise est resté dans les annales avec sa déclaration pétrie d'orgueil et de dédain :

"It was only down for a few hours. I have far more concern over the fact of my train turning up 10 minutes late or having to queue for a coffee than them wasting my time with this sort of rubbish." [65]

« Le site fut inaccessible pendant quelques heures seulement. Je suis plus ennuyé par mon train arrivant avec 10 minutes de retard ou par le temps que je perds lorsque je fais la queue pour prendre mon café du matin que pour ces gens qui me font perdre mon temps avec ce genre d'ânerie. »

Sauf que les quelques heures d'inaccessibilité du site font beaucoup plus de dégâts qu'un retard de train de 10 minutes. Au retour en ligne, un fichier de sauvegarde du site web est mis, par erreur ou négligeance, à disposition du public. Le fichier (de 350 Mb) contient, entre autre, des copies des e-mails envoyés par ACS:Law[66]. Bien évidemment, certains se disent alors qu'il serait dommage de ne pas profiter de l'aubaine ! Le fichier se retrouve donc lâché sur divers torrents, ce qui permet à de nombreuses personnes d'en faire des copies[67].

Le scandale qui s'ensuit cause la chute d'ACS:Law et met en pleine lumière les pratiques abusives des industries créatives et de leurs défenseurs. ACS:Law a pour habitude d'adresser ses lettres à des internautes identifiés grâce à un logiciel produisant une quantité élevée de faux positifs. Bon, passe encore, on se dit que ça arrive. Mais les témoignages[68] et e-mails fuités lors d'Operation

24 : ACS:Law se défendait d'utiliser de tels procédés.

Payback révèlent que l'étude d'avocats avait largement outrepassé ses prérogatives : la société s'est substituée à l'enquêteur, au juge et au jury, ne laissant aucun recours au présumé coupable[69]. L'accusation de téléchargement de films porno (souvent gay)[70] envers des internautes hommes mariés ou à la retraite est particulièrement prisée par ACS:Law. Pour éviter que cette accusation s'ébruite, les présumés coupables payaient 500 à 600 livres sterling à ACS:Law[71]. Les débats parlementaires sont alors relancés. Et la porte est ouverte à une autre forme d'hacktivisme…

QUAND L'HACKTIVISME RENCONTRE LES LANCEURS D'ALERTE : WIKILEAKS

Le lulz grinçant et dérangeant évolue et se transforme donc avec ceux qui rient. Le processus social qui a fait se transfigurer les trolls pénibles de 4chan en « *futur de l'activisme* » est fascinant. Un activisme irrévérencieux, certes, mais aussi très puissant et sans frontières. AnonOps justifie l'utilisation de moyens illégaux (DDoS) par un argumentaire souvent utilisé pour motiver la désobéissance (civile) : à partir du moment où l'on ne reconnaît pas la légitimité d'un système de règles, la notion de légalité est non pertinente. Une telle position est éminemment politique ; elle diffère fondamentalement de celle de formations telles que le Parti Pirate[25] qui s'inscrit dans un système politique existant et joue selon ses règles[26].

25 : Le Parti Pirate (PP) est un parti ayant pour devise : « liberté, démocratie, partage ». Son objectif est la néation de politiques publiques sur la base de la protection des droits et libertés fondamentales, aussi bien dans le domaine numérique qu'en dehors. La légalisation du partage hors marché et la lutte contre le fichage abusif en font également partie. Créé à l'origine en Suède, le PP a essainé dans plusieurs pays et a ajourd'hui des représentants élus en tant que députés dans divers parlements (dont le Parlement européen).

26 : Au moment de l'Operation Payback, les Partis Pirates américain et britannique avaient exhorté les AnonOps de cesser leurs agissements et de revenir à une contestation dans les limites de la loi. (http://www.psu.com/forums/showthread.php/245537-DDoS-attacks-on-pro-copyright-groups-Pirate-Parties-and-Operation-Payback?p=5287480) . Les PP trouvaient qu'Operation Payback était un énorme obstacle aux efforts d'acteurs plus traditionnels tels que ces partis eux-mêmes, qui essaient de changer le système en jouant selon ses règles. La réponse d' AnonOps peut être résumée à «chacun son approche, merci». La lettre ouverte d'AnonOps est toujours disponible : http://www.pandasecurity.com/mediacenter/src/uploads/2010/11/opopenlettertopp.pdf

Dans la sphère numérique et le même registre, on trouve aussi WikiLeaks. L'hacktivisme *à la* Anonymous rencontre celui des lanceurs d'alerte courant 2010. WikiLeaks, célèbre site qui prétend « ouvrir les gouvernements », a vu le jour en 2006 en Islande. Son fondateur vedette, Julian Assange, est un cyberactiviste australien. La mission que se donne alors WikiLeaks est d'exposer les secrets des gouvernements pour les soumettre à l'examen des citoyens. Une forme radicale de participation citoyenne à la gouvernance, en somme. Cet objectif – travailler dans l'intérêt commun – est particulièrement important car il est la base (et la justification aux yeux de beaucoup) du fonctionnement de WikiLeaks et de son total irrespect pour les lois des États-nations.

Les chemins des deux collectifs ne pouvaient donc que se croiser. Ainsi, par exemple, suite au lancement du Project Chanology début 2008, WikiLeaks publie en mars de la même année les « bibles » secrètes de la Scientologie, exposant au monde entier les programmes d'endoctrinement détaillés de la secte. Trois jours après cette publication, les avocats de la Scientologie menacent WikiLeaks de poursuites pour… violation du droit d'auteur ! Le choix est simple : soit les « bibles » sont retirées du site, soit l'Église de la Scientologie engage des poursuites pour contrefaçon au motif que WikiLeaks a publié des contenus soumis au droit d'auteur sans autorisation des ayants droit. Intimidation classique s'il en est. L'histoire fait alors un peu de bruit, notamment parce que WikiLeaks s'est abstenu de supprimer les documents[72], mais surtout parce que la réaction de la Scientologie a confirmé qu'il s'agissait bien de leurs contenus. Autre exemple, quand un Anonymous s'est introduit dans la boîte e-mail Yahoo! de Sarah Palin, WikiLeaks s'est empressé de publier les captures d'écran. Elles sont d'ailleurs toujours visibles sur son site web[73].

Malgré les millions de documents archivés depuis 2006, WikiLeaks n'attire véritablement l'attention internationale qu'en avril 2010 avec la publication d'une vidéo, connue sous le titre de *Collateral Murder* (« Assassinat collatéral »). La vidéo date

de 2007 et montre une intervention américaine dans la capitale irakienne, Bagdad. La vidéo est saisissante, et par plusieurs aspects : on est projeté à la place de l'opérateur d'un hélicoptère Apache AH-64 au milieu d'une frappe aérienne. On « se voit » tirer et tuer plusieurs personnes (on voit les corps s'affaisser lourdement). On apprend que les hommes sont assassinés par erreur ; il s'agit en réalité de deux journalistes de l'agence Reuters et ce que le militaire a pris pour des armes sont en réalité des caméras. La vidéo devient encore plus glauque lorsque l'on se rend compte qu'une camionnette avec une famille à bord s'arrête pour tenter de ramasser les corps. L'hélicoptère Apache tire sur la camionnette, tuant la famille (parents et enfants). On est glacé lorsqu'on entend l'un des opérateurs rire en découvrant que l'un des corps est celui d'une jeune fille, ce à quoi le pilote de l'hélicoptère répond nonchalamment : « *Bon, beh, ils n'avaient qu'à pas ramener leurs gosses sur le champ de bataille !* »

Alors, oui, la vidéo a eu un effet explosif sur les médias, les universitaires, les politiciens et les militaires du monde entier. Le fait de tirer et de tuer délibérément une famille de civils constitue un crime de guerre[74]. L'agence Reuters essayait sans succès depuis 2007 de consulter les enregistrements des conditions dans lesquelles les journalistes avaient trouvé la mort. Était-ce pour cacher ces crimes que les autorités américaines n'avaient jamais déclassifié l'enregistrement vidéo ?

Nous savons aujourd'hui que la personne ayant fourni la vidéo est Chelsea Manning[27]. Manning s'est confiée à Adrian Lamo – ex-hacker et, apparemment, petit donateur à WikiLeaks – lors d'échanges écrits dans lesquels Lamo a menti sur son identité (il a prétendu être journaliste et prêtre) et promis que les échanges resteraient confidentiels. Il a non seulement menti, mais il a aussi contacté les autorités, dont le FBI, pour leur dire que Manning était à l'origine de la fuite des documents[75]. Par conséquent,

27 : Manning est transgenre. À l'époque des faits, elle se prénommait Bradley.

Manning a été arrêtée en juin 2010, jugée par une cour militaire et condamnée à trente-cinq ans de réclusion[28]. Lors d'une conférence de hackers en juillet 2010 organisée par Emmanuel Goldstein (cofondateur de *2600*, le magazine de *phreaking*), Lamo est présent. L'émotion est forte, l'indignation l'est encore plus, il est hué et traité de « mouchard », etc.[76]

« L'IMPÔT DISSIDENCE »

En novembre 2010, WikiLeaks et ses partenaires médias (l'espagnol *El País*, le français *Le Monde*, l'allemand *Der Spiegel*, le britannique *The Guardian* et l'américain *The New York Times*) commencent à publier des centaines de milliers de « câbles diplomatiques », également transmis par Manning. Il s'agit de télégrammes provenant de la diplomatie américaine, des mémos confidentiels. Nouvelle révélation explosive : les « câbles » détaillent des faits de corruption au sommet de plusieurs États (Tunisie, Égypte, Gabon, Soudan, Libye, etc.), fournissent moult exposés de politique extérieure et intérieure de bon nombre de pays où les Américains ont une représentation diplomatique, parlent de terrorisme, relatent affaires et scandales. Le corpus[77] couvre une période allant de décembre 1966 à février 2010, autant dire une sacrée palanquée de palabres.

Les réactions[78] ne se font pas attendre : des articles de presse outrés, un groupe de travail de la CIA dont l'acronyme traduit inopinément la sidération des pouvoirs (WikiLeaks Task Force, abrégé en WTF[29]), des condamnations de gouvernements du monde entier… La réaction la plus dévastatrice vient cependant du monde des affaires. Plusieurs géants américains font écho à l'outrage de membres du gouvernement américain : Amazon

28 : Quelques jours avant de céder la place à Donald Trump, le président Obama a commué la majorité de la peine de Chelsea Manning. Elle devrait être libérée en mai 2017.
29 : Acronyme exprimant usuellement l'exaspération.

coupe promptement les accès de WikiLeaks aux serveurs, PayPal gèle le compte où arrivent les donations, Apple supprime l'appli WikiLeaks de son AppStore seulement trois jours après l'avoir approuvé, EveryDNS met un terme au contrat d'hébergement des services web du site, Visa et Mastercard bloquent tous les produits financiers (cartes, dons, etc.) liés à WikiLeaks…[30] L'ensemble de ces initiatives visent à réduire au silence l'impertinent site web et à l'empêcher de trouver les moyens de faire davantage de dégâts.

Face à cette répression violente, perçue comme une attaque sans précédent à la liberté d'expression et au droit à l'information, Operation Payback se transforme : les Anonymous lancent Operation Avenge Assange[79]. Des centaines de sites miroirs apparaissent[80] ; les sites web et les services en ligne de Visa, Mastercard, PayPal et autres sont attaqués avec des DDoS massifs.

Dans son livre[31], Biella Coleman décrit de manière très détaillée comment Operation Avenge Assange a été décidée et exécutée avant de discuter de son impact sur le collectif Anonymous en général. On y suit les discussions habituelles pour trouver un consensus : « OK, soutenir WikiLeaks est ce que veut la majorité ; mais maintenant, que faire ? » S'ensuit une longue discussion sur les cibles. En effet, le blog de PayPal a déjà été attaqué, mais le hacker n'a pas été clairement identifié (et le fait que la personne se revendique d'Anonymous ne signifie pas grand-chose). Il apparaîtra plus tard qu'un des AnonOps principaux était derrière l'attaque, un peu en mode « projet perso », pour ne pas interférer avec Operation Payback. Le débat assez enflammé fait émerger plusieurs cibles dont PayPal ; la discussion n'est plus de savoir s'il

30 : Ce qui a donné naissance à cette très belle parodie de publicité Mastercard détournée au profit de WikiLeaks http://www.dailymotion.com/video/xjp1q4 (un lulz élégant, mais non moins grinçant).

31 : *Coding Freedom – The Ethics and Aesthetics of Hacking*, E. Gabriella Coleman, Princeton University Press, 2013.

faut attaquer PayPal, mais quelle partie provoquerait plus d'impact (dont médiatique). Ces discussions ont lieu début décembre 2010. Entre le 6 et le 8 décembre, de nombreuses attaques ont lieu contre les sites web de divers services et autorités sous la bannière Operation Avenge Assange.

L'ensemble de ces attaques est l'apothéose d'Anonymous. Malgré le caractère passablement boiteux des ressources techniques (pas toujours assez de machines pour parvenir à une force de frappe suffisante)[32], l'opération cristallise l'attention et pose les bonnes questions sur la vendetta engagée contre WikiLeaks et Julian Assange : que reproche-t-on exactement à WikiLeaks et à Assange qui justifie qu'en une semaine des entreprises telles qu'Amazon, PayPal, Visa et Mastercard décident tout simplement de ne plus leur fournir de services ? Mais alors qu'on s'apprête à bloquer les soutiens financiers de WikiLeaks, il reste possible de faire des dons au Ku Klux Klan[33] *via* les services Mastercard. Qu'est-ce qui justifie cette différence flagrante de traitement ? Malgré toutes les critiques que l'on peut adresser aussi bien à Anonymous qu'à WikiLeaks, les mesures restent très agressives et injustifiées. Zeynep Tufekci, sociologue des technologies de l'information, parle d'une « *taxe dissidente* »[81].

"The real cause for concern is the emergence of an Internet in which arbitrary Terms-of-Service can be selectively employed by large corporations to boot content they dislike. What is worrisome is an Internet in which it is very easy to marginalize and choke information. The fact that information is "there" in a torrent, or openly on a website that is not easily accessible or has been vilified, is about as relevant as your right to shout at your TV.

[...]

32 : Olson, Parmy (June 5, 2012). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Hachette Digital, Inc.
33 : Le Ku Klux Klan est une organisation suprématiste blanche qui promeut des idées xénophobes et d'extrême droite. Elle fut fondée en 1865 aux États-Unis.

What the WikiLeaks furor shows us is that a dissent tax is emerging on the Internet. As a dissident content provider, you might have to fight your DNS provider. You might need to fund large-scale hosting resources while others can use similar capacity on commercial servers for a few hundred dollars a year. Fund-raising infrastructure that is open to pretty much everyone else, including the KKK, may not be available. This does not mean that WikiLeaks cannot get hosted, as it is already well-known and big, but what about smaller, less-famous, less established, less well-off efforts? Will they even get off the ground?"

« Le vrai sujet d'inquiétude est l'émergence d'un Internet où des conditions d'utilisation arbitraires peuvent être employées sélectivement par de larges corporations pour retirer du contenu qui leur déplaît. Ce qui est dérangeant, c'est un Internet où il est très facile de marginaliser et d'étrangler l'information. Le fait que cette information soit « là », sous forme de torrent ou bien ouvertement présente sur un site web qui n'est pas facilement accessible ou qui a été calomnié, est aussi pertinent que votre droit de hurler sur votre télé.

[…]

Ce que la fureur autour de WikiLeaks nous montre, c'est qu'un "impôt dissidence" est en train d'émerger sur Internet. En tant que fournisseur de contenu dissident, vous devez vous battre avec votre fournisseur de DNS. Il se peut que vous ayez besoin de payer [beaucoup] pour des ressources d'hébergement à grande échelle tandis que d'autres ont accès à la même infrastructure fournie par des services grand public pour quelques centaines de dollars par an seulement. Les infrastructures permettant de récolter des fonds sont disponibles pour plus ou moins n'importe qui, le KKK compris, mais peuvent ne pas l'être [pour vous]. Cela ne signifie pas nécessairement que WikiLeaks ne peut pas être hébergé puisque c'est déjà important et bien connu, mais qu'en est-il des plus petits, moins bien connus, moins fournis financièrement ? Pourront-ils décoller tout court ? ».

TOUT CE BRUIT POUR QUOI ?

L'un des fondateurs de l'EFF (*Electronic Frontier Fondation*) et auteur de la Déclaration d'indépendance du cyberespace (1996), J. Perry Barlow, utilise une expression intéressante pour illustrer ce qu'Operation Payback et Operation Avenge Assange ont produit : « *a shot heard around the world* », un tir entendu de par le monde. L'expression fait référence à des évènements historiques comme le début de la Révolution américaine[82] (qui a débouché sur la guerre d'indépendance des États-Unis) ou l'assassinat de l'archiduc François-Ferdinand, considéré comme l'élément déclencheur de la Première Guerre mondiale.

La motivation de WikiLeaks a été clarifiée à différentes reprises : défendre la liberté d'expression et promouvoir une plus grande transparence dans la gouvernance et des gouvernants. Mais qu'est-ce que cette détonation a produit ?

Le pouvoir d'abord. Comme le dit l'un des participants : *« Nous étions tous en train de changer. Nos conceptions du pouvoir, de ce qui est possible dans le monde, de ce qu'une personne peut réaliser avec ce nouvel outil appelé l'internet : toutes ces idées nous transformaient tellement vite qu'on sautait d'une Épiphanie à l'autre en une semaine. Niveau personnel, en ce qui me concerne, j'étais forcé de revoir l'idée que je me faisais de ce mouvement nommé Anonymous. Pendant les deux dernières années, ma perception a évolué : au départ, je les considérais comme un gang de cyber punks nihilistes, puis avec le temps, je les voyais comme une distraction gentiment ennuyeuse du côté du front de l'activisme numérique. […] Mais cette semaine [N.D.T. : pendant laquelle Operation Avenge Assange a eu lieu] a changé tout ça. »*

Et l'auteur de continuer en parlant d'Anonymous comme de « *la force la plus puissante de résistance et de changement de l'histoire humaine* »[83]. Commander X, comme il s'appelait parmi les Anonymous, est le pseudonyme d'un homme qui a traversé

les montagnes séparant l'État de Washington aux États-Unis et la Colombie britannique au Canada pour fuir la prison. Le pouvoir dont il est question reste celui du collectif. Bien sûr, les membres individuels s'enhardissent aussi, certains allant jusqu'à parler à des journalistes en se posant en « porte-parole ». Ce genre d'initiative personnelle n'est pas bien vu. Lorsque cela s'est produit peu après Operation Avenge Assange, la personne a été directement exclue du collectif : « Tu n'as même pas participé aux attaques, donc tu n'as pas partagé le risque d'une action illégale avec nous, de quel droit parles-tu en notre nom ? »[84] Se la jouer perso et sans avoir fait ses preuves n'est pas quelque chose que la *do-ocratie* tolère.

L'idée de l'hacktivisme « à la Anonymous » comme de la contestation du futur (*the protest of the future*) est présente aussi bien dans ce témoignage que dans diverses analyses[85]. Le pouvoir collectif que cette vision renferme est exaltant. Lorsque quelques semaines seulement après Operation Avenge Assange, la « Révolution du jasmin » débute en Tunisie, Anonymous s'y implique. L'idée du pouvoir libérateur renforcé et nourri par Internet voit alors ses beaux jours.

Bien sûr, cette vision est, diront certains, simpliste, voire naïve. Parmy Olson dénonce à juste titre le défaut du lulz : troller en bande organisée des gens qui ne peuvent pas se défendre (des ados, etc.) juste parce qu'on s'ennuie n'est pas un comportement positif, loin de là. La pomme de discorde principale reste cependant l'utilisation de DDoS comme faire-valoir d'un point de vue. Nous l'avons évoqué, l'usage d'outils illégaux peut être justifié par l'argument de légitimité transformant ainsi un outil illégal en un moyen de désobéissance civile numérique. En effet, on peut voir ce genre de tactiques comme de la résistance non-violente, ou même comme des *sit-in* virtuels[86]. De plus, comme on vient de l'évoquer, les campagnes ne ressemblent pas vraiment à celles que l'on connaît habituellement de la part d'entités contestataires : il n'y a pas des mois de préparation attentive

en amont du jour J. C'est plutôt une contestation sauvage, un flashmob continu. La *do-ocratie* et le hasard des présences sur IRC modulent ainsi le visage de chaque acte de contestation. Il est évident que, numérique à part, ce type d'action contestataire n'a rien de nouveau : une Rosa Parks s'asseyant dans le carré de places réservé aux Blancs dans le bus ou les Femens s'introduisant dans un rassemblement du FN ne sont que quelques exemples parmi d'autres de contestation violant la loi en vigueur. C'est un débat politico-philosophique qui se joue ici autour des formes acceptables, ou encore optimales, de militantisme et d'activisme d'opposition.

Mais il ne s'agit pas seulement de la légalité de l'outil. Beaucoup de personnes, journalistes et chercheurs, qui n'ont pas nécessairement de problème avec le recours à des pratiques illégales, ont dénoncé l'usage de DDoS comme une façon de faire ce que l'on dénonce. Vous lancez une attaque DDoS pour dénoncer le fait que des études d'avocat à la solde de multinationales d'ayants droit vous privent de votre droit fondamental d'accès à l'information ? Mais pendant que le site web ciblé par votre DDoS est inaccessible, vous empêchez ces mêmes gens d'exercer leur droit fondamental à l'expression libre, non ? Il serait sans doute hypocrite de pleurer sur le triste sort d'un géant tel que PayPal, dont le site est tombé pendant une petite heure, ou de compatir aux malheurs d'ACS:Law. Cet argument tient donc jusqu'à un point : la liberté des uns s'arrête où commence celle des autres... Sans parler du fait que rendre inaccessible le site web de PayPal pendant une heure ne constitue pas un obstacle à leur liberté d'expression exercée sur des blogs, par des employés, des communicants, des pubs, des lobbyistes, etc. En fait, rendre des services électroniques inaccessibles *via* une attaque DDoS est surtout problématique pour les petites organisations, celles qui n'ont ni les moyens ni les ressources pour faire face et pour qui une interruption de service peut causer de véritables passages à vide.

Si la discussion autour de l'utilisation de DDoS comme outil de résistance à l'ère d'Internet peut continuer à l'envi, les Anonymous décident de ne pas s'y noyer. En réalité, la constatation est rapide : actions spectaculaires = titres de presse sensationnalistes. Comme ceux-ci ont une durée de vie fort réduite, le collectif décide de changer d'approche et de porter la contestation d'une manière différente.

ANONYMOUS EVERYWHERE : NOUVELLES STRATÉGIES, NOUVEAUX COMBATS

Fin 2010-début 2011 marque le début des « révolutions arabes ». Comme nous le disions, rien n'évolue dans le vide : les « câbles » diplomatiques de WikiLeaks concernant des figures politiques du monde entier contenaient aussi une bonne quantité de rapports sur le pouvoir en place en Tunisie et en Égypte. Ainsi, lorsque la publication des télégrammes débute, WikiLeaks crée divers partenariats ; parmi ceux-ci, le site tunisien d'information indépendante Nawaat. Ses membres récupèrent les « câbles », les traduisent en français et lancent TuniLeaks dans la foulée. Ces documents révèlent ce que tout le monde en Tunisie sait déjà : la corruption la plus folle règne au palais présidentiel. Outre ces preuves de malversations et abus de biens sociaux, les Tunisiens apprennent des détails sur le régime alimentaire du tigre du gendre de Ben Ali, le président dictateur tunisien de l'époque. Et à peine trois semaines plus tard, un vendeur de légumes s'immole dans la ville de Sidi Bouzid, lançant ainsi la « Révolution du jasmin » qui déboulonna Ben Ali du pouvoir.

Les Anonymous prennent de leur côté contact avec des activistes tunisiens. Leur popularité contribue à attirer l'attention des médias internationaux. Petit à petit, ses membres s'impliquent dans le mouvement contestataire en Tunisie, en partie parce qu'ils sont mécontents de la censure des « câbles » de TuniLeaks par le gouvernement en place : c'est OpTunisia[87]. Au tout début de 2011,

à peine après le jour de l'An, l'équipe de résistance numérique se fait plus active. Il n'est cependant plus question de faire seulement des DDoS contre des sites de ministères et d'administrations publiques : il faut quelque chose de plus solide. Diverses vulnérabilités sont exploitées : des bases de données gouvernementales sont compromises, le site web du Premier ministre tunisien affiche pendant un moment le message d'Anonymous en soutien à la révolution populaire, etc. Un petit script pour le navigateur Firefox est développé pour permettre aux Tunisiens de naviguer sur le web sans censure gouvernementale[88], une création que d'aucuns ont nommé « *an artful hack* » (soit un hack ingénieux). Le reste appartient à l'Histoire.

Le 25 janvier 2011 débute la révolution égyptienne. En accord avec les demandes des contestataires dans la rue, Operation Egypt n'attaque pas les médias (à la botte du gouvernement de l'époque) ni n'appelle à la violence. Dans ce cas, l'aide principale est venue du groupe Telecomix[89], un autre collectif d'hacktivistes avec « *une passion radicale pour la liberté* »[90] : fourniture d'outils tels que des VPN et Tor (voir chapitre 03), établissement de relais IRC vers Twitter permettant aux gens dans les manifestations d'envoyer, en tapant sur IRC, des tweets et ainsi de laisser sortir l'information vitale à propos de ce qu'il se passait sur place. Le 28 janvier est un jour de répression policière extrêmement violente et de black-out après la décision de l'ex-président égyptien Moubarak de bloquer l'accès à Internet dans le pays. Le groupe Telecomix travaille d'arrache-pied pour le rétablir, en se servant de vieux modems (ceux que nous avions autrefois, crachotant, bipant et dont la connexion passait par le téléphone). Avec l'aide d'Anonymous, les deux groupes d'hacktivistes récupèrent tous les vieux fax en état de marche en Égypte. Ils permettent de rétablir des communications, d'envoyer des explications pour les premiers soins et de recevoir témoignages et annonces d'Égypte. Le black-out médiatique est contourné. Bien sûr, le lulz y a aussi eu son rôle. Des membres d'Anonymous se déridٍent en commandant

des centaines de pizzas (toujours sans les payer !) pour les faire livrer dans les ambassades tunisiennes et égyptiennes de divers pays occidentaux.

L'implication d'Anonymous à travers OpTunisia et Operation Egypt[34] démontre non seulement que s'impliquer auprès de ceux qui ont besoin d'aide est important, mais également que certains principes ne souffrent pas d'exception. Par exemple, plusieurs nouveaux venus sur les canaux IRC d'Operation Egypt ont réclamé à cor et à cris qu'Anonymous fasse ses tours de magie et DDoS les sites web de divers médias parce qu'ils étaient sous contrôle gouvernemental. Les demandes ont été systématiquement rejetées : ce n'est pas parce qu'on n'aime pas ce qu'un média écrit qu'on doit l'empêcher de le faire. L'hacktivisme se veut une histoire de justice sociale et de respect des droits fondamentaux, pas une bande de justiciers capricieux lynchant des groupes de personnes pour le goûter. Afin de remettre les choses au clair, les membres des différents groupes d'hacktivistes créent alors un document intitulé *How to Protest Intelligently* (« Comment manifester intelligemment »)[91]. Une bonne partie des approches et outils numériques développés pour OpTunisia et Operation Egypt a été réutilisée dans d'autres pays de l'Afrique du Nord et du Moyen-Orient, jusqu'en Iran[92].

LULZSEC : LA VENGEANCE DU LULZ

Les Anonymous s'impliquent de plus en plus dans des combats politiques et humanistes. Pendant que tous les yeux sont braqués sur la fuite du dictateur tunisien Ben Ali mi-janvier 2011 et la démission de son collègue égyptien un mois plus tard, une société de sécurité informatique américaine, HBGary Federal, se retrouve dans l'œil du cyclone.

34 : J'ai suivi ces opérations de très près en tant que chercheur et écrivain, sans prendre parti à ce qu'il se faisait.

Le P.-D.G. de HBGary Federal s'est déjà vanté en 2010 d'avoir utilisé des méthodes d'ingénierie sociale et d'investigation à sources ouvertes pour démasquer des membres d'Anonymous[93]. Il est apparu plus tard qu'il souhaitait vendre ces informations au FBI. Début 2011, ce monsieur se vante encore plus fort que ça y est, voici les noms des coupables. Le 5 février 2011, une attaque informatique d'envergure vise HBGary Federal[35] : non seulement le site web est rendu inaccessible, mais les bases de données et les e-mails sont récupérés par les attaquants, et le compte Twitter du P.-D.G. est compromis. Ensuite, les choses prennent des proportions vertigineuses.

Les attaquants récupèrent des rapports, des présentations PowerPoint et des documents qui ressemblent fort à des réponses à des appels d'offres émis par le Gouvernement fédéral et quelques agences de sécurité et de renseignement. Un peu comme à l'époque de la chasse aux sorcières sous le maccarthysme, les documents fournissent moult détails sur la stratégie que HBGary Federal et ses acolytes proposent de lancer à l'encontre de WikiLeaks, de ses donateurs et de divers journalistes couvrant les fuites (Glenn Greenwald entre autres). Les documents prévoient également de produire des contenus prenant des libertés avec la réalité (des « *fakes news* »). En outre, HBGary Federal a répertorié une quantité plutôt impressionnante de *0days* (voir chapitre 01) et détaille dans des échanges d'e-mails l'intention de vendre ceux-ci au plus offrant. Ces e-mails et les montants en jeu (plus de 2 millions de dollars[94]) constituent une des premières preuves tangibles d'un tel marché. Par ailleurs, les techniques de surveillance de la concurrence et de cibles d'intérêt stratégique décrites dans ces documents prennent également des libertés avec la loi et ce qui est permis dans le domaine de l'intelligence économique. Assez normal pour une entreprise privée qui se voit alors, sans se départir de son arrogance, comme « *la CIA privée* ».

35 : Une excellente explication (même si un peu technique par endroits) : http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

Ainsi, même si les informations obtenues l'ont été avec des moyens illégaux et sur la base d'un désir de vengeance plutôt que motivés par de grands idéaux, ces documents ont permis de saisir un peu plus clairement la mesure des capacités de surveillance privée, à visée économique entre autres, qui existent[36].

Le hack de HBGary Federal intervient alors que le FBI commet une série d'arrestations suite aux DDoS d'Operation Avenge Assange. Dans les e-mails de HBGary Federal, il est question de récupérer de nouveaux contrats avec les agences de renseignement telles que le FBI en leur vendant les noms des Anonymous prétendument identifiés ainsi que les services pour en identifier d'autres à l'avenir. L'arrogance du P.-D.G. de l'entreprise qui suinte de ces e-mails n'arrange pas les choses. La vengeance continue… Le dimanche 6 février 2011, alors que les Américains regardent le Super Bowl, le compte Twitter personnel du P.-D.G. est compromis et se met à déverser un tas de mots haineux, de vulgarités et de propos racistes ; les e-mails privés et professionnels du bonhomme sont donnés en pâture *via* The Pirate Bay ; son adresse personnelle, ses problèmes de couple et ses vantardises professionnelles sans fondements sont exposés. Par la suite, HBGary Federal sera racheté par une grande entreprise de sécurité également engagée dans l'identification d'Anonymous, dont ceux impliqués dans cette attaque.

« SE MOQUER DE VOTRE SÉCURITÉ »

Vu l'engagement politique d'Anonymous et le parti pris pour des « fuites éthiques » (*ethical leaks*), certains estiment nécessaire de suivre une autre voie : LulzSec est né, même si ses membres ne se détachent pas complètement d'Anonymous. Le leitmotiv de LulzSec est assez clair : *Laughing at your security* (« Se moquer de votre sécurité »). Contrairement à Anonymous, où plusieurs

36 : Nous reviendrons sur la figure ambivalente du lanceur d'alerte dans le chapitre suivant.

chercheurs et journalistes sont admis sur des canaux IRC dédiés, LulzSec ne parle qu'à une seule personne externe : la journaliste de *Forbes*, Parmy Olson. La touche LulzSec ? Des contenus publiés via le service web pastebin, un compte Twitter irrévérencieux et le Nyan Cat[37], le chat animé pixellisé gris qui fait sortir un arc-en-ciel infini de son derrière. Le porte-parole virtuel du groupe est aux antipodes de cette imagerie : on le reconnaît facilement à son monocle, son chapeau melon et ses moustaches fines de dandy français.

Vers la mi-avril 2011, LulzSec s'introduit dans les systèmes informatiques de la chaîne conservatrice Fox News. Comme il n'y a pas de saillie particulière de la part de Fox, les données volées ne sont pas rendues publiques. Entre mai et juin 2011, LulzSec se déchaîne : vous vous souvenez probablement de la fuite massive de données personnelles chez Sony Pictures. Comme le note NextInpact, « *le pire selon le groupe est que la totalité des données ne disposait d'aucun chiffrement : les mots de passe étaient ainsi stockés en clair sur les serveurs. Pour LulzSec, il n'y avait donc plus qu'à "se servir". Les hackers estiment qu'avec un si faible niveau de protection, Sony demandait pratiquement à être piraté. L'affichage en clair des informations est une faute conséquente, surtout lorsque l'on sait que n'importe quel système*

37 : https://en.wikipedia.org/wiki/NyanCat/

d'exploitation moderne propose un chiffrement à la volée des données chez le particulier. »[95] Le site web de la CIA, celui d'une ONG affiliée au FBI, des sites web de contenus pour adultes ainsi que plein de sites de jeux vidéo populaires y passent. Et presque à chaque fois, les bases de données personnelles des utilisateurs de ces sites web sont rendues publiques.

La motivation de LulzSec n'est donc pas l'argent[96], mais bien le lulz et le chaos que leurs actions[97] ne manqueront pas de provoquer[98]. Le message politique est occasionnel et porte surtout sur l'emprisonnement de Chelsea Manning[99] (source de WikiLeaks, voir page 174). De nombreux hackers font de leur mieux pour empêcher ces actions[100] et démasquer les membres de LulzSec[101]. Les motivations sont alors diverses : patriotisme[102], désaccord avec l'exhibition publique de données personnelles de milliers de personnes, etc. Encore une fois, on peut vivement critiquer les méthodes employées ou encore le temps qu'ils font perdre aux autorités qui doivent traiter les plaintes pour les piratages faits pour le lulz. Mais de nombreux spécialistes de la sécurité informatique[103] ont trouvé que les actions de LulzSec ont fait passer un message très clair : la sécurité des systèmes et des services en ligne n'est pas accessoire, ce n'est pas une dépense inutile pour les entreprises, ce n'est pas un élément anodin de la vie de l'internaute. En effet, il faut garder à l'esprit qu'exploiter les vulnérabilités n'est pas l'apanage de LulzSec, et que, contrairement à d'autres, les membres de LulzSec n'ont jamais vendu les données obtenues dans ces compromisions. Et s'il est sordide de retrouver ses identifiants dans une fuite de comptes personnels en provenance de www.pr0n.com, il ne faut pas s'étonner de voir son compte Facebook compromis quand on se contente d'identifiants tels qu'un login « admin » et un mot de passe « 123456789 »[104]. Il y a dorénavant un avant et un après LulzSec[105].

Les membres de LulzSec sont arrêtés, jugés et condamnés à des peines diverses. LulzSec court définitivement à sa perte

lorsque Sabu, un de ses membres les plus actifs, se mue en informateur pour le FBI. Les membres de LulzSec sont arrêtés, jugés et condamnés à des peines diverses.

OPERATION ANTISEC, LA FIN D'UNE ÈRE

LulzSec et Anonymous se retrouvent en juin 2011 dans le cadre d'AntiSec, une série d'attaques, de hacks et de fuites ciblant les agences de renseignement, les banques et des entreprises dont le fonds de commerce est la sécurité informatique. Le but ? Dénoncer et empêcher le fonctionnement de toutes sortes d'organisations responsables de la censure et la surveillance sur Internet[106], ainsi que celles qui font du profilage racial et usent et abusent de lois répressives sur le droit d'auteur[107]. Le lancement d'AntiSec est également concomitant avec la transformation de Sabu en mouchard du FBI.

Des quantités phénoménales de données issues de différentes institutions de police sont rendues publiques. On apprend que le FBI étudie un programme spécial de monitoring prévisionnel d'individus susceptibles d'enfreindre la loi. AntiSec s'est attaqué, avec un succès quelque peu mitigé, à Booz Allen Hamilton, l'employeur d'Edward Snowden. Ce qu'AntiSec n'a pas pu obtenir en 2011, Snowden l'a fait fuiter en 2013. C'est d'ailleurs grâce à ces documents que l'on a relevé la première preuve tangible d'interférence gouvernementale (*via* attaques DDoS) dans les réseaux et outils numériques utilisés par Anonymous[108].

En plein milieu d'Operation AntiSec, divers membres de LulzSec et d'Anonymous sont arrêtés. C'est de cette époque que vient la phrase poético-révolutionnaire : "*You cannot arrest an idea*"[109] (« Il est impossible d'arrêter une idée »). Plus tard, lorsque lumière est faite sur le rôle d'informateur de Sabu, ces arrestations commencent à faire sens : les hacktivistes ont été donnés aux autorités. Le « Sabutage », jeu de mots (grinçant) entre Sabu

et sabotage en vogue à l'époque, a également mis en évidence d'autres secrets, par exemple l'implication et le rôle très ambivalent du FBI dans le hacking et le vol de données de la société Stratfor. Operation AntiSec avait en effet mis la main sur une quantité non négligeable de données client de Stratfor (e-mails, numéros de carte bancaire, etc.), entreprise dont le fonds de commerce est le renseignement géopolitique. Ces intrusions et fuites ont compté Sabu, alors déjà informateur depuis plusieurs mois du FBI, parmi les participants les plus actifs. La raison de l'inaction du FBI qui, forcément au courant, aurait pu contribuer à l'amélioration de la sécurité de Stratfor n'est toujours pas claire. Quoi qu'il en soit, les données récupérées chez Stratfor ont été fuitées *via* WikiLeaks à qui des membres d'AntiSec ont fourni la totale pour vérification et publication. Il n'en reste pas moins que le FBI, *via* Sabu et donc indirectement AntiSec, a réussi à compromettre et à s'introduire illégalement dans les systèmes informatiques de divers pays[110].

ANONYMOUS : QUEL HÉRITAGE ?

Comme depuis ses débuts, Anonymous continue à être un collectif multifacette dynamique. En janvier 2012, il participe, aux côtés d'acteurs du numérique tels que Wikipédia, Google, etc. au Blackout Day (le 18 janvier), une web-manifestation contre les projets de loi SOPA et PIPA ; pour afficher son opposition, chaque site web participant noircit ses contenus pour montrer à quoi il ressemblerait si les lois SOPA et PIPA entraient en vigueur. L'action est suivie par des milliers de sites partout dans le monde, y compris en France. Le lendemain, le site MegaUpload disparaît du web et son fondateur Kim Dotcom est arrêté. Anonymous entreprend alors sa plus grande campagne de DDoS (plus importante encore que lors d'Operation Payback et Operation Avenge Assange) : des dizaines de sites web d'organisations d'ayants droit sont rendues inaccessibles.

La réaction au suicide d'Aaron Swartz, le cofondateur du site web Reddit, est également suivie d'un déchaînement. Swarz était un activiste connu et un acteur respecté de la communauté scientifique et technique[38]. Pour beaucoup, son suicide a été un acte de désespoir face au harcèlement judiciaire qu'il subissait pour avoir rendu accessible une base de données de publications scientifiques pendant son temps au MIT. Le seul agissement illégal dans son cas avait été d'aller à l'encontre de la règle absurde, en vogue dans les milieux scientifiques, qui commande de payer à des éditeurs le droit de lire des publications déjà payées par le contribuable. En guise de punition, il encourait trente-trois ans de prison. Anonymous a également permis de découvrir et de constituer des preuves suffisantes dans différents cas d'abus sexuels, en révélant un viol collectif à Steubenville, en traquant les auteurs de contenus *revenge porn* sur divers sites web, etc.

Bien sûr, le propos n'est pas de justifier ni glorifier des actions de ce que d'aucuns pourraient considérer comme des justiciers 2.0, mais de souligner leur importance en tant que catalyseurs de débat public autour de problématiques ignorées ou souffrant d'un manque d'attention chronique. Plus encore, ces actions (et tant d'autres) permettent de mettre en exergue des processus sociaux, politiques et même économiques de mise en danger de certains citoyens à cause de leur couleur de peau, de leur genre ou de leur situation professionnelle. Ce n'est pas un hasard si des membres d'Anonymous et de LulzSec s'engagent dorénavant auprès d'associations et d'ONG respectées telles que *Privacy International,* ainsi qu'auprès de partis politiques tels que le Parti Pirate, influençant à leur manière la vie politique au sens large et ses évolutions[39]. Anonymous et AntiSec ont également inspiré d'autres personnes et collectifs pour trouver des moyens

38 : Un documentaire a été réalisé en sa mémoire : *The internet's Own Boy*. https://www.youtube.com/watch?v=7ZBe1VFy0gc

39 : Leurs déboires avec la justice ne se sont pas toujours soldées par des peines lourdes, d'où un engagement plutôt public.

d'accès aux documents d'entreprises privées commercialisant des technologies à double usage auprès de gouvernements dictatoriaux.

L'héritage, si l'on peut dire, d'Anonymous et des opérations diverses que nous avons détaillées jusqu'ici est une prise de conscience majeure de ce qui est possible. C'est aussi une foulitude d'hacktivistes, lanceurs d'alerte et journalistes qui continuent à veiller à ce que les démocraties survivent.

03

LE LANCEUR D'ALERTE : TRAÎTRE OU JUSTICIER ?

Nous avons déjà brièvement évoqué le site WikiLeaks, lancé le 4 octobre 2006. Même s'il fait très vite fuiter des documents (sur la Scientologie, sur la Somalie, sur le Kenya ou Guantanamo…), il ne devient un acteur important qu'en 2010, avec la publication de *Collateral Murder*. Suit la publication des « câbles », fin 2010, soit 250 000 télégrammes diplomatiques américains, qui connaît un retentissement international. Si, au fil des années, WikiLeaks continue ses actions, son positionnement évolue, comme toute la sphère numérique.

« Bon, la question de WikiLeaks est une question compliquée, qu'on ne réglera pas en trois minutes. Mais disons qu'il y a d'abord le problème d'Assange lui-même, coincé depuis quatre ans dans l'ambassade d'Équateur à Londres et sous le coup d'une demande de mandat d'arrêt international émis par la Suède, où il est accusé de viol mineur. Il y a aussi les accusations de faire le jeu de la Russie – Assange a eu en 2012 une émission sur Russia Today, télévision financée par le Kremlin – mais surtout, les Russes sont fortement soupçonnés d'être derrière le piratage de 20 000 mails du parti Démocrate qui ont été publiés par WikiLeaks à la fin du mois d'août [2016]. »

Ainsi s'exprimait Xavier de la Porte dans sa chronique quotidienne[40] sur la radio France Culture en octobre 2016. Et de compléter en questionnant le rôle de WikiLeaks dans l'écosystème de l'information ; puis, par voie de conséquence, la manière dont fonctionnent les systèmes de gouvernance de nos pays.

« Donc, oui, WikiLeaks est devenu un objet très ambigu, ce qui fait l'affaire de tous ceux qui, depuis le début, dénoncent les objectifs et le mode de fonctionnement du site. Mais il y a à mon avis d'autres questions. »

Oui, WikiLeaks a changé à jamais la manière dont l'information circule et a profondément influencé les rapports de forces en présence. Cependant, l'impression de regarder un combat de boue demeure et laisse un goût amer. Et rien ne permet de dire qui gagne, on sait seulement qui perd. Retour sur dix ans de tumultes.

LES LANCEURS D'ALERTE : UNE NOUVELLE FORME DE JOURNALISME ?

WikiLeaks n'a pas inventé les lanceurs d'alerte, loin s'en faut. Il n'a pas non plus inventé le journalisme d'investigation, il n'y a qu'à voir la longévité de l'hebdomadaire satirique *Le Canard Enchaîné*. En fait, c'est une autre façon de faire du journalisme qui s'est développée. La manière de WikiLeaks est unique en ce qu'elle se concentre autour de la manipulation d'outils numériques complexes : pour faire fuiter des informations, les lanceurs d'alerte doivent passer par des outils chiffrés et sécurisés ; pour les extraire de la masse de fichiers et leur donner un sens, les journalistes doivent savoir se servir d'outils logiciels de fouille de données. La capacité de les transcrire, de raconter une histoire, ne vient qu'après.

40 : http://www.franceculture.fr/emissions/la-vie-numerique/wikileaks-10-ans-et-quelque-chose-change. Le terme « viol mineur » est quelque peu étrange et même choquant mais il semble une bonne traduction d'un crime considéré comme tel par la loi suédoise : https://www.theguardian.com/media/2010/dec/17/jullian-assange-p-and-a.

« Wikileaks a eu un rôle très important dans la mise au jour de certaines informations. »

Maxime Vaudano, journaliste au *Monde*
et datajournaliste pour Les Décodeurs

RS : Qui es-tu et comment en es-tu venu à travailler avec les Panama Papers ?

MV : Je travaille au Monde.fr depuis 2013, et comme datajournaliste aux Décodeurs depuis la création de la rubrique en 2014.

C'est en tant que datajournaliste que j'ai été amené à intégrer la cellule d'enquête sur les Panama Papers en 2015, pour apporter un regard et des méthodes un peu différentes des enquêteurs traditionnels.

RS : Est-ce la première fois que tu travailles sur des informations fournies par des lanceurs d'alerte ?

MV : Oui. D'habitude je travaille plutôt sur des sources ouvertes, avec une vocation de pédagogie et de mise en forme de l'info.

RS : J'ai deux questions déguisées en une. Si l'on y regarde de plus près, on ne peut pas dire que WikiLeaks fait du journalisme. Quel est ton positionnement sur le rôle d'intermédiation que ces différents acteurs pourraient ou devraient avoir ?
L'exemple des Panama Papers est très pertinent dans la mesure où l'implication de journalistes a été significative et il s'agit du leak le plus important à ce jour en termes de volume de données. Les informations divulguées l'ont été de manière toujours constructive, digne et respectueuse. WikiLeaks ne peut pas se vanter d'agir

ainsi en toutes circonstances. Que peut-on dire de son évolution, sur le plan éthique par exemple ?

MV : Wikileaks a eu un rôle très important dans la mise au jour de certaines informations. Je pense qu'il gagnerait à collaborer avec des médias plutôt que de publier des informations brutes. Cela donne plus de crédibilité aux informations (qui peuvent être vérifiées), et les rend surtout beaucoup plus accessibles et compréhensibles au public. Typiquement, les révélations récentes sur la CIA ont eu beaucoup moins d'impact que celles de Snowden, non seulement parce qu'on « savait déjà », mais aussi parce que le travail journalistique était moins poussé. De même, Wikileaks a un impact très faible dans ses révélations sur les accords de libre-échange (TPP, TISA, etc.), contrairement à Greenpeace qui collabore avec les médias.

Sur les Panama Papers, cette intermédiation était encore plus importante, car :

– il y avait un enjeu de protection des données personnelles, qui fourmillaient dans les documents (numéros de téléphone, adresses personnelles, informations sur la vie privée, etc.) ;

– il y avait un énorme enjeu de mise en contexte des données et d'enquête derrière (le simple fait qu'un nom apparaisse dans les Panama Papers ne signifie pas qu'il ait une société offshore, et encore moins qu'il ait fait quelque chose d'illégal).

Wikileaks est aujourd'hui dans une démarche très militante, qui affaiblit à mon sens son image et la crédibilité de ses révélations (ce qui n'empêche pas qu'elles peuvent être authentiques et intéressantes). Je ne dis pas qu'il faudrait absolument qu'ils travaillent avec des grands médias, mais ils gagneraient à s'entourer de personnalités plus « indépendantes » pour analyser et crédibiliser leurs documents.

Aujourd'hui donc, ce type de fuite fait presque partie du quotidien… Des fichiers sont rendus publics en masse. Ils concernent une grande variété de sujets : l'évasion fiscale (LuxLeaks, Panama Papers), les dessous cradingues du foot (Football Leaks), etc. Les documents sur l'optimisation fiscale à grande échelle connus sous le nom de Panama Papers sont par exemple la plus grosse fuite de données réussie à ce jour, et cela ne fait que préfigurer des changements encore plus grands. Certains des plus grands *leaks* publiés par Julian Assange ont été fournis par les Anonymous. Mais WikiLeaks n'a pas attendu les hacktivistes de 4chan pour faire des révélations (assassinats extrajudiciaires et corruption au Kenya, gestion de la prison de Guantanamo, etc.). Et ces faits d'armes journalistiques lui ont valu des prix prestigieux de la part d'Amnesty International et d'Index of Censorship.

L'existence de WikiLeaks a donc changé la manière dont on perçoit l'information et le rôle du journalisme. Ce dernier est nommé « le quatrième pouvoir » pour illustrer l'ensemble des moyens pouvant servir de contre-pouvoir face aux trois pouvoirs incarnant l'État (pouvoir exécutif, législatif et judiciaire)[111]. Wiki-Leaks a certes irrémédiablement altéré le fonctionnement de ce quatrième pouvoir, mais a-t-il pour autant changé quelque chose au fonctionnement de nos démocraties ? C'était, il faut s'en souvenir, le but premier de Julian Assange. Mais, ceux qui, à l'apparition de WikiLeaks, ont défendu la nécessité du secret, ceux qui ont dénoncé les méfaits de l'idéologie de la transparence, ont eu le temps de se rassurer : WikiLeaks n'a pas vraiment rendu l'exercice du pouvoir plus transparent[41].

41 : Comme le soulignent certains détracteurs, l'absence de transparence dans le fonctionnement de WikiLeaks lui-même n'a pas joué en faveur de cet idéal. La critique peut être un peu facile : elle occulte notamment la question de la sécurité de ceux qui font WikiLeaks.

COMMENT ÇA MARCHE EXACTEMENT, WIKILEAKS ?

WikiLeaks est un média en ligne dont l'objectif principal, on l'a dit, est la dissémination de documents originaux provenant de sources anonymes, le plus souvent des lanceurs d'alerte. Lorsque l'attention du monde se porte sur WikiLeaks en 2010 avec la publication de *Collateral Murder* et des « câbles » diplomatiques américains, l'entité se définit comme une organisation à but non commercial. Dans la définition actuelle, cette mention n'existe plus[42].

Nous l'avons vu, WikiLeaks publie divers documents secrets dès avant 2010. En dix ans, le mode d'action de l'organisation évolue constamment. Entre 2006 et 2008, le site fonctionne comme un wiki : chacun peut non seulement lire, mais également publier et éditer des contenus. De cette façon, le lectorat a un rôle actif dans le choix de ce qui est accepté pour publication et de la manière dont ces informations sont publiées. C'est pourquoi on y trouve du matériau « brut » : les contenus sont publiés tels quels, pratiquement sans intervention éditoriale.

Puis cette approche change, particulièrement lors de la diffusion de *Collateral Murder* en avril 2010. La vidéo est très bien travaillée et montée pour constituer une déclaration politique à elle seule. De nombreuses critiques sont adressées à WikiLeaks concernant le montage et, sans surprise, les mécontents parlent de désinformation. Des enquêtes judiciaires ultérieures prouveront que le montage de *Collateral Murder* n'a en rien altéré le document original pour le rendre plus choquant. C'est même plutôt le contraire puisque des scènes encore plus néfastes pour l'armée américaine n'y figurent pas. Là où on peut donner raison à ses critiques, c'est que, en effet, cette vidéo est un produit politique et vise à exprimer un point de vue politique, pas seulement à informer.

42 : https://wikileaks.org/What-is-Wikileaks.html (dernière mise à jour publiquement affichée : 3 novembre 2015)

L'évolution de WikiLeaks se poursuit avec les « câbles » diplomatiques : c'est la première fois que WikiLeaks travaille en étroite collaboration avec des médias reconnus. Ainsi, les télégrammes – le « matériau brut » – ne sont-ils pas seulement lus et édités dans la foulée[112], ils sont également publiés et analysés[113]. Ce traitement de l'information permet alors de montrer l'impact de ces communications sur les interactions politiques mondiales. Avec cette approche, nous sommes à des années-lumière d'une publication brute. Nous mettons également de côté le produit informationnel promouvant un point de vue politique singulier. En effet, chacun des médias a accès à la totalité des « câbles » et peut travailler selon l'angle et les problématiques qui s'en dégagent, en accord avec sa propre ligne éditoriale.

Ce modèle perdure pendant plusieurs années. En 2011, WikiLeaks rend publics des documents révélant avec force détails les pratiques atroces qui ont cours dans la prison de Guantanamo ainsi que les Spy Files[114] (documents provenant d'entreprises développant des technologies à double usage)[43].

QUI EST JULIAN ASSANGE ?

Julian Assange est le fondateur controversé de WikiLeaks… et une figure quelque peu romanesque. Assange a déjà dit auprès de différentes personnes, et même publiquement : « WikiLeaks, c'est moi. » Il est très probablement la personne qui anime le compte Twitter *@wikileaks*. Cette identité, que l'on peut qualifier de fluide, est peut-être réelle, ou peut-être pas ; il n'en reste pas moins qu'Assange est connu pour être un membre actif des Cypherpunks (voir chapitre 03). Ce mouvement, né dans les années quatre-vingt-dix,

43 : Ces derniers ont un statut légal particulier car l'emploi qui peut en être fait peut être tout à fait anodin (quoique…) comme beaucoup moins avouable… Ainsi, un logiciel destiné à bloquer l'accès à Facebook entre les murs d'une entreprise pour éviter les dégâts de la procrastination peut être également vendu (avec de meilleurs bénéfices) à des gouvernements peu enclins à laisser leurs citoyens accéder à des sites qu'ils jugent dangereux. C'est parce que les usages peuvent différer selon l'opérateur que ces logiciels sont difficiles à réglementer d'un point de vue légal. Les documents de Stratfor mentionnés précédemment en sont un très bon exemple.

plaide pour une gouvernance anarcho-libertarienne et a donné naissance à des technologies et des théories fondamentales telles que des outils de chiffrement, des monnaies et des réeaux Internet décentralisés. Les Cypherpunks sont également à l'origine de cryptome.org, un site que l'on peut considérer comme l'ancêtre de WikiLeaks.

Connu sous le pseudo « Proff », Assange est présent sur les listes de diffusion cypherpunk dès 1993-1994. Cela n'a rien de surprenant quand on sait qu'il a été poursuivi pour intrusion dans des systèmes informatiques dès 1991. Il conçoit et érige les techniques cryptologiques en moyens à la fois de défense et d'attaque. Le chiffrement assure l'anonymat et permet la divulgation en sécurité des secrets d'État ; si ces actes peuvent contribuer à révéler les arcanes du pouvoir et permettent au passage de renverser quelques gouvernements peu respectueux des libertés, ce n'est pas de refus ! L'idée cristallise notamment en 1996 lorsque l'un des Cypherpunks, John Young, crée *cryptome.org* comme un outil de divulgation de documents gouvernementaux. Au début des années deux mille, *cryptome.org* est devenu, en cinq ans d'existence, le centre de publication de rapports classés, et une vraie épine dans le pied des agences de renseignement américaines.

C'est sur cryptome.org que l'on retrouve une série d'essais[115] qu'Assange publie en 2006 et qui détaillent sa philosophie politique. On y lit l'opposition forte à ce qu'il appelle « *des gouvernements fondés sur le secret et sur la conspiration autoritaire* », dont les États-Unis font (sans surprise) partie. La manière de combattre ces systèmes de gouvernance est abordée de façon très pragmatique : il ne s'agit pas seulement d'ouvrir un peu la porte (« *la vérité ne suffit pas* »[116]), il faut dégrader la capacité du système à conspirer. Mettre des grains de sable dans les rouages[117]: c'est l'idée de transparence radicale dont WikiLeaks s'est fait le symbole.

En lisant ces documents, notamment *Conspiracy as Governance,* on trouve décrites des approches que l'on a vues à l'œuvre.

"Consider what would happen if one of these parties gave up their mobile phones, fax and email correspondence — let alone the computer systems which manage their [subscribers], donors, budgets, polling, call centers and direct mail campaigns. They would immediately fall into an organisational stupor and lose to the other."

« Réfléchissez à ce qu'il se passerait si l'un de ces partis rendait publics les numéros de téléphone, les correspondances par fax et e-mails ou plus encore, les systèmes informatiques de gestion de leurs adhérents, soutiens, financeurs, sondages, centres d'appel et campagnes de mailing direct. Ce parti tomberait immédiatement dans une stupeur organisationnelle et perdrait au profit de l'autre [parti]. »

La « *stupeur organisationnelle* » est induite par l'anxiété permanente qu'une nouvelle fuite de messages puisse intervenir à n'importe quel moment :

"The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive 'secrecy tax') and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaptation."

« Plus une organisation est secrète ou injuste, plus les fuites [qu'elle subit] induisent la peur et la paranoïa au sein de ses coteries dirigeantes et planificatrices. Ceci devrait se traduire par la minimisation de l'efficience des mécanismes de communication interne ([soit] une augmentation de "l'impôt secret cognitif") et, ainsi, par un déclin conséquent du système cognitif au sens large, ce qui produirait une diminution de la capacité à s'accrocher au pouvoir car l'environnement requiert alors des facultés d'adaptation. »

L'idée de base est très simple : si l'on peut empêcher les gens qui nous gouvernent d'avoir des secrets, ils n'auront pas d'autre choix que d'opérer différemment. Il est évident qu'à partir du moment où une

organisation doit compartimenter, chiffrer et veiller constamment au secret de ces informations et données, la paranoïa change la manière de fonctionner. Ce genre d'idéologie politique se défend : que l'on y adhère ou pas, il est question de visions philosophiques de la gouvernance.

Depuis 2011 cependant, le site et son fondateur laissent passer des positions indéfendables, pour le moins bizarres (antisémites et homophobes, pour être précis[118]), et de plus en plus complotistes[119]. Nous avons vu que Julian Assange a même eu droit à son programme sur RT (Russia Today)[120], une chaîne nationale russe directement liée au Kremlin et connue pour faire de la propagande et déformer la réalité de manière systématique (et très professionnelle). La mention de journaux tels qu'*Al Masry Al Youm* et *Al-Akhbar*, connus pour leur proximité avec le maréchal Al-Sissi, actuel président égyptien, comme « partenaires et sponsors » n'arrange rien à l'image de WikiLeaks. Cette tendance est allée crescendo. Le compte Twitter *@wikileaks* a défendu le fondateur du site d'extrême droite Breitbart et grand fan de Donald Trump[121], et s'est opposé[122] au bannissement par Twitter d'un troll notoire d'extrême droite ayant orchestré une campagne raciste.

Enfin, et cela a son importance, la position d'Assange sur la divulgation de données personnelles sensibles sans les rendre anonymes est assez claire[123] : si cela arrive, c'est tant pis, c'est assumé. Est également assumée la conséquence de ce type de publication : des membres de WikiLeaks pourraient avoir « *du sang sur les mains* »…

L'ÉVOLUTION DE WIKILEAKS

La collaboration de Wikileaks avec les différents médias se tarit donc, en partie à cause de la pression énorme exercée sur l'organisation, de sa situation financière difficile et de l'imbroglio juridique autour d'Assange. Par ailleurs, la notoriété que WikiLeaks

a acquise lui permet de s'affranchir des collaborateurs précédents (même si la collaboration avec certains médias reste d'actualité).

Divers évènements ont conduit à une telle situation. Certains philosophes misanthropes l'ont écrit : « *L'homme est un loup pour l'homme*. » Pour des proches de WikiLeaks, cela devient : « *La plus grande menace pour les journalistes d'investigation, ce sont les autres journalistes d'investigation.* »[124] L'adage est de Jakob Appelbaum, ex-développeur de Tor et collaborateur de WikiLeaks, bien connu dans les milieux hacktivistes[44]. Ambiance règlement de comptes avec la profession et surtout avec d'anciens confrères du *Spiegel*. En effet, le qualifier lui, mais aussi d'autres collaborateurs de WikiLeaks, de « *cyberactiviste* », donc lui refuser la qualité de journaliste, peut le mettre gravement en danger, puisqu'un tel qualificatif les exclue du milieu journalistique et de la protection juridique qui en découle. Ceux qui en prennent pour leur grade, c'est *The Guardian*, qu'Appelbaum qualifie de « *publication absolument la plus merdique en langue anglaise* »… Le cahier des doléances et les attaques personnelles envers les journalistes du *Guardian* qui collaboraient avec WikiLeaks sont révélés. Ils sont accusés d'avoir empêché la publication par ProPublica de documents fournis par WikiLeaks ; de n'avoir rien dit sur les pressions subies par les services de renseignement anglais en 2013, qui ont mené à la destruction par le journal de nombreux documents fuités par Snowden ; de n'avoir envoyé qu'un panier de savons et des chaussettes propres à Assange lorsque ce dernier s'est réfugié à l'ambassade d'Équateur à Londres ; etc. Ambiance…

44 : Suite à diverses révélations sur des agressions sexuelles dont il se serait rendu coupable, Appelbaum a quitté Tor. Un site web avec des témoignages des descriptions d'abus par Jake Appelbaum existe (http://jacobappelbaum.net/) comme une manière d'informer la communauté du problème et d'en appeler à une solution émanant de la communauté. Ainsi, aucune plainte ne semble avoir été déposée (la confiance en les forces de l'ordre de beaucoup de ce milieu n'est pas au beau fixe). Comme avec le projet Tor, des organisations spécifiques où Appelbaum était significativement impliqué ont été contactées pour porter les griefs à leur attention et demander aux entités de prendre des mesures.

Il est indiscutable que travailler avec WikiLeaks et Assange n'est pas de tout repos. Mais, de l'aveu du rédacteur en chef du *Guardian*, les journalistes ont également beaucoup appris de la paranoïa d'Assange[125]. Les choses semblent s'être gâtées dans les semaines précédant la publication des « câbles » diplomatiques à l'automne 2010. The Guardian avait pris l'habitude de travailler avec WikiLeaks et les deux principaux partenaires, *The New York Times* et *Der Spiegel*. Or Assange, souhaitant assurer une diffusion des documents en sa possession plus large encore, négocie des partenariats avec de nombreux autres médias : Channel 4, Al-Jazeera, etc. C'est là que les problèmes commencent. Assange demande par exemple au *Guardian* de « boycotter » *The New York Times* qui a eu l'outrecuidance de publier un portrait le vouant quelque peu aux gémonies. Pire encore, à force de fournir des documents à de multiples rédactions, des fuites se produisent. Peu après, Al-Jazeera et sa *Transparency Unit* publient de nombreux documents sur les négociations au Moyen-Orient. Des « mini-WikiLeaks » émergent, dont certains subsistent encore aujourd'hui.

Ces problèmes ont un impact négatif sur l'organisation. Daniel Domscheit-Berg (surnommé « DDB »), le numéro deux de WikiLeaks, fait sécession, détruit des milliers de documents[126] et crée son propre site, OpenLeaks. Suite à des films racontant l'histoire de WikiLeaks et notamment *Le Cinquième pouvoir*[127], basé sur le livre de Domscheit-Berg *Inside WikiLeaks*, l'organisation règle ses comptes en 2013, au travers de son propre documentaire, *Mediastan*[128]. Le départ fracassant de DDB cause beaucoup de dégâts. Il est par exemple exclu du Chaos Computer Club (l'organisation hacktiviste allemande qui organise le CCC), renforçant ainsi l'effet clivant sur la communauté. S'attirer les foudres du CCC, c'est signe de gros souci tant l'organisation est prestigieuse et respectée[129]. D'après le livre de DDB, les accusations de viol contre Assange contribuent énormément à fracturer l'organisation, notamment car Assange confond ses propres démêlés avec la justice et la situation de WikiLeaks. Alors que beaucoup des soutiens de WikiLeaks défendent alors publiquement Assange,

et rejettent ces accusations en les considérant comme une façon de déstabiliser et de dénigrer l'organisation, il apparaît que cette histoire ne fait pas l'unanimité en interne. Cette conflictualité semble provoquer l'isolement d'Assange dont l'apogée sera – seulement quelques semaines plus tard – sa fuite à l'ambassade d'Équateur.

En parallèle de ces dissensions, le blocus financier organisé par PayPal, Visa et Mastercard suite à la divulgation des « câbles diplomatiques » met WikiLeaks à rude épreuve. Il y a même un bref moment, fin 2011, pendant lequel le site n'est plus accessible car ses opérateurs se consacrent à la levée de fonds. La situation devient surréaliste en octobre 2012, peu avant les élections présidentielles américaines, quand WikiLeaks annonce la publication de nouveaux documents et qu'un clic sur le lien dirige l'internaute sur… une page de dons impossible à désactiver. C'est un *paywall*, expression pour le moins explicite : il faut payer pour « sauter le mur » et pouvoir lire. L'argent, c'est le nerf de la guerre, mais que WikiLeaks transforme sa « *transparence radicale* » en *paywall,* c'est quand même un peu trop. Anonymous, entre autres, s'en émeut et prévient WikiLeaks qu'en agissant ainsi, ils vont « perdre [leurs] derniers alliés »[130].

Quelques jours plus tard, Anonymous prend ses distances avec WikiLeaks en publiant un long communiqué[131] où le collectif explique en quoi l'organisation les dérange :

"We have been worried about the direction WikiLeaks is going for a while. In the recent month the focus moved away from actual leaks and the fight for freedom of information further and further while it concentrated more and more on Julian Assange. It goes without saying that we oppose any plans of extraditing Julian to the USA. He is a content provider and publisher, not a criminal.

[…]

But WikiLeaks is not – or should not be – about Julian Assange alone. The idea behind WikiLeaks was to provide the public with information that would otherwise being kept secret

by industries and governments. Information we strongly believe the public has a right to know.

[…]

As far as money is concerned, we understand that WikiLeaks lives from donations. And it is fine to ask for them as long as this is done in an unostentatious manner. This is clearly not the case anymore, even though the overall situation cannot be that bad: According to the Transparency Report of the Wau Holland Stiftung, Julian received 72.000 Euros only for project coordination in 2011 – this does not include travel costs. And 265.000 Euros were spent on 'campaigns'. (Note that the 139.000 Euros in donations only accounts for the funds that went through the Wau Holland Stiftung, it does not include any donation to WikiLeaks directly).

The conclusion for us is that we cannot support anymore what WikiLeaks has become - the One Man Julian Assange show. But we also want to make clear that we still support the original idea behind WikiLeaks: Freedom of information and transparent governments. Sadly we realize that WikiLeaks does not stand for this idea anymore."

« L'évolution de WikiLeaks nous inquiète depuis un certain temps. Ces derniers mois, l'accent est mis de moins en moins sur les nouvelles révélations et sur la liberté d'information, mais de plus en plus sur Julian Assange. Il va sans dire que nous sommes totalement opposés à l'extradition de Julian aux États-Unis. Julian est fournisseur de contenu et éditeur, pas un criminel.

[…]

Mais WikiLeaks ne se résume pas – ou, du moins, ne devrait pas se résumer – à Julian Assange. Le concept à la base de la création de WikiLeaks était de rendre publiques des informations qui, sans l'intervention de cette organisation, auraient été tenues secrètes par les entreprises et les gouvernements. Nous sommes foncièrement convaincus que c'est le droit du grand public d'avoir accès à ces informations. [...]

Sur le plan financier, nous sommes bien conscients que ce sont les dons qui permettent à WikiLeaks d'exister. Et ce n'est pas un problème tant que ces dons ne sont pas sollicités de façon ostentatoire. Or il semble que ce soit devenu le cas, même si la situation dans son ensemble n'est pas aussi négative qu'elle le paraît : selon le rapport sur la transparence du Wau Holland Stiftung, Julian a reçu 72 000 euros pour son travail de coordination en 2011 – hors frais de déplacement. Et 265 000 euros ont été dépensés pour « des campagnes ». (Il faut préciser que les 139 000 euros de dons n'incluent que les sommes d'argent gérées par le Wau Holland Stiftung, et non les dons versés directement à WikiLeaks).

La conclusion à laquelle nous nous voyons forcés d'arriver est que nous ne pouvons plus soutenir l'incarnation actuelle de WikiLeaks – en un mot le One Man show de Julian Assange. Mais nous souhaitons affirmer clairement que nous continuons à soutenir le concept de départ de WikiLeaks, à savoir la liberté d'information et la transparence politique. Force est de reconnaître, malheureusement, que cette idéologie n'est plus au centre de WikiLeaks. »

Le côté transgressif semble avoir cédé la place à… quoi au juste ? Il est inutile de verser dans l'angélisme pathétique sur la pureté de la cause ; néanmoins, comme le souligne Anonymous, il y a une différence fondamentale entre chercher à se faire des sous à tout prix et défendre une noble cause. Le côté VRP pique, au moins autant que le personnage d'Assange : après avoir produit *Mediastan*, le « *road movie géopolitique* » pour « *rétablir la vérité sur WikiLeaks* » et lui-même, Assange s'est également fendu d'un livre. Lors de la conférence annoncée en grande pompe mais criante de vacuité marquant le dixième anniversaire de l'organisation, Assange, portant un t-shirt barré d'un grand « truth » (« vérité »), annonce un rabais de 40 % sur le prix éditeur… La transformation de WikiLeaks est spectaculaire.

Lors de cette conférence justement, Assange explique, à sa manière très romanesque et idiosyncrasique, en faisant référence à Voltaire et au postmodernisme, son « *idéal romantique* » de l'histoire « *qui n'appartient pas à notre temps, mais au passé ou peut-être à l'avenir* ». Il annonce la nouvelle phase opérationnelle de WikiLeaks, celle de WikiLeaks Task Force[45]. Il s'agit de groupes de bénévoles recrutés *via* Twitter et opérant sur le réseau social. Ils auront en charge de combattre les nombreux ennemis de l'organisation. Et si vous avez lu ce qui précède, vous vous doutez bien que la liste des « ennemis » est longue et variée : les ex-collaborateurs, les différentes éditions de journaux tels que *The Guardian* ou *The New York Times*, des politiciens libéraux, des entreprises IT (Information Technologies)… et à peu près n'importe qui en désaccord ouvert avec les positions de WikiLeaks. Pour se défendre, l'organisation aura besoin « *d'une armée* ». Le besoin de défendre sa création est compréhensible, mais la manière n'en reste pas moins curieuse.

WikiLeaks retourne alors à l'approche de départ : la publication de documents bruts, sans filtre éditorial. Cette approche crée des problèmes et des risques supplémentaires. Le rapprochement supposé avec la Russie, à travers la collaboration étroite entre WikiLeaks, Assange et RT.com, le positionnement public d'Assange sur Clinton qu'il définit comme un danger pour WikiLeaks et toute l'histoire autour des e-mails fuités du parti Démocrate font que tous les doutes sont possibles. La communication récente de WikiLeaks passe essentiellement par le compte Twitter de l'organisation, lequel est très probablement animé par Assange. Ainsi, des phrases comme « *des sources officielles non nommées aux États-Unis* [confirment les pressions américaines sur le gouvernement équatorien] » ou « *les élections américaines sont truquées* » nourrissent toutes les théories du complot. Lorsque Snowden critique publiquement la manière de publier des documents sans les rendre préalablement anonymes, la réponse de WikiLeaks est une attaque personnelle en règle[132].

45 : Le retour de la vengeance de WTF ?

Enfin, l'idée d'une WikiLeaks Task Force, une armée de bénévoles défendant l'organisation contre les gens qui la critiquent, rappelle un peu trop les pratiques de nombreux gouvernements peu démocratiques ou encore d'entreprises privées : on les appelle généralement de la propagande ou… des relations publiques. Dire qui a tort ou qui a raison est, dans ce cas, loin d'être facile. Rappelons qu'Assange vit dans l'ambassade d'Équateur à Londres, dans une seule pièce, depuis août 2012, sans sortir au risque de se faire arrêter et extrader. Que l'on soit d'accord ou pas avec ses idées ne change rien à la pression constante que de telles circonstances peuvent exercer sur une personne et son équilibre mental. Au moins deux rapports médicaux rendus publics en 2014 et en 2016 font état d'une santé aussi bien physique que mentale en danger[133]. Comme à chaque fois que de nombreux acteurs et des agissements complexes entrent en jeu, les jauger ne peut être résumé par des jugements simplistes « bon » ou « méchant ».

LE CAS #AKPLEAKS

Mi-juillet 2016, WikiLeaks annonce une fuite à venir contenant de nombreux documents secrets de l'AKP (le parti en pouvoir en Turquie). Elle promet non seulement de découvrir la correspondance électronique du président turc Erdogan, mais aussi de faire la lumière sur les préparatifs du coup d'État raté. Le 18 juillet 2016, le compte *@wikileaks* fait monter la mayonnaise : « *Vous attendez notre nouvelle publication de 100 000+ documents sur ce qui a mené au #TurkeyCoup* [putsch en Turquie] *? Explorez nos publications précédentes sur Erdogan.* »[46] Le 19 juillet 2016, il annonce : « *À venir mardi : les #ErdoganEmails : 300 000 e-mails internes du parti d'Erdogan, AKP, couvrant jusqu'au 7 juillet 2016.* »[47]

Comme beaucoup de médias français l'ont rapporté, le putsch raté a été organisé et mené par une partie de l'armée turque,

46 : https://twitter.com/wikileaks/status/755051054170005504
47 : https://twitter.com/wikileaks/status/755171322288861184

composée principalement d'officiers de rang intermédiaire, pour chasser le président Erdogan et sa majorité du pouvoir. La chasse aux sorcières qui suit le coup d'État avorté – et qui a toujours cours – provoque en deux semaines la fermeture de quarante-cinq journaux, vingt-trois stations de radio et seize chaînes de télé[134], ainsi que l'arrestation de milliers de personnes. Le président Erdogan en profite pour faire ce à quoi beaucoup d'analystes s'attendaient : élargir sa mainmise sur le pays et réduire les libertés civiques.

On comprend donc pourquoi les annonces de WikiLeaks concernant la publication des e-mails d'Erdogan et des édiles d'AKP ont de quoi susciter un grand intérêt. Le 19 juillet 2016, WikiLeaks publie « *une première partie des e-mails d'AKP* »[135] et écrit :

« Les documents ont été obtenus une semaine avant la tentative de coup d'État. Nous avons cependant avancé la date initialement prévue pour leur publication en réponse aux purges entreprises par le gouvernement [turc] après la tentative [de putsch] avortée. Nous avons vérifié les documents et la source, laquelle n'a aucun lien avec les éléments ayant organisé le coup, ni n'est liée d'une manière quelconque à un parti ou un État rival. »

De nombreux médias occidentaux en ont parlé, surtout pour dire que, suite à cette publication, la Turquie a bloqué l'accès à WikiLeaks[136]. Et WikiLeaks a renchéri dans le même sens[137] tweetant que « le gouvernement Erdogan a officiellement ordonné le blocage de WikiLeaks après la publication de 300 000 e-mails de son parti, l'AKP ». Une telle action n'a rien de surprenant : les révélations de WikiLeaks font toujours des mécontents et la Turquie est connue pour son habitude de surveiller les communications numériques et de censurer fréquemment sites web et autres réseaux sociaux.

Mais l'histoire ne s'arrête pas à ces escarmouches, somme toute banales. Des signaux d'alarmes commencent à tinter. Quelques

activistes et journalistes tweetent[138] peu après la publication par WikiLeaks que « *99 % des e-mails* » semblent être issus de forums ou de Google groups publics ou sont simplement des spam. D'autres parlent de poèmes envoyés par e-mail[139] ou mentionnent que « *la municipalité a offert des gâteaux de semoule aux habitants pour la fête de l'Aïd* »[140]. Yasin Darbaz, un universitaire, tweete alors : « *Tous les #AKPemails sont des spams. Ce ne sont pas des e-mails officiels. Te moques-tu du monde @wikileaks ?* » Plus bas, après qu'un internaute le traite d'« Erdogan troll », Darbaz précise : « Avant de me répondre, vérifie les e-mails. En majorité, ce sont des Google groups, des forums et des spams. Je n'ai pas trouvé de vrai e-mail officiel. » Ragip Soylu, le correspondant à Washington du journal turc en langue anglaise *Daily Sabah,* dit : « *Premier regard : des milliers d'e-mails publiés par @wikileaks comme #AKPemails ne sont pas des e-mails officiels [émanant] du parti AK. Ce sont en majorité des forums Google et des e-mails non liés au parti.* »

Une partie non négligeable des messages proviennent ainsi de Google groups publics, donc n'appartenant pas et n'étant pas géré ou affiliés avec l'AKP, et contiennent des blagues douteuses et toutes sortes de théories du complot. Si on utilise « *akparti.org.tr* » (le nom de domaine de l'AKP) comme filtre dans le champ « De : », on obtient quelques 683 e-mails[141]. Si on ajoute le même nom de domaine au champ « Pour : », le nombre de e-mails tombe à 275… Et encore, parmi ceux-là, il y en a qui sont du spam[142]. Ce dernier point peut être à la fois positif et négatif : oui, il y a du spam, mais cela dénote aussi une certaine exhaustivité de l'information. En effet, si les spams étaient filtrés, on pourrait par exemple se demander si des détails particuliers ont été omis dans la préparation des documents. Cependant, même en prenant en compte ces considérations, la conclusion est sans appel : les e-mails publiés sont assez loin des annonces de documents exclusifs contenant la correspondance privée d'Erdogan, de son cercle proche au sein d'AKP ou des échanges des organisateurs du coup d'État raté. Le plus

important : ils n'ont aucun intérêt pour l'information du public…

Après la première publication d'e-mails du 19 juillet, WikiLeaks rend public le restant des documents le 21 juillet 2016 (ces documents ne sont plus accessibles en ligne). C'est à ce moment-là que les choses tournent au vinaigre. L'ampleur des dégâts est impressionnante quand on s'intéresse à ce qu'il y a dans ces fichiers. En effet, le fait que les gens de WikiLeaks ne lisent pas le turc et publient des documents sans aucun rapport et sans aucun intérêt public a déjà bien entamé le peu de confiance qu'il peut rester vis-à-vis de la plate-forme. Mais d'après Zeynep Tufekci et divers activistes et journalistes turcs, un palier supplémentaire est franchi le 21 juillet : les documents contiennent les données personnelles de millions de citoyens turcs. Ainsi, parmi les fichiers contentieux, on trouve[143] des listes de membres de l'AKP (environ 10 millions de membres encartés). Pire encore, on y trouve aussi des données sur toutes les femmes inscrites sur les listes électorales dans 79 des 81 départements turcs. Le total se monte à 20 millions de citoyennes turques listées dans des fichiers Excel avec leurs noms et prénom ainsi que le nom de jeune fille si elles sont mariées, la date et le lieu de naissance, les adresses personnelles et numéros de téléphone. Les données concernant les électrices membres d'AKP contiennent des détails privés supplémentaires tels que le numéro d'identité citoyen. Celui-ci est très important car il permet d'accéder à divers services publics. Des fichiers additionnels révèlent également les relations de parenté pour les membres encartés de l'AKP, avec des informations personnelles telles qu'adresses et numéros d'identité citoyens. Cela ouvre la porte aux pires scénarios (harcèlement, usurpation d'identité, etc.). Ces citoyennes sont mises en danger, d'autant plus que Zeynep Tufekci affirme avoir vérifié les données.

Michael Best est l'une des personnes ayant envoyé les données à WikiLeaks. La source des fichiers est Phineas Fisher, la personne responsable de la compromission et la fuite d'e-mails de Hacking Team (voir chapitre 02). Dans un billet de blog[144] suivant la

publication de l'article de Zeynep[145], Best explique les différents évènements de cette « *tempête… [qu'il aurait] pu prévenir* ». Depuis, il a également supprimé les fichiers des torrents qu'il avait mis en place et a contacté d'autres personnes pour les inviter à faire de même. Le comportement de WikiLeaks n'a pas changé pour autant : le compte Twitter continue à promouvoir l'URL vers les données personnelles de citoyens, même si les données ne sont plus chez Wikileaks (elles se promènent cependant sur des torrents).

En fait, WikiLeaks a fait ce qu'on appelle du *doxxing*, en bonne et due forme (voir chapitre 02). Les échanges qui suivent les arguments de Zeynep sur Twitter sont houleux et accablants[146]. WikiLeaks campe sur ses positions et refuse de reconnaître sa négligence. Le compte WikiLeaks traite notamment Zeynep Tufekci d'« *apologiste d'Erdogan* » en réponse à la demande de commentaire et de clarification de Dunja Mujatovic, directrice pour la liberté des médias de l'Organisation pour la Sécurité et la Coopération en Europe (OSCE). Cette insulte est non seulement diffamatoire mais aussi ridicule[147] tant elle est éloignée de la réalité[48]. Plus tard, WikiLeaks bloque Zeynep Tufekci sur Twitter[148]. C'est très troublant quand on pense qu'il s'agit d'une universitaire reconnue, qui a juste eu l'outrecuidance de demander que l'organisation prenne ses responsabilités et reconnaisse l'énormité de l'erreur. Et elle ne fut pas la seule [149] !

Un autre point est soulevé qui fait moins les gros titres. Dans les #AKPleaks, les e-mails sont non seulement sans intérêt, mais il y a également de nombreux malwares. Le chercheur en sécurité informatique Vesselin Bontchev[150] a en effet isolé les fichiers vérolés et démontré que les e-mails publiés sans aucun travail préalable par WikiLeaks contiennent plus de quatre-vingt variantes de malwares[151]. D'un point de vue informatif, il est intéressant et

48 : Zeynep Tufekci est connue pour ne pas porter la politique du président Erdogan dans son cœur : voir par exemple http://www.nytimes.com/2016/07/20/opinion/how-the-internet-saved-turkeys-internet-hating-president.html

même précieux d'avoir accès à ce genre d'exécutables. Cependant, ces logiciels malveillants peuvent s'installer sur n'importe quel ordinateur. Il suffit de télécharger l'archive des e-mails pour l'étudier ou la sauvegarder. WikiLeaks a eu tort de ne pas avoir signalé contre la présence de ces malwares.

Au-delà des attaques personnelles et autres sensibleries pétries d'orgueil, le contexte immédiat de la publication de ces données fait froid dans le dos. En pleine chasse aux sorcières d'après coup d'État, une organisation tierce a simplement rendu publiques les données personnelles de citoyens et de membres du parti malgré les règlements de compte que cela pourrait engendrer. De plus, ces agissements et le refus de reconnaître ses erreurs minent la confiance que d'aucuns ont dans les lanceurs d'alerte et donnent raison à ces dirigeants d'inspiration plus ou moins démocratique qui tentent régulièrement de censurer les contenus. Comment peut-on raisonner et défendre les lanceurs d'alerte lorsqu'on se voit opposer ce cas-là et le dangereux étalage de données personnelles ? Le scandale concomitant sur les fuites d'e-mails des Démocrates américains et leur origine étrange en est d'autant plus troublant.

LES #DNCLEAKS ET L'AFFAIRE CLINTON

En même temps que la fuite des e-mails d'Erdogan (qui n'en sont pas), WikiLeaks publie près de 20 000 e-mails échangés au sein du parti Démocrate américain. C'est le #DNCleaks, du *Democratic National Committee* ou DNC, la plus haute instance du parti. Cette publication a semé une sacrée pagaille dont les effets se font encore ressentir plusieurs mois plus tard.

En bref, des e-mails sont rendus publics deux jours avant le début de la convention démocrate – l'équivalent d'une université d'été qui désigne officiellement le candidat du parti à l'élection présidentielle – à Philadelphie. Hillary Clinton et Bernie Sanders sont au coude à coude quand ce dernier accepte de s'éclipser et

de se rallier à Clinton, au grand désarroi d'une large partie de ses soutiens. Or les 20 000 messages des #DNCleaks révèlent beaucoup de choses dont, entre autres, la volonté dans l'appareil du parti Démocrate d'empêcher l'ascension de Bernie Sanders. On se doute que l'enthousiasme déjà tiédasse des soutiens de Sanders envers Clinton n'en sort pas renforcé ! Par ailleurs, une quantité non négligeable de données personnelles non anonymisées et sensibles est aussi donnée en pâture à tout internaute… Alors que l'on peut admettre l'intérêt d'une transparence des échanges du parti Démocrate, on doit condamner la manière irresponsable dont a été faite la dissémination de numéros de titres d'identité, de sécurité sociale ou encore de cartes bleues d'employés démocrates. D'aucuns peuvent également critiquer le déséquilibre de traitement – pourquoi le parti Républicain n'y a pas aussi eu droit ? – ; la réponse est relativement simple : on ne peut pas publier des documents dont on ne dispose pas. Reprocher à une organisation de ne pas avoir fait fuiter des informations qu'elle n'a pas ressemble un peu à lui reprocher de ne pas avoir piraté le parti en question...

Peu après, WikiLeaks publie également les « Podesta mails »[152], soit plus de 20 000 documents appartenant à l'origine au directeur de campagne de Hillary Clinton, John Podesta. Ces messages ont porté un coup dur à la candidate. Si une quantité non négligeable de ces documents montrent un travail honnête, acharné, d'élaboration politique, le linge sale y est néanmoins bien représenté. On retrouve quelques thématiques principales : le financement de la fondation Clinton, les relations très (trop) proches de la candidate avec de gros pontes de Wall Street, le mécanisme de travail de l'équipe élargie de campagne et des prises de décisions et enfin, des échanges plus dignes d'un journal people que d'un média sérieux et respecté comme *Le Monde*. Le financement de la fondation est clairement un élément d'intérêt public et d'importance géopolitique. Or un audit a montré que les conflits d'intérêts n'ont jamais été considérés dans la liste des risques pesant sur l'organisation. On apprend par

ailleurs de ces e-mails que certains des bienfaiteurs de la fondation Clinton sont des Qataris dont les dons auraient eu en contrepartie une rencontre privilégiée avec Bill Clinton[153]. Comme cela s'est fait pendant que Mme Clinton était aux Affaires étrangères, le conflit d'intérêts est assez flagrant. On peut continuer avec les liens des Clinton et de Wall Street : la proximité de la candidate avec les milieux de la finance fait qu'elle peut être perçue comme manquant d'indépendance[49]. Vous me direz, depuis son élection en novembre 2016, Trump fait largement pire en nommant un ex-directeur de Goldman Sachs comme secrétaire d'État à l'économie (équivalent de notre ministre de l'Économie) ou en continuant de diriger personnellement son empire.

Il n'en reste pas moins que l'intrusion et la publication subséquente de ces correspondances sont perçues comme des actions malveillantes[154]. Cette zizanie a également des relents de guerre froide. Les dirigeants du parti Démocrate soupçonnent les sources de WikiLeaks d'être, dans ce cas, russes[155]. Il est très difficile de s'exprimer sur ces points car, à l'heure où nous écrivons ces lignes, l'histoire se fait. Et trier l'information solide de l'ivraie est très difficile. Nous n'avons pas ou peu de recul et il est probable que nous n'apprendrons le fin mot de l'histoire que dans quelques années. Permettons-nous donc un peu de spéculation en cherchant à relier ces arguments à ce que cela signifie pour WikiLeaks ; mais gardons en tête que toute conclusion reviendrait à se proclamer Madame Soleil 2.0.[50]

On a évoqué précédemment les liens troubles entre Assange, WikiLeaks et le gouvernement russe. Spéculer sur les interactions entre Assange et Poutine reviendrait à faire du très mauvais James Bond et à s'éloigner du vrai problème. La question est ailleurs :

49 : Pour un retour détaillé sur les détails découverts dans les mails fuités, voir http://www.vox.com/policy-and-politics/2016/10/20/13308108/wikileaks-podesta-hillary-clinton

50 : Les aspects plus techniques de cette histoire sont abordés dans le chapitre précédent.

est-ce qu'une organisation militant pour la transparence de la vie publique devrait accepter des informations en provenance de services de renseignement étrangers ? La différence avec *Collateral Murder* et les « câbles » est énorme : c'est Chelsea Manning, à l'époque membre des forces armées américaines, qui transmet ces documents portant sur les activités potentiellement illégales du gouvernement qu'elle sert. Dans le cas Snowden, la configuration est similaire. Mais pour #DNCleaks et les e-mails de Podesta, il s'agit d'informations et de documents peut-être obtenus suite à l'intrusion illégale d'un État dans les systèmes d'un autre État[51]. La « *transparence radicale* » devient une cour de récré géante où le règlement de compte se fait sur la base d'intérêts personnels et/ou politiques. Et des règlements de comptes entre États par fuites interposées seraient-ils pour autant gages de transparence véritable de la vie publique ? Chercher à savoir qui est le moins pire en regardant qui a le linge le moins sale n'est pas l'approche la plus constructive en matière de gouvernance démocratique.

Début octobre 2016, une nouvelle fuite d'e-mails est rendue publique par WikiLeaks. Et là, comme le note avec à-propos Andréa Fradin dans le média en ligne Rue89, on a trouvé « *des e-mails au milieu des photos de bite* »[156] d'Anthony Weiner, ex-compagnon de la conseillère de Clinton, Huma Abedin. Malgré l'absence d'informations pertinentes, le FBI rouvre l'enquête contre Clinton. On est à moins d'une semaine du jour du scrutin présidentiel… Clinton perd, Trump choque tous les jours les experts et autres observateurs, Obama accuse Poutine d'ingérence. On ne sait pas ce qu'a véritablement gagné le peuple.

51 : Certains pourraient être tentés de dire qu'à ce compte-là, il n'y aurait plus de presse d'investigation car les données utiles sont presque toujours obtenues illégalement. Il y a cependant une différence entre l'approche d'enquête journalistique lors d'une investigation et l'intrusion dans des systèmes informatiques. Dans le premier cas, on peut obtenir des informations par des moyens légaux aussi bien qu'illégaux ; dans le deuxième, le moyen est toujours illégal.

VÉRITÉ VS. PROPAGANDE : LES DEUX FACES D'UNE MÊME MONNAIE ?

De nombreux observateurs notent l'idylle qui semble exister entre Assange et Trump : des tweets de soutien de la part de WikiLeaks, des déclarations du nouveau président américain selon lesquelles WikiLeaks est plus digne de confiance que les enquêteurs des services de renseignement et de sécurité américains[52]…

Comment se fait-il qu'Assange et WikiLeaks soient devenus les fidèles de Donald Trump ? Tout semble les opposer : WikiLeaks argue pour davantage de vie privée et moins d'implication des États-Unis dans les affaires d'autres pays, s'opposant ainsi à la surveillance des communications, les assassinats ciblés par drones et à l'existence même de Guantanamo Bay. Trump, quant à lui, est en faveur d'une « *fermeture d'Internet* », l'autorisation et l'utilisation plus fréquente d'assassinats extrajudiciaires et l'institutionnalisation de Guantanamo pour que cela devienne une maison d'arrêt permanente et accepte d'autres types de détenus. À ses débuts d'hacktiviste, à la fin des années quatre-vingt, Assange admirait les activistes antinucléaires ; Trump s'est déjà exprimé en faveur d'une utilisation plus fréquente d'armes nucléaires…

Aucune de ces incohérences ne semble avoir gêné Assange pour la publication des e-mails du DNC et de Podesta. Or rendre publics les e-mails du parti Démocrate ou encore des messages coquins du QG démocrate, c'est une chose ; mais devenir le grand gourou des soutiens d'extrême droite de Trump et autres suprématistes blancs en est une autre. L'adoration vouée à Assange et WikiLeaks est telle que, quelques heures avant les célébrations du dixième anniversaire de WikiLeaks, de nombreux conspirationnistes pro-Trump publient partout que ce soir-là « *Assange fuitera des documents qui vont dévaster Clinton.* »[157] Beaucoup de bruit

52 : http://mashable.com/2017/01/04/trump-favors-assange-over-fbi-cia/#DtHuX5upUPqd

pour rien, d'après Andréa Fradin de Rue89[158]. Il n'empêche que l'attitude d'Assange dans cette histoire est troublante : lorsque les fuites sont attribuées à des hackers russes, il soutient qu'elles viennent en réalité d'un employé du DNC, Seth Rich. Ce dernier a été la malheureuse victime d'un vol à main armée, mais cela n'a pas empêché Assange de clamer que « *nos sources courent des risques* ». Des assertions péremptoires et dénigrantes, comme l'a dénoncé la famille du défunt[159], que rien ne vient étayer et qui, mêlées à d'autres déclarations et agissements, ont de quoi faire très sérieusement douter des allégeances d'Assange.

En effet, de nombreux faisceaux d'indices suggèrent une coordination entre les fuites publiées par WikiLeaks, son positionnement et certains évènements majeurs de la dernière campagne présidentielle américaine[160]. Les #DNCleaks ont un intérêt pour les citoyens, mais à quoi sert ce mini-sondage Twitter[161] autour des raisons de l'effondrement physique de Clinton lors des commémorations du 11-septembre ? Avant d'être effacé, le sondage propose des options telles que la maladie de Parkinson, la sclérose en plaques ou encore « *des allergies et traits de personnalité* »… Cette dernière option est vraiment bizarre. Les e-mails de John Podesta sont rendus publics littéralement dans la demi-heure suivant le scandale provoqué par les propos de Trump glorifiant ce qui apparaît comme des agressions sexuelles. La fuite contenant des détails sur les émoluments reçus par Clinton pour ses discours, intervient également peu avant le deuxième débat entre les deux candidats et est perçue[162] comme une manière de distraire l'attention publique des propos de Donald Trump sur les violences sexuelles. Ce genre d'action de la part de WikiLeaks a même choqué un ex-employé de la CIA, emprisonné puis renvoyé pour avoir confirmé à la presse que l'Agence s'est réellement rendue coupable de torture.

PEUT-ON FAIRE CONFIANCE À WIKILEAKS ?

Da !

Mauvaise blague à part, alors que l'impact de WikiLeaks sur la façon dont est perçue l'information et sa valeur politique est incontestable, la question de la confiance que l'on peut lui accorder se pose avec force.

Revenons un peu en arrière… En mars 2010, WikiLeaks publie un rapport fuité, *The Pentagon Report*[163]. Le document est daté de 2008 et évalue la dangerosité du site web pour l'armée américaine. D'après ce rapport, même si le média peut être considéré comme une voix critique nécessaire au sain fonctionnement de la démocratie, sa propension à une « *ouverture extrême* » constitue une menace. Et de préciser que seul 1 % des documents reçus est en dessous du seuil minimum de crédibilité et d'exactitude défini par le site lui-même. Ces documents ne seront jamais rendus publics. En conclusion, le rapport spécifie que la confiance est le « *centre de gravité* » de WikiLeaks et préconise une attaque en règle contre les lanceurs d'alerte et autres sources :

"Wikileaks.org uses trust as a center of gravity by assuring insiders, leakers, and whistleblowers who pass information to Wikileaks.org personnel or who post information to the Web site that they will remain anonymous. The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter others from using Wikileaks.org to make such information public."

« Wikileaks.org utilise la confiance comme un centre de gravité en assurant les initiés, ceux qui font fuiter des informations et les lanceurs d'alerte qui transmettent des informations au personnel de Wikileaks.org ou qui transmettent des informations *via* le site web, qu'ils resteront anonymes. L'identification, l'exposition ou encore le licenciement ou les poursuites judiciaires contre des proches, des

"fuiteurs" ou des lanceurs d'alerte passés et actuels, peuvent nuire ou détruire ce centre de gravité et dissuader d'autres personnes d'utiliser WikiLeaks.org pour rendre publiques de telles informations. »

Comme on le mentionne plus tôt dans ce chapitre, c'est entre la publication de *Collateral Murder* et celle des « câbles » diplomatiques que Chelsea Manning est trahie (voir page 175) et détenue dans des « *conditions inhumaines* »[164]. Assange commence à parler plus ouvertement des peurs qui l'habitent quant aux possibles agissements émanant d'agences de renseignement[165]. Après la publication des télégrammes diplomatiques, la tornade de diffamation, de critiques souvent infondées et autres attaques personnelles s'est déchaînée *ad nauseam.* Il serait évidemment conspirationniste et péremptoire d'affirmer que ces attaques ont été coordonnées et/ou instiguées par des personnes haut placées dans les sphères gouvernementales. Il n'en reste pas moins que leur violence et leur diversité font bizarrement écho à la préconisation du *Pentagon Report.*

La caractérisation sociopolitique de WikiLeaks comme « *ennemi de la communauté internationale* »[166] – pour reprendre les mots de la ministre aux Affaires étrangères américaine de l'époque, une certaine Hillary Clinton – et les incitations d'ex-diplomates reconvertis en stars de Fox News à traiter Assange comme un terroriste[167] sont la partie émergée de l'iceberg de haine qui s'est déchaîné à l'encontre de WikiLeaks et de son rédac-chef. Et lorsque la plainte pour agression sexuelle est déposée contre Assange, le déchaînement et l'attention médiatique atteignent un nouveau sommet de frénésie. C'est compréhensible, direz-vous : quoi de plus vendeur que des histoires sordides de politique et de sexe ? D'après *The Guardian* qui a publié le texte intégral de la plainte[168], les accusatrices ont spécifié qu'Assange s'est comporté de « *manière irrespectueuse* » envers les deux plaignantes et de « *façon agressive* » avec l'une d'elles. Bien évidemment, la loi suédoise fournit de nombreux garde-fous aux femmes, tels que la liberté de s'opposer à la poursuite d'un acte de nature sexuelle et une réaction malencontreuse du garçon frustré peut constituer un délit. L'implication du conseiller juridique des

plaignantes, personnalité politique suédoise connue pour ses fortes prises de position féministes, a significativement joué dans la décision des prétendues victimes de transformer l'équivalent d'une main courante en plainte transmise directement au tribunal[53]. Ainsi, la manière dont les plaintes ont été traitées et dont l'enquête n'a pas eu lieu mais a été immédiatement remplacée par un mandat d'arrêt international, constitue un faisceau d'indices interprété par beaucoup comme un acte politique punitif à l'encontre d'Assange[54]. On se souviendra également de l'« *impôt dissidence* », et de la manière dont Visa, MasterCard, Paypal, Amazon et autres acteurs privés ont fait de leur mieux pour faire barrage au fonctionnement de WikiLeaks. Il est très difficile, dans ces circonstances, de se prononcer clairement en faveur de certains acteurs plutôt que d'autres.

Pour revenir à la question épineuse de la confiance en WikiLeaks, rappelons par exemple qu'avant de rendre public les « câbles » diplomatiques, Assange entre en contact avec le Département d'Etat américain[169] à propos de l'anonymisation des documents. On peut imaginer le dilemme des agents gouvernementaux : soit contribuer à la modification déjà commencée par WikiLeaks et ainsi légitimer les actions de l'organisation, soit ne pas les assister et risquer une anonymisation insuffisante qui mettrait en danger des employés du gouvernement. Dans une lettre datée de la veille de la publication des premiers télégrammes, le département d'État refuse de participer et demande la remise des documents[170]. WikiLeaks a donc alors quelques considérations éthiques et cherche à minimiser les risques encourus par des tierces personnes qui se retrouveraient involontairement mises en cause. En 2016, cette tentative d'éthique et de mitigation des risques n'est plus à l'ordre du jour. On l'a vu, non seulement les données personnelles sensibles de tierces personnes peuvent se retrouver publiées et disséminées sur le web et

53 : Davide Leigh & Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy*, 2011

54 : Des éléments de réflexion : http://www.cjr.org/behind_the_news/the_wikileaks_equation.php Par ailleurs, Glenn Greenwald, à l'époque journaliste à *Salon* et fervent défenseur d'Assange, a fait la meilleure couverture et analyse des évènements.

« Ils ont le risque pour dénominateur commun, mais chaque contexte est différent. »

Olivier Tesquet, journaliste à *Télérama*

RS : Qui es-tu et comment en es-tu venu à t'intéresser à WikiLeaks et aux lanceurs d'alerte ?

OT : Je m'appelle Olivier Tesquet, j'ai 29 ans, et je suis journaliste à *Télérama*, où je suis depuis cinq ans les questions liées aux cultures numériques, aux libertés publiques et au renseignement. Avant ça, j'ai travaillé un an chez Owni, pionnier du data journalisme en France, où j'ai notamment coordonné notre collaboration technique avec WikiLeaks.

Aussi loin que je me souvienne, je me suis intéressé à WikiLeaks avant de découvrir l'existence des lanceurs d'alerte. J'étais en stage à *L'Express* à l'été 2009, et ce petit site commençait à faire parler de lui. À l'époque, ses publications ne concernaient encore que des pays sous le radar des médias, comme le Kenya ou le Sri Lanka. Instinctivement, j'ai senti qu'ils pouvaient être l'instrument de bouleversements plus importants. J'étais alors en contact avec Daniel Domscheit-Berg, le bras droit d'Assange, avec qui il s'est ensuite brouillé de manière irrémédiable. À partir de 2010, WikiLeaks a véritablement bousculé le jeu médiatico-diplomatico-politique, avec les rapports de guerre d'Irak et d'Afghanistan, la vidéo *Collateral Murder* puis, en 2011, les 250 000 télégrammes diplomatiques du Cablegate.

C'est en voyant le sort réservé à Chelsea Manning, la source présumée de WikiLeaks, que j'ai pris conscience du rôle des lanceurs d'alerte, de leur importance et des dangers

qu'ils encourent. Dès lors, j'ai commencé à m'intéresser à d'autres cas, aux États-Unis d'abord, avec Thomas Drake (que j'ai rencontré, en compagnie d'autres lanceurs d'alerte, à Washington, en juin 2012, un an presque jour pour jour avant l'affaire Snowden[1]). J'ai aussi échangé avec des lanceurs d'alerte en France, d'Irène Frachon (scandale du Mediator) à Stéphanie Gibaud (UBS). À chaque fois, j'essaie d'écouter leurs histoires, avec leur singularité, pour ne pas les enfermer dans ce rôle sacrificiel du lanceur d'alerte. Depuis quelques années, on a tendance à vouloir faire d'elles et d'eux un corps social homogène, quand il faut justement s'évertuer à les rendre uniques. Ils ont le risque pour dénominateur commun, mais chaque contexte est différent.

RS : Si l'on y regarde de plus près, on ne peut pas dire que WikiLeaks fait du journalisme. Quel est ton positionnement sur le rôle d'intermédiation que ces différents acteurs pourraient ou devraient avoir ?

OT : Julian Assange s'est toujours rêvé en rédacteur en chef de WikiLeaks. Il utilise d'ailleurs le terme d'« editor » ou de « publisher » [p*our y définir son rôle, NdR].* Quand WikiLeaks a fait irruption sur la scène médiatique, ils ont très vite décidé de collaborer avec des titres prestigieux : le *New York Times* (NYT), le *Guardian*, *Der Spiegel*, etc. À l'exception notable du *Spiegel*, les rapports se sont vite envenimés avec les autres journaux, par incompréhension mutuelle : la presse a toujours eu du mal à voir autre chose qu'une source chez Assange, goûtant peu son ingérence éditoriale ;

1 : http://www.telerama.fr/monde/aux-etats-unis-le-combat-solitaire-des-whistleblowers-patriotes-de-la-transparence,85185.php

et de son côté, Assange a reproché leur manque de courage aux journalistes (au NYT notamment).

C'est une véritable relation passionnelle : WikiLeaks se rêvait en média, et les médias ont voulu faire leur aggiornamento grâce à WikiLeaks, mais ces deux mondes sont quelque part restés hermétiquement clos. Aussi imparfaite fut-elle, cette collaboration a quand même eu des effets très concrets : on a vu se multiplier les collaborations entre titres – parfois au sein de consortiums – lors de « méga fuites », notamment les affaires fiscales (Panama Papers, LuxLeaks, Football Leaks, etc.). WikiLeaks a également sensibilisé beaucoup de journalistes d'investigation à mieux protéger leurs sources.

RS : Penchons-nous sur le cas Panama Papers ou le cas Snowden. Dans chacun d'eux, l'implication de journalistes a été significative. Les informations divulguées l'ont été de manières toujours constructives, dignes et respectueuses. WikiLeaks ne peut pas se vanter d'agir ainsi en toutes circonstances. Que peut-on dire de son évolution, sur le plan éthique par exemple ?

OT : Depuis la campagne présidentielle américaine, WikiLeaks s'est bunkerisé, volontairement ou non (sa situation personnelle n'aide pas). Par orgueil, Assange s'est senti dépossédé : on l'a par exemple vu vertement critiquer les Panama Papers, en regrettant un tri des informations qu'il a assimilé à de la censure. Je crois que, pendant longtemps, on a sous-estimé sa radicalité : à la différence d'un Snowden, qui œuvre pour le seul intérêt public, Assange est un idéologue qui veut changer le monde, n'hésitant pas à user de stratagèmes pour imposer son agenda. Sa lutte à mort

avec Hillary Clinton en est la preuve éclatante : il la déteste depuis le Cablegate et a tout fait pour miner sa campagne. Dans ces conditions, WikiLeaks et son audience ont muté ; beaucoup de soutiens historiques leur ont tourné le dos, et ceux qui voulaient la peau d'Assange il y a quelques années sont devenus de fervents soutiens (un Sean Hannity sur Fox News, à tout hasard). Aujourd'hui, la confiance est entamée : WikiLeaks est un acteur à part entière du jeu qu'il n'a cessé de dénoncer depuis dix ans.

via des torrents, mais les documents peuvent également contenir des logiciels vérolés constituant un risque supplémentaire.

Si l'on revient au questionnement de la connivence étrange entre Trump et WikiLeaks/Assange, on peut très bien imaginer qu'il n'y a pas de véritable collaboration entre les deux parties. Au lieu de cela, il se peut que WikiLeaks ait saisi l'opportunité de se remettre en selle et de jouer un rôle déterminant sur l'échiquier politique. Ainsi, plutôt que d'accepter une présidence lisse et prévisible de Clinton, Assange peut avoir décidé de donner un coup de pouce à Trump, pas nécessairement parce qu'il est plus en accord avec lui, mais parce qu'une présidence Trump constituerait un renouveau. C'est le genre de propos soutenus par le cercle proche d'Assange[171]. Les deux explications font aussi froid dans le dos l'une que l'autre…

Enfin, et puisqu'on parle de confiance et d'acteurs faisant un usage intensif d'outils numériques, on peut se demander si le numérique a réellement un rôle déterminant dans ce débat : après tout, c'est un site web et des intrusions dans des systèmes informatiques qui ont permis à ces évènements d'avoir lieu. Est-ce donc bien la faute à Internet ? (question troll par excellence) Publier les données personnelles de citoyens et citoyennes turcs

est une décision de celui qui décide de les rendre publiques. Or, celles-ci n'ont aucune valeur ajoutée à une démarche d'ouverture de la gouvernance.

Qu'en est-il de la valeur ajoutée de la publication des e-mails du parti Démocrate et de la campagne de Clinton ? Outre des détails sur les opérations pas toujours reluisantes de la fondation Clinton et des possibles conflits d'intérêts, une bonne partie de ces messages ne résiste pas à l'examen de l'apport à une meilleure gouvernance. Par définition, une correspondance privée est… privée. Dénoncer un conflit d'intérêts est nécessaire, mais rendre publiques les blagues de mauvais goût de certains membres de la campagne de Clinton ne l'est pas, et c'est à ce niveau que l'on peut sentir la confiance se tarir. Le focus ici n'est donc pas tant le comment (compromission de systèmes de communications privées, par extension, « Internet »), mais quoi (ce qu'on fait de ce que l'on a obtenu). Le traitement de ces informations – génération de *fake news* et propagande contre analyse et critique constructive et argumentée – est ce qui justifie ou pas la confiance que l'on a dans le messager.

On peut faire ici un parallèle avec la fameuse lettre à Mazzei. Nous sommes à la fin du XVIII^e^ siècle. Filipo Mazzei, un médecin italien, est un ami proche du président américain Thomas Jefferson. C'est d'ailleurs à Mazzei que l'on attribue la formulation « tous les hommes sont créés égaux » (« *All men are created equal* »), intégrée à la Déclaration de l'Indépendance des États-Unis d'Amérique, faite et proclamée par Jefferson lui-même. Les e-mails de l'époque, ce sont les échanges épistolaires. Dans une lettre à Mazzei suite au traité de Jay mettant fin aux bisbilles franco-britanniques de l'époque, Jefferson exprime sa frustration ; les termes de l'accord sont en effet peu avantageux pour la France à laquelle il est un soutien fervent. Jefferson s'exprime en termes fleuris sur l'élite de Washington : l'administration y est « *anglicane, monarchique et aristocratique* » à l'image de celle en Angleterre et les officiers militaires sont « *tous des hommes timides qui préfèrent le calme*

du despotisme à la mer tumultueuse de la liberté… [c]ela vous donnerait un accès de fièvre si je vous nommais les apostats qui ont basculé à ces hérésies, des hommes qui étaient des Samson dans le champ [de bataille] et des Solomon au sein du conseil, mais à qui la catin d'Angleterre a rasé les cheveux ».

Rien ici de plus normal : des amis s'écrivent et partagent leurs opinions personnelles. Le problème est que la lettre a été donnée à la presse. S'ensuit une série de traductions en français, puis probablement en italien – ou l'inverse, ce n'est pas clair – puis re-traduction en anglais et publication par la presse américaine. Toute cette histoire a lieu en l'espace de trois mois, en 1796, et précède les élections présidentielles de décembre, que Jefferson a perdues. Ambiance qui rappelle étrangement 2016… Avoir confiance en un messager, se servant ou pas du numérique, est ainsi une question autrement plus complexe que la simple discussion autour de l'outil utilisé. Le cas WikiLeaks n'en est qu'une illustration plus actuelle dont l'importance globale est amplifiée et nourrie par sa nature.

L'AMBIVALENCE DU LANCEUR D'ALERTE

Grâce à ou à cause de WikiLeaks, la figure du lanceur d'alerte a acquis une fonction sociale d'une dimension nouvelle. De nombreuses critiques ont été émises, que ce soit en faveur ou en défaveur des lanceurs d'alerte. Vous ne serez pas surpris de lire qu'il est difficile de trancher : chaque critique est formulée en fonction du système de valeurs politiques propre à la personne qui l'exprime.

Tout tourne autour de la valeur de l'information divulguée et partagée, et de l'équilibre risques-bénéfices. Bénéfices pour qui ? Et risques pour qui ? L'idée qui sert de toile de fond à WikiLeaks et à de nombreuses autres initiatives dont nous avons un peu parlé plus haut est celle de la transparence et de la fin de l'asymétrie informationnelle. Avec l'avènement de

diverses implémentations technologiques destinées à résoudre les problèmes de gouvernance liés à l'inégal partage d'informations entre gouvernants et gouvernés, les idées d'ouverture, de participation citoyenne et de réduction des écarts entre les gens investis du pouvoir et les autres se propagent comme une traînée de poudre. WikiLeaks et Anonymous sont une façon moins « choupinou-Instagram-compatible » et plus brute de décoffrage de parvenir à une transparence de la gouvernance politique et à une meilleure participation citoyenne dans la vie de la cité.

En évaluant les actions de lanceurs d'alerte, il est question de résoudre l'équation entre intérêt public et menace. Ainsi, lorsque WikiLeaks demande au Département d'État de contribuer à l'anonymisation de documents, l'effort vise à limiter au maximum les effets indésirables et les risques personnels qu'encourent des individus qui se retrouveraient indûment exposés. Tandis qu'on peut dénoncer la divulgation d'informations classées, la publication des « câbles » est dans l'intérêt public et celui-ci prévaut. Dans le cadre de la publication des prétendus e-mails du cercle proche d'Erdogan par contre, l'analyse des contenus a montré qu'il n'y avait aucune information d'intérêt public, même pire : des individus innocents se sont retrouvés exposés et des informations personnelles et sensibles les concernant ont été divulguées sans leur accord préalable. Dans ce dernier cas, c'est un problème de sécurité des personnes.

On peut également voir la question d'un point de vue un peu différent : si certaines informations sont classées « confidentiel » ou « secret-défense », c'est pour ne pas qu'elles tombent entre de mauvaises mains, et pas nécessairement parce que l'on veut absolument les cacher aux citoyens. Il est certain que donner à un ennemi les positions des forces armées est au mieux une boulette, au pire une haute trahison pouvant compromettre une stratégie militaire. La compétition intense entre acteurs privés et les situations de conflits armés sont autant de raisons de ne pas divulguer des informations sensibles à tous les vents.

Si cette critique est tout à fait rationnelle et justifiée, elle ignore cependant le nuancier des faits classés et devant rester classés. Dans le cas de *Collateral Murder*, WikiLeaks a publié des preuves d'assassinat et de potentiels crimes de guerre. En quoi les cacher sert-il la sécurité nationale ? Parce que ne pas divulguer ces documents revient également à ne pas poursuivre les auteurs de ces crimes manifestes. Du coup, la question devient : fermons-nous l'accès à une information pour protéger les intérêts de la nation ou pour cacher des faits délictueux ou criminels ? Dans le cas des fuites autour de la guerre en Afghanistan ou en Irak par exemple, il n'y a pas eu de cas recensé d'employé du gouvernement ayant subi des désagréments ou dont l'intégrité physique aurait été menacée. Ici, le compromis se joue de nouveau entre les impératifs de sécurité nationale et ceux des valeurs morales fondées sur la défense de l'intérêt public. Ce dernier englobe non seulement le droit d'accéder à des informations en lien avec la gouvernance du pays, mais également la notion de « redevabilité ». Cela signifie que les citoyens doivent avoir la possibilité de demander aux gouvernants de rendre des comptes. L'ambivalence de WikiLeaks reste entière dans ce contexte. Mais qu'en est-il des #AKPleaks et des #DNCleaks ?

Le #DNCleak est intéressant non seulement parce qu'il est encore très actuel, mais également parce qu'il pose (de nouveau) la question de la confiance. La « *transparence radicale* » promue par WikiLeaks semble s'exprimer complètement ici. Qu'est-ce qui apporterait plus de transparence que la publication de machinations préélectorales d'un des partis dans la course ? La publication des communications internes de tous les partis, par exemple[55]. Car cette action est entachée par les soupçons de vendetta personnelle d'Assange contre Clinton et la médiatisation de la possibilité d'une interférence russe dans la gouvernance américaine.

55 : Cette approche peut être difficile avec Trump qui n'utilise pas le mail : https://www.bloomberg.com/politics/articles/2016-06-20/trump-strategy-meeting

Les rancunes personnelles sont le premier point d'achoppement dans cette histoire. En 2012, Anonymous a pris ses distances avec WikiLeaks dénonçant le « *one man show qu'est devenue* »[172] l'organisation.

"The idem behind WikiLeaks was to provide the public with information that would otherwise be kept secret by industries and governments. Information we strongly believe the public has a right to know.

But this has been pushed more and more into the background, instead we only hear about Julian Assange, like he had dinner last night with Lady Gaga. That's great for him but not much of our interest. We are more interested in transparent governments and bringing out documents and information they want to hide from the public."

« L'idée derrière WikiLeaks était de fournir au public des informations qui seraient sinon tenues secrètes par des entreprises et des gouvernements. [Il s'agit] d'informations que, nous le croyons fermement, le public a le droit de connaître.

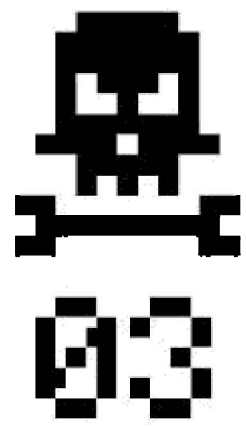
Mais cela a été relégué toujours davantage à l'arrière-plan ; à la place, nous entendons seulement parler de Julian Assange, par exemple de son dîner hier soir avec Lady Gaga. C'est super pour lui mais ce n'est pas vraiment intéressant pour nous. Nous nous intéressons davantage à la transparence des gouvernements et à la diffusion des documents et informations qu'ils souhaitent cacher du public. »

De son côté, Alex Gibney, l'auteur du film *We Steal Secrets : The Story of WikiLeaks*, raconte ses « *six heures d'agonie* »[173] en compagnie d'Assange en 2013. Il explique comment la discussion qu'il a eue avec Assange a constamment dérivé loin des questionnements éthiques pour se concentrer sur le ressentiment personnel du fondateur de WikiLeaks à l'encontre de ses contradicteurs et sur la vengeance qu'il leur promettait. L'ego joue un rôle prépondérant ici. Assange a pris des positions publiques très fortes contre Hillary Clinton, alors comment, dans ce cas, ne pas voir le #DNCleak comme une vendetta ?

Cette discussion ne nous fait pas vraiment honneur : les bisbilles personnelles sont du niveau d'une cour de récré. La possibilité d'interférence russe est cependant intéressante. Nous avons vu qu'Assange avait son programme sur la chaîne gouvernementale Russia Today ; la rumeur qui attribue le hack ayant fourni les e-mails à des Russes semble plausible étant donné l'opposition éternelle entre États-Unis et Russie (voir chapitre 01). Si l'on veut jouer l'avocat du diable et user des mêmes arguments, on pourrait arguer de l'intérêt public qu'aurait la divulgation de la source de ces e-mails. Les doutes qui planent au-dessus de WikiLeaks et de la nature de sa relation avec la Russie ont aussi trait au passif peu recommandable d'Assange qui a fuité des documents pour servir ses propres intérêts personnels. En 2010, Assange transmet 90000 « câbles » diplomatiques relatifs à la Russie, à des pays de l'Europe de l'Est et à Israël à un mystérieux journaliste du nom de Israel Shamir. Ce dernier les propose par la suite à des médias russes pro Poutine pour la modique somme de 10000 USD. De sérieux doutes existent également sur l'impact de certains de ces télégrammes en Biélorussie : Shamir est suspecté de les avoir transmis au dictateur Loukashenko juste avant la purge de ce dernier contre ses opposants. Enfin, le hasard faisant bien les choses, Israel Shamir est également le père du journaliste suédois Johannes Wahlstrom, lequel a organisé et coordonné une campagne de dénigrement à l'encontre des deux femmes ayant accusé Assange d'agression sexuelle. Il ne faut cependant pas oublier la notion de vie privée. Assange est connu pour sa posture radicale. En 2010 par exemple, avant la publication des fuites liées à l'Afghanistan et à l'Irak, les documents relatifs à l'intervention américaine en Afghanistan sont publiés sans les noms d'une centaine d'Afghans ayant collaboré avec les Américains. Des hacktivistes travaillant avec WikiLeaks se sont débrouillés pour retravailler les documents et enlever les noms avant de rendre les documents publics. Voilà une démonstration élégante d'une gestion efficace des données sensibles. Cette attention n'a cependant pas duré… Toujours en 2010, après le refus du

Département d'État d'y contribuer, les « câbles » diplomatiques sont publiés par WikiLeaks sans anonymisation. Idem dans le cas des #AKPleaks, sans tenir compte de la purge après le coup d'État raté.

Dans le cas des #DNCleaks, la question de la vie privée relève encore plus du nœud gordien. D'une part, on peut arguer que les employés gouvernementaux, qu'ils soient chargés de mission ou fonctionnaires, ont à répondre du contenu de leurs correspondances (voir l'affaire concernant Sarah Palin, page 159). La publication des messages échangés par l'équipe de campagne de Hillary Clinton et les pontes du parti Démocrate, à condition que ceux-là couvrent des informations d'intérêt public, ne relève pas de la vie privée. Mais publier des données personnelles et les échanges familiaux desdits employés ou fonctionnaires qui ont pu se glisser dans les e-mails professionnels n'a rien de normal. Nous avons vu que la confiance est « *le centre de gravité* » de WikiLeaks, la sphère numérique en général ayant un effet amplifiant sur le rôle de messager dans beaucoup de cas. Si la confiance est un messager investi du pouvoir amplificateur du web, c'est la crédibilité de WikiLeaks et, par extension, de ce que l'on peut faire avec le numérique dans cette sphère qui est en jeu. Au début, à l'âge d'or de WikiLeaks, la crédibilité de l'organisation était incontestable. Aujourd'hui, WikiLeaks est dans la bouche de Donald Trump à chaque déclaration, à partir du moment où un journaliste écrit sur WikiLeaks, la personne s'attire les foudres de centaines d'utilisateurs de Twitter aux vues politiques très (très) à droite. Avec le jeu trouble auquel se livre Assange, de moins en moins aligné avec l'adage « la fin justifie les moyens », il devient très difficile de continuer de faire confiance à WikiLeaks. Plus encore, notre monde étant de plus en plus tributaire de la technologie, des données et des algorithmes, on peut légitimement s'interroger sur les pouvoirs et contre-pouvoirs qui s'y logent et en résultent. Assange cristallise en partie ces tensions et ces problématiques profondes. En tant que tel, il laissera une trace ambivalente dans l'histoire moderne.



03

LE DARKWEB : DES MOTS ET DES MAUX

× × ×

01

OÙ EST LE DARKWEB ?

Dans la stupeur caniculaire de l'été 2016, le député de Paris du parti Les Républicains Bernard Debré défraie la chronique en découvrant, sidéré et outré, le darkweb. Immortalisé dans une vidéo[1], le député s'exclame, choqué : « *la France est une plaque tournante de la drogue, un supermarché de la drogue !* » Mieux : la France est tellement en perdition que M. Debré s'est apparemment fait livrer cocaïne et champignons hallucinogènes à l'Assemblée nationale, en collaboration avec le quotidien très à droite, *Valeurs Actuelles*. Celui-ci ne manque pas de taxer La Poste de « *premier dealer en France* » : en effet, les drogues achetées par le député ont été livrées de façon tout à fait ordinaire, en colis, et dans les délais impartis par le service postal français. Dans son élan, Bernard Debré est également intervenu sur la chaîne de télévision LCI[1] évoquant l'« *incroyable* » Darknet *(sic)*, un « *supermarché* » où l'on peut acheter « *de tout* », énumérant aussi bien « *des kalachnikovs, du TNT, des faux billets, des organes à greffer* » que de la cocaïne. D'après le député, on peut se procurer tous ces objets en quelques clics et en payant simplement avec une carte bancaire.

> *« Le Darknet dérégule même les dealers de drogue (physiques) en France ! C'est l'ubérisation de la drogue. »*[2]

Les journalistes de *Valeurs Actuelles* ont fait tester les produits achetés : la cocaïne notamment est « *la plus pure possible* »,

1 : https://www.youtube.com/watch?v=RaUGdrik74Q
2 : https://twitter.com/LCI/status/747705766019207169?ref_src=twsrc%5Etfw

et « *pour un prix semblable à celui du marché* ». Alors qui sait, peut-être que les dealers de rue feront eux aussi leur transformation digitale *(sic)* pour être dans l'air du temps… Le député a, quant à lui, trouvé la solution miracle pour que la France arrête d'être un « *marché de la drogue* » : interdire le bitcoin.

Quelques minutes et deux paragraphes auront suffi pour révéler la méconnaissance des enjeux du numérique par certains élus, le sensationnalisme politiquement orienté de certains médias et les amalgames anxiogènes qui frôlent la désinformation[3]. La peur primaire de ce que l'on ne connaît pas et qui ne nous est pas facilement accessible nourrit des fantasmes effrayants, c'est humain. Mais peut-être que tenter de démystifier et comprendre de quoi il s'agit est une option intéressante, surtout quand on est investi par ses concitoyens du pouvoir de proposer et voter les lois de la République.

Alors, qu'est-ce que le darkweb ? Est-ce pareil que le Darknet ? Mais alors, pourquoi parfois cela s'appelle-t-il « deep web » ? Comment va-t-on « là-bas » ? Et que trouve-t-on dans ces coins obscurs ? N'est-ce vraiment qu'un repaire de criminels ? Si certains passages vous semblent difficiles ou trop détaillés à suivre, c'est normal : on parle de mécanismes complexes, très dynamiques, impliquant de nombreux acteurs. Dites-vous bien cependant que vous n'avez pas à tout retenir pour comprendre les enjeux, lesquels sont effectivement de plus en plus riches et complexes.

3 : Lorsque, comme moi, à ce moment-là, on travaille au sein d'une start-up suisse spécialisée dans le bitcoin et autres cryptomonnaies, et qui a une licence d'opérateur financier délivrée par l'Autorité fédérale de surveillance des marchés financiers en Suisse, entendre « il faut une loi pour interdire le bitcoin en France », votre réaction est : « tiens, c'est étrange ». En plein buzz français autour de la blockchain – une technologie inhérente au bitcoin – et des institutions telles que la Caisse des dépôts et consignations, les banques BNP et Société Générale, l'assureur Axa… qui s'y intéressent fortement, les propos de Bernard Debré semblent, à mon sens, venir d'un autre âge.

LE DARKWEB N'EST PAS UN ENDROIT

« *Le dark web (« web sombre ») est une portion de la Toile à laquelle on accède par un logiciel.* » C'est vrai que d'habitude, on utilise des poneys… Cette phrase, tirée d'un article[4] publié par le site web *The Conversation*, ne veut pas dire grand-chose. En effet, comment accéder au web (et à Internet) sinon avec un logiciel ? On utilise des navigateurs web (Mozilla Firefox, Chrome, Safari, etc.) et des clients e-mail (Thunderbird, Outlook, etc.) pour accéder à une partie ou à une autre de « *la Toile* » sans parler du fait que notre système d'exploitation (Windows, MacOS, Ubuntu, etc.) est un logiciel géant à lui tout seul.

On apprend dans ce même paragraphe introductif qu'il y aurait un « *web officiel* ». On ne sait pas ce que c'est et encore moins qui a décrété que c'est officiel, mais ces formulations annoncent la couleur. Et effectivement, l'article continue dans la même veine menaçante :

« De nombreux sites marchands y font leurs affaires ; ils vendent principalement des produits illicites, drogues et armes à feu, payables en cryptomonnaie, le Bitcoin. Dans le dark web, on a même pu se cotiser sur une plate-forme de financement participatif pour organiser des assassinats.

En raison de l'anonymat quasi total qui y règne, c'est une terre d'élection pour tous ceux qui cherchent à se faire oublier des gouvernements et de la justice. On y trouve ainsi des lanceurs d'alerte qui recourent au dark web pour communiquer avec les médias. Mais ce sont les pédophiles, les terroristes et les criminels qui l'utilisent le plus. »

Tout est fait ici pour faire (très) peur ; aucune source, aucune ressource n'est citée pour étayer ces affirmations. Pour un site web tel que *The Conversation*, qui se targue de ne donner la parole

4 : http://theconversation.com/le-dark-web-quest-ce-que-cest-47956

qu'à des chercheurs et universitaires, la qualité de cet article est discutable. Allez, au lieu de tirer sur l'ambulance, explicitons cette nébuleuse de concepts qu'est le darkweb. Nous nous attarderons également sur les détails techniques, nécessaires pour appréhender la complexité de la question. La question cruciale de ce chapitre touche à des mécanismes, pas à des lieux. Qu'est-ce qui explique l'émergence et la persistance de ces réseaux alternatifs ? Et comment posent-ils de véritables défis à l'idée que l'on se fait de la confiance à l'ère du numérique ?

Commençons par les bases : les mots « darkweb », « deep web » et « Darknet » ne sont pas interchangeables. Le mot « web » n'équivaut pas le mot « net » ; cela revient à dire qu'Internet n'est que l'ensemble des sites web. Ce réductionnisme est dangereux car non seulement il omet la diversité des services existants (l'e-mail, les protocoles de chat, etc.) mais aussi parce qu'il ignore totalement l'histoire et les motivations des architectes des darknets. Parce qu'en réalité, il n'y a pas un Darknet, mais plusieurs, et il est donc d'autant plus idiosyncrasique de l'orthographier avec un « D ».

Clarifions d'abord le « deep web »[5]. Ce dernier fait référence à ce qui n'est pas indexé par un moteur de recherche classique tel que Google. Cette partie non indexée du web n'a rien de « dark » : les contenus protégés par un mot de passe, par exemple, ne sont pas indexés par les moteurs de recherche traditionnels[6]. Si vous publiez un statut Facebook que seuls vos amis peuvent voir, ce contenu ne sera pas indexé par les moteurs de recherche qui ne « voient » que les statuts publics. Il en est de même avec les articles sur les sites web d'un journal comme *Le Monde*, que l'on ne peut consulter que si on y est abonné, ou avec vos

5 : Le terme date de 2000 et est décrit en détails dans cet article de recherche : http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf.

6 : Il y a différents types de contenus autres que ceux protégés par mot de passe qui composent le « deep web » : voir à ce sujet la page Wikipédia dédiée https://fr.wikipedia.org/wiki/Web_profond (en français) ou https://en.wikipedia.org/wiki/Deep_web (en anglais).

relevés bancaires disponibles après connexion à votre service de banque en ligne. C'est, somme toute, plutôt un bon point : ce serait vraiment désagréable de retrouver ses relevés bancaires en tapant quelques mots-clés dans la barre de recherche. Donc félicitations : vous allez sur le « deep web » tous les jours !

Au tour des darknets et du darkweb. L'internet grand public que l'on connaît n'est pas le seul réseau d'ordinateurs au monde ; des implémentations alternatives[7] existent depuis les années 1970, à commencer par un réseau dédié à la défense et séparé de l'Arpanet[2]. Le darknet est un réseau superposé (appelé encore « réseau overlay », pour reprendre le terme anglais) : ce sont des services type internet déployés sur un ensemble de protocoles et d'infrastructures déjà existants[3]. Cette définition reprend finalement un tas de services, pas seulement un darknet : la VoIP (voix sur IP), de plus en plus utilisée pour la téléphonie moderne, crée un réseau overlay.

Prenons le cas de la Poste pour illustrer de manière plus concrète notre propos : les courriers circulent entre expéditeurs et destinataires. Cette circulation s'effectue *via* des protocoles et infrastructures déjà en place. Ainsi les conventions sont-elles standardisées : il faut mettre un timbre (enfin, sauf si vous écrivez à la Présidence de la République ou au Père Noël), déposer le courrier dans une boîte à lettres d'où il sera pris en charge par les employés du bureau de Poste qui le trieront et classeront. Lorsque le classement est fait, le transport est organisé vers un centre de tri de la commune de destination où le facteur de votre destinataire le récupère pour le livrer. Mais comme vous le savez, l'infrastructure de la Poste permet également la circulation d'autres services tels que les colis, les lettres recommandées avec accusé de réception, etc. De la même manière, différents types de darknets existent en fonction de leur infrastructure : les réseaux pair-à-pair et les réseaux mixtes (mixnet) anonymes.

7 : Une implémentation est un système d'exploitation ou un logiciel adapté aux besoins et à la configuration informatique de l'utilisateur.

QUI SONT CES TUYAUX ET QUELS SONT LEURS RÉSEAUX ?

Les réseaux pair-à-pair (*peer-to-peer* en anglais), abrégés P2P, servent le plus fréquemment à l'échange de fichiers. Une catégorie particulière du P2P est le réseau F2F (pour *friend-to-friend,* soit « ami à ami »). La particularité des réseaux F2F est que la connexion, anonyme et chiffrée, ne se fait qu'entre amis. Ainsi, seules les personnes à qui vous faites confiance peuvent échanger des fichiers avec vous. La confiance est matérialisée par une reconnaissance de leur adresse IP ou de leur signature numérique. Cette confiance est également transitive : si vous êtes mon ami(e), les vôtres, qui ne sont pas dans mon réseau, peuvent indirectement échanger des fichiers avec moi. Dans ce cas, les protocoles F2F n'utilisent pas mon adresse IP mais une sorte de « canal » se chargeant de faire suivre automatiquement et anonymement les fichiers et les demandes de fichiers.

L'un des premiers et plus anciens darknets F2F est Freenet[4]. Il existe (pour le grand public en tout cas) depuis le mois de mars 2000. Nous avons déjà évoqué les logiciels libres (voir chapitre 01) : Freenet en est un, ainsi que les différents logiciels qu'il regroupe. Ceux-ci permettent de créer et de naviguer parmi des pages web, d'échanger des e-mails, de parler via un chat type IRC, etc. Freenet a depuis le début été pensé et créé comme un réseau politique. Nous reviendrons sur l'importance significative des idéologies politiques au long de ce chapitre car celles-ci sont un pilier des darknets[8]. Reprenons notre métaphore postale. Si l'on souhaite envoyer des livres à nos amis, on prend la liste de leurs adresses personnelles et on les leur envoie. Si l'on veut en envoyer à des amis de nos amis, on peut le faire indirectement aussi, en faisant transiter par les connexions communes. Comme on le mentionnait dans le chapitre 02, l'accès à l'information et à la connaissance disponibles en ligne a joué un rôle structurant dans l'évolution du numérique au

8 : Darknet est par exemple un terme de Freenet justement, celui qui correspond aux connexions F2F https://freenetproject.org/documentation.html.

sens large. Il en est de même ici : les réseaux F2F se popularisent surtout en tant que « darknet » en 2002, lorsque des chercheurs de Microsoft publient un article intitulé « *The Darknet and the Future of Content Distribution* »[5]. Connaissant les tentatives d'entreprises telles que Microsoft d'instaurer des technologies DRM (*Digital Rights Management,* « gestion des droits numériques »[6]), il n'est pas étonnant de lire dans ce texte que la présence de darknets constitue l'obstacle principal au développement des DRM[7]. En effet, ces derniers sont aussi connus comme des « verrous numériques » car ils empêchent les utilisations de contenus numériques suivant le contexte, soumettant l'utilisation au bon vouloir du créateur du support. Les technologies DRM fonctionnent de la même manière : la lecture d'un support peut être limitée à une zone géographique ou à un modèle d'appareil. Leurs concepteurs ont même poussé le zèle en tentant de créer des DRM capables de compter le nombre de personnes regardant un DVD : si ce nombre excède celui autorisé par la société vendant le DVD, ce dernier ne se lance pas… Bonjour l'ambiance devant la télé pour décider qui doit partir pour que les autres puissent regarder le film ! Cela peut paraître ridicule, mais ces contraintes hérissent depuis toujours les défenseurs de logiciels libres et open source, ainsi que tous ceux qui défendent une circulation libre de l'information et de la connaissance.

Petit à petit, la notion de « darknet » est sortie du cercle des spécialistes et internautes avertis pour entrer dans les médias généralistes. Ces réseaux mixtes anonymes, les mixnets, ont gagné en renommée et sont devenus « le Darknet ». Dans la suite de ce livre, on ne parlera que du darknet le plus connu, un mixnet déployé *via* le logiciel d'anonymat Tor. Aujourd'hui, on peut schématiser en considérant que la plupart des darknets F2F ont également une composante mixnet. Cela permet d'en populariser l'utilisation. Ainsi, Freenet a été étendu dès 2008 pour autoriser les échanges au-delà du cercle d'amis. I2P et Zeronet ont des composantes très diverses dont le partage de fichiers. Mais d'autres, tels que GNUnet ou RetroShare, continuent à faire du seul F2F.

Avant de se plonger en eaux méconnues, n'oublions pas de mentionner le darkweb. De manière similaire au web « clair », le darkweb est une couche applicative : on a le réseau (protocoles de transmission de données) et au-dessus, on peut faire des sites web, des blogs, des réseaux sociaux, etc. Ces derniers, la couche « de dessus », constituent le web. La majorité des darknets intègrent aujourd'hui cette couche web. Le darkweb est donc l'ensemble des sites web d'un darknet. Dans le cas le plus fréquent, qui est le nôtre dans ces pages, on parle également d'*onionland* (que l'on pourrait traduire par la « Terre d'oignons ») en référence au logiciel *The Onion Router*, plus connu comme Tor, qui permet l'existence d'un darkweb.

Vous l'avez compris, « le Darknet » n'existe pas, contrairement aux darknets. Avant d'explorer le plus célèbre des darkwebs, l'*onionland*, intéressons-nous rapidement au fonctionnement de Tor, aux origines de ces technocultures alternatives et à une des cryptomonnaies les plus célèbres : le bitcoin.

TOR : CE NE SONT PAS LEURS OIGNONS

Tor[8] a été initialement conçu par la marine américaine comme outil de chiffrement et d'anonymisation de ses communications ; dès 2004, le code source du logiciel est rendu public. Un projet associatif est alors monté. Ainsi, lorsque l'on parle de Tor aujourd'hui, on parle du projet associatif indépendant de la marine et, plus largement, du gouvernement américain (ou d'un quelconque autre gouvernement)[9]. Le fonctionnement de Tor est celui d'un réseau overlay distribué ; il est composé de nœuds (des serveurs *via* lesquels transite le trafic) dont la liste est publique[9].

9 : Un débat aux saveurs complotistes existe selon lequel les financements de Tor étant en grande partie de sources publiques, l'organisation obéit nécessairement à ses bailleurs de fonds. S'il est vrai que l'association touche des subventions publiques, il est également vrai que rien dans une telle démarche ne permet d'affirmer qu'il y a des clauses secrètes associées. Pour toute personne qui aime à fouiller dans les rapports financiers et fiscaux, ceux-là sont disponibles sur le site web du Tor Project.

Le nom de Tor, comme nous l'avons précisé ci-dessus, reprend la métaphore de l'oignon. Comme on le verra par la suite, il peut en faire pleurer plus d'un. Ce n'est pas de larmes dont il est question ici, mais de chemises d'oignon. Ces « chemises » sont les nœuds du réseau Tor ; ce sont elles qui assurent l'anonymat de la navigation. Pour faire simple, voici les étapes d'habillage :

0. Récupération de la liste des nœuds : si vous passez par le navigateur Tor (un navigateur Mozilla Firefox modifié), cette opération est faite automatiquement et sans que vous vous en rendiez compte.

1. Nous souhaitons aller sur wikipedia.fr : on tape cette URL dans la barre d'adresse du navigateur, on clique sur « Entrée ». Le navigateur, à condition d'être connecté à Internet, envoie la requête. La sélection des relais qui feront transiter le message est faite : un circuit (ou une chaîne de relais) est ainsi créé. Le chiffrement de votre requête se fait ici et aucun nœud du circuit ne « sait » quel est son ordre dans la chaîne[10].

2. La requête est prise en charge. C'est ici qu'intervient l'idée d'oignon : imaginez que le cœur d'un oignon soit votre message. Donc, les paquets (vous savez, on en parlait dans l'introduction, c'est ainsi que fonctionne Internet) constituant la requête sont encapsulés dans trois couches de chiffrement. Ces dernières correspondent aux différents relais du parcours dans le réseau Tor. Pour accéder au message, il faut « faire tomber les chemises ». La partie protection de l'anonymat est assurée par le fait que votre adresse IP est visible par ce nœud n° 1, mais pas par les nœuds suivants du circuit.

3. Le nœud n° 2 reçoit les paquets chiffrés ; ce relais ne voit que deux adresses IP : celle de son prédécesseur et celle de son héritier, le nœud n° 3. La première « chemise », soit la couche de chiffrement la « plus externe » si l'on veut, est enlevée à cette réception.

4. Le nœud n° 3 récupère ensuite les paquets chiffrés ; ceux-là sortent du circuit Tor et sont envoyés vers le serveur-cible. Il ne voit que l'adresse IP de son prédécesseur et de sa cible.

En parlant de nœuds, épargnons-nous en au cerveau : on ne s'étendra pas sur les différents chiffrements-déchiffrements à chaque étape du circuit. Ce qui compte, c'est qu'une seule étape du circuit est au courant de votre adresse IP et que chaque saut de nœud à nœud au sein du circuit est chiffré. Toute personne qui le souhaite peut héberger des nœuds et contribuer ainsi à enrichir le réseau[10]. Si vous hébergez un relais Tor, vous verrez du trafic passer mais vous n'en saurez pas grand-chose vu qu'il sera chiffré (l'équivalent numérique du gloubiboulga, on en reparlera brièvement plus loin). Enfin, aucun des nœuds ayant servi à faire aboutir votre requête ne connaît la totalité du circuit. Pour l'utilisateur, ces étapes sont totalement transparentes : vous demandez une adresse, elle est servie, point[11].

Ce que l'on vient de décrire est le principe de fonctionnement de Tor. L'utilisation que l'on peut en faire est de deux grands types : naviguer sur le web clair en restant anonyme ; utiliser les services cachés de Tor. Dans les deux cas, l'approche la plus simple et courante est d'installer le navigateur Tor et de l'utiliser en lieu et place du navigateur habituel. Contrairement au web clair, les services cachés (les fameux *.onion*) ne peuvent être créés et visités qu'en utilisant Tor. Ils permettent de masquer l'adresse IP de serveurs les utilisant ; il n'est donc pas possible de savoir qui opère ni où est située cette personne. Leur mise en place requiert une première configuration locale du serveur (par la personne le gérant) ; celui-ci est ensuite pointé par Tor pour permettre à des personnes extérieures d'y accéder. Lorsque le serveur est pointé, il reçoit une adresse en .onion (*16chiffresetlettres.onion*). Le service caché est prêt !

Toute personne, quelles que soient ses motivations, peut ainsi se servir de l'outil. Les usages faits par des dissidents politiques en sont un bon exemple. Les tentatives pour compromettre le réseau

10 : En France par exemple, l'association Nos Oignons en héberge plusieurs. N'hésitez pas à les approcher si vous souhaitez des informations ou proposer votre soutien. https://nos-oignons.net/

11 : Vous pouvez consulter la thèse de doctorat d'Éric Freyssinet (pp. 44-45), pour un descriptif détaillé du fonctionnement de Tor en français https://crimenumerique.files.wordpress.com/2015/12/theseericfreyssinet-lutte_contre_les_botnets.pdf

Tor sont nombreuses et continuelles. Certains essaient de le bloquer sur le territoire d'un pays (en bloquant les adresses IP des nœuds par exemple) ou de l'attaquer avec des approches techniques malveillantes pour altérer durablement son fonctionnement. Diverses attaques permettent de « dé-anonymiser » les utilisateurs, c'est-à-dire d'enlever les « chemises » et plus largement de collecter des détails tiers sur le système afin d'avoir accès à des informations permettant d'identifier les utilisateurs. Dans la suite de ce chapitre, on ne s'intéressera qu'aux usages relatifs au darkweb *onionland*.

LES CYPHERPUNKS : LE CHIFFREMENT COMME ÉTENDARD

On peut retracer l'idée d'un cyberespace sans surveillance et respectueux de la vie privée aux Cypherpunks. Le nom de ces derniers est une contraction, à l'origine humoristique[11], entre « cyberpunk » et « cipher ». Le cyberpunk est un genre littéraire dont le nom provient de la combinaison entre cybernétique et punk. Si vous connaissez William Gibson (*Neuromancien, Mona Lisa s'éclate*) ou Phillip K. Dick (*Blade Runner, Total Recall* adaptés au cinéma par Paul Verhoeven, ou encore *Minority Report* adapté par Stephen Spielberg), vous connaissez le genre cyberpunk. La narration touche toujours à la tension profonde entre une société technologiquement très avancée et l'impact déstructurant de cette même technologie sur le tissu social et sociétal. Ces dystopies technico-scientifiques sont habituellement grinçantes et assez pessimistes. Le mot « cipher » signifie, lui, en anglais, « chiffre », au sens de cryptographie. C'est le moyen par lequel un message clair est transformé en message chiffré. Si, par exemple, nous décidions que chaque lettre a d'un message est remplacée par des triangles, le message résultant d'une telle réécriture sera un autre message, chiffré par substitution (on remplace un signe par un autre).

De « chiffre » est dérivé « chiffrement », soit le fait, par des moyens informatiques, de chiffrer un message, soit de transformer

un message d'une façon telle que seulement des acteurs spécifiques peuvent y accéder. Il existe le chiffrement à clés symétriques et celui, plus complexe, à clés asymétriques. Dans le cas du chiffrement symétrique, on utilise le même mot-clé pour chiffrer le message. Certains protocoles utilisant cette approche permettent de chiffrer de gros messages : ils sont ainsi performants[12]. Mais la faiblesse principale du chiffrement symétrique reste la nécessité, préalable au chiffrement lui-même, de partager une clé secrète identique entre les parties concernées. Le risque est donc de voir le système compromis si la clé est interceptée par une tierce partie.

Dans le cas du chiffrement asymétrique, deux clés existent : l'une est dite privée (seul son propriétaire la connaît), l'autre est dite publique (on peut la diffuser largement). C'est un avantage clair par rapport au chiffrement symétrique en ce que rendre publique l'une des clés permet le chiffrement et l'authentification de l'envoyeur sans risquer la compromission du système entier. La clé publique « reconnaît » sa partenaire et permet de déchiffrer le message. Ainsi, je suis la seule à pouvoir chiffrer mon message clair avec ma clé privée mais toute personne ayant ma clé publique pourra le déchiffrer. L'inverse est vrai aussi : toute personne m'envoyant un message chiffré avec ma clé publique est sûre que je saurai le déchiffrer avec ma clé privée correspondante. L'opération est mathématique[12]. Ainsi, outre la garantie de confidentialité du message, le chiffrement permet un contrôle de l'intégrité : on peut être raisonnablement sûrs que le message n'a pas été modifié lors de son acheminement.

Enfin, le chiffrement asymétrique permet une deuxième chose : la signature numérique, c'est-à-dire l'authentification de l'origine du message. En sécurité informatique, l'identification

12 : Les détails cryptographiques et mathématiques ne sont pas pertinents pour la discussion que nous avons ici. La thématique est cependant très intéressante et est rendue accessible par le livre de Simon Singh, *Histoire des codes secrets*, dont je recommande la lecture. S'il ne nous permet pas de devenir des spécialistes, il retrace brillamment l'histoire humaine de la recherche de la sécurité des communications.

et l'authentification ne sont pas interchangeables. Il est tout à fait possible d'identifier qu'un message provient de *kimkardashian@gmail.me* mais ce n'est que si ce message a été chiffré avec la clé privée de Mme Kardashian que je pourrai authentifier qu'elle en est bien l'expéditrice. L'authentification permet donc de passer un cran au-dessus de l'identification : on s'assure que la personne qui nous écrit est bien celle qu'elle prétend être. Enfin, ce procédé assurant également l'intégrité du message, on peut donc être sûr que personne n'a modifié notre message entre le moment où il est envoyé et celui où il est reçu.

Pour finir, rappelons ce que vous devinez ou savez déjà : les techniques de chiffrement sont nombreuses, évoluent en permanence, ont des fonctionnalités différentes et sont utilisées par différents services. Puisque nous avons parlé de Tor et d'anonymisation, précisons que le chiffrement permet la confidentialité et la sécurité, notions qu'il convient de distinguer d'anonymat. Communiquer en utilisant du chiffrement ne vous rend pas anonyme ; l'anonymat ne garantit pas le chiffrement. Si vous voulez camoufler le contenu d'un message, vous le chiffrez. Si vous voulez dissimuler l'identité de son expéditeur, vous utilisez un outil d'anonymat. Si vous voulez la combinaison, vous utilisez des moyens d'anonymisation (tel que Tor) et de chiffrement.

LA PREMIÈRE BATAILLE POUR LE CHIFFREMENT

Les points les plus techniques désormais clarifiés et la signification du chiffrement expliquée, revenons à l'histoire des Cypherpunks. Ceux-ci se préoccupent d'anonymat, de vie privée et de droits numériques. L'idée essentielle est de protéger ces caractéristiques vitales de la vie humaine grâce à des outils dédiés. La valeur fondamentale est la liberté : ne pas dépendre d'un système politique centralisé qui infantilise, ne pas vivre sous surveillance, avoir accès à des services financiers de base, etc. Très longtemps avant l'avènement d'Internet et du web grand public, il était déjà

important de chiffrer les échanges[13]. Comme nous l'avons expliqué dans l'introduction, les débuts d'Internet sont militaires. Ce désir de protection des communications est donc tout sauf surprenant. Dès les années 1970, des réflexions se mettent à développer cette idée, mais c'est surtout le travail de l'universitaire américain David Chaum qui marque les débuts des Cypherpunks. Figure quelque peu tutélaire, il théorise l'anonymat des communications électroniques en 1981[13] (!) et les premières monnaies numériques dès 1982[14]. Le travail de Chaum sur les réseaux anonymes a donné naissance aux mixnets, dont on a déjà parlé (voir p. 241).

Différentes personnes contribuent à élargir la réflexion et les outils. Ainsi, vers la fin des années 1980, la communauté devient une sorte de mouvement travaillant pour promouvoir l'utilisation d'outils de chiffrement comme un moyen d'établir de nouvelles interactions sociétales et politiques. Julian Assange faisait alors partie des Cypherpunks. Dès 1992, la célèbre liste de diffusion des Cypherpunks devient le principal forum d'échanges techniques autour de la cryptographie, la politique et l'impact de la technologie sur la société. La lire s'approche d'un travail à temps plein (en moyenne, deux cents messages par jour) et on peut, de temps à autre, y voir des gens inscrits « à l'insu de leur plein gré », petit service rendu par quelqu'un qui ne leur veut pas que du bien… Les canulars de l'époque étaient à haute valeur intellectuelle, c'est certain.

Le contexte est extrêmement important pour comprendre la signification des Cypherpunks. Les thèmes principaux incluent la vie privée à l'ère du numérique (eh oui, déjà dans les années 1990) et le pouvoir d'un gouvernement de surveiller les communications électroniques. C'est l'époque où le gouvernement américain considère tout logiciel de chiffrement au même titre qu'une munition destinée à l'export, donc comme une menace sérieuse à la

13 : Le chiffre de César est par exemple l'un des chiffres les plus anciens. On retrouve l'apparition du chiffre déjà au XVI^e siècle avant J. C. (https://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie#Les_premi.C3.A8res_m.C3.A9thodes_de_chiffrement_de_l.27Antiquit.C3.A9).

sécurité nationale. Ce genre de produit est donc interdit à l'export par la loi, étant donné qu'il est possible de l'utiliser en dehors des États-Unis. Connue comme la première Cryptowar[15], la période est mouvementée : le créateur de PGP (« Pretty Good Privacy », le tout premier outil de chiffrement grand public), Phil Zimmermann, fait l'objet de poursuites pendant plusieurs années. Pour démontrer l'ineptie de telles restrictions, Zimmermann publie la totalité du code source de PGP sous forme de livre universitaire papier[16]. Certes, l'export de munitions est prohibé, mais celui des livres est protégé par le premier amendement de la constitution américaine. Dans le même état d'esprit, des codes et des clés de chiffrement ont également décoré des t-shirts. On savait s'amuser à l'époque.

La législation a depuis changé, les poursuites ont été abandonnées : si des restrictions persistent, les outils de chiffrement ne sont plus considérés comme des armes interdites à l'export[14]. Zimmermann et ses collègues ont créé PGP Inc. pour se consacrer au développement d'outils divers basés sur PGP. En 1997, PGP Inc. est racheté par Network Associates Inc., plus tard racheté par McAfee[15]. Comme le code source de PGP était ouvert, d'autres développements entrepreneuriaux ont également vu le jour et ont été acquis en 2010 par Symantec. Si les noms McAfee et Symantec sonnent familiers, c'est parce qu'il s'agit de deux gros éditeurs commerciaux de solutions antivirus.

L'ENNEMI EST-IL LE TERRORISME OU LES MATHS ?

Pour de nombreux observateurs et experts, la deuxième Cryptowar a cours depuis environ l'année 2015. Il y eut en effet une recrudescence fulgurante des mesures législatives, tentées ou abouties, de mettre à mal le chiffrement. Ainsi, suite aux attaques terroristes

14 : En France, il faut attendre la LCEN de 2004 pour que l'utilisation du chiffrement soit libérée (l'exportation en est toujours soumis à autorisation). Voir http://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie/
15 : Connue depuis 2013 comme Intel Security.

de janvier 2015 à Paris, le Premier ministre britannique de l'époque, David Cameron, provoqua l'ire d'une communauté aussi surprenante que vaste en appelant à introduire une interdiction légale du chiffrement au Royaume-Uni[17]. Le problème avec une telle (dé)mesure est que de nombreux services numériques quotidiens se retrouveraient « à poil » sur Internet : les banques en ligne, l'e-commerce, etc. nécessitent l'utilisation de HTTPS pour assurer la sécurité des transmissions de données client. Interdire l'utilisation du chiffrement au Royaume-Uni pour empêcher des terroristes en devenir de s'en servir peut être considéré comme absurde.

Suite aux mêmes attaques terroristes, John Brennan (le directeur de la CIA sous Obama, voir chapitre 02) a attaqué les limites déjà peu efficientes imposées par le gouvernement américain à la surveillance des communications[18]. En France, le gouvernement français du premier ministre de l'époque, Manuel Valls, a amorcé l'adoption, en procédure accélérée, de la loi sur le renseignement. Celle-ci a été (vivement) discutée à l'Assemblée, avant d'être définitivement adoptée, car introduisant des mesures d'interceptions ; parmi celles-ci, l'équivalent de l'atteinte au secret des correspondances[19] comme incidence d'une collecte massive de données, ou encore l'installation de sondes d'interception et des « boîtes noires » d'analyse automatique du réseau au niveau des fournisseurs d'accès Internet.

Les modifications apportées par la loi sur le renseignement s'ajoutent à une batterie de mesures légales. Le Code de procédure pénale permet déjà aux « *officiers de police judiciaire de requérir de toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition* », soit de leur remettre les informations qui permettent l'accès à ces données[20]. En outre, seulement quelques mois auparavant, une autre loi renforçant les mesures de lutte contre le terrorisme[21] avait déjà modifié et étendu le chapitre « *De la mise au clair des données chiffrées nécessaires à la manifes-*

tation de la vérité » du Code de procédure pénale. Il en est de même avec l'introduction, à l'été 2016, d'une autre loi de lutte contre le terrorisme et le crime organisé[22]. Cette dernière élargit par ailleurs et de manière significative les opportunités d'utilisation de procédés d'interception (les *IMSI catchers* dont nous avons parlé au chapitre 01). À toutes ces nouvelles mesures de recueil de données et de moyens d'expertise s'ajoutent des tentatives et déclarations hostiles au chiffrement qui dépassent les frontières nationales. On peut par exemple rappeler le bras de fer qui a opposé, outre-Atlantique, le FBI et Apple, suite aux tentatives du FBI de forcer Apple à développer une porte dérobée permettant l'accès aux contenus de l'ensemble des téléphones similaires. Ce conflit, qui s'est soldé par le développement d'une solution « maison » par le FBI sans le secours d'Apple, a cependant fait resurgir des positions en faveur d'un affaiblissement légal du droit au chiffrement.

Demandons-nous alors quels sont les nombreuses méthodes utilisées pour affaiblir ou limiter le chiffrement. Lors de la première Cryptowar, l'introduction de portes dérobées ou de moyens permettant à l'exécutif d'accéder à des données chiffrées[16] étaient courants. Une autre approche affaiblissant le droit au chiffrement est la certification obligatoire, par l'État, des fournisseurs de services ou solutions de chiffrement. Il s'agit également d'un système utilisé pendant la première Cryptowar aux États-Unis ; une telle certification signifierait en pratique que des services que l'État ne s'estime pas en mesure de contrôler peuvent être rendus illégaux. Appliquer un coût de certification à un service ou produit logiciel serait par ailleurs néfaste pour l'entrepreneuriat car imposerait des dépenses additionnelles à de petites structures, ce qui se résumerait à mettre un frein à l'agilité et l'innovation. D'autres moyens, plus techniques, impliquent d'imposer une limitation de la longueur des clés. Dans le cas du chiffrement, la taille a une importance : plus la clé est longue, plus il faut de temps pour effectuer les opé-

16 : Les portes dérobées sont des failles intentionnelles laissées par les concepteurs de produits et services pour permettre un accès, ici aux autorités.

rations mathématiques permettant de la « casser ». Or, si les clés sont compromises ou affaiblies d'entrée, la confiance qu'on y met le sera également. Ceci vaut pour tout service ou produit utilisant le chiffrement, chose totalement quotidienne pour nous et nos usages en ligne. Ainsi revient-on à la nécessité de bien distinguer les tenants et aboutissants de décisions politiques, industrielles et légales : combattre le terrorisme, la pédophilie et le crime organisé n'est pas une raison suffisante à l'affaiblissement du chiffrement. L'institution judiciaire a les moyens de poursuivre des infractions pénales et à justifier que, pour ce faire, il soit porté atteinte à des libertés individuelles et collectives.

Ce qui est important ici, c'est que toutes ces actions se déroulent dans des conditions d'encadrement respectant des principes de nécessité et de proportionnalité. Autrement dit, le délinquant ou le criminel reste un internaute comme les autres : qu'il s'agisse de quelqu'un communiquant des instructions pour commettre un attentat ou d'un pédophile ayant trouvé comment écouter des babillages enfantins *via* une poupée Barbie connectée, on parle de gens qui commettent des infractions. Par ailleurs, est souvent évoqué l'argument que le chiffrement diminue les pouvoirs d'enquête. Il faut relativiser : des moyens d'expertise divers et permissifs existent déjà qui permettent d'obtenir des informations sans nécessiter de décrypter les messages : faire appel à des experts judiciaires, des juges d'instruction, infiltrer[17], etc. Ainsi, il revient à l'enquêteur d'imaginer des approches alternatives qui permettraient d'appréhender des agissements et constituer des preuves sans que les moyens pour ce faire compromettent la sécurité et la vie privée des citoyens.

17 : Les informations disponibles quant aux pratiques de communication de djihadistes par exemple montrent qu'ils utilisent la messagerie Telegram surtout pour son « réseau social » (donc, discussion de groupe) mais peu s'en servent en sa version chiffrée. Ainsi, l'infiltration ici relève d'une pratique traditionnelle d'enquête, le chiffrement ne jouant aucun rôle dans l'obtention d'informations. Par ailleurs, toutes les études spécialisées des usages du darkweb menées jusqu'à présent révèlent «*la quasi-absence de l'extrémisme islamique* » dans ces espaces. On y reviendra.

NOUS AVONS TOUS QUELQUE CHOSE À CACHER

Nous le voyons bien : les Cypherpunks ont eu un impact significatif sur le fonctionnement actuel de nombreuses composantes fondamentales du monde numérique. Celles-là n'en finissent pas de moduler et impacter notre gouvernance. Les motivations de la création acharnée et passionnée de ces outils sont ce que l'on connaît comme le *Cypherpunk Manifesto*[23]. Dans ce texte, quatre grands thèmes sont présentés comme les piliers du mouvement :

1 – vie privée et secret des communications ;

2 – anonymat numérique ;

3 – censure et surveillance ;

4 – cacher qu'on se cache.

Le secret des communications est une revendication évidente. Il s'agit de préserver le fait que ce que j'écris dans mes messages est lu seulement par le(s) destinataire(s). Quand on bavarde entre amis par exemple, on n'a pas envie d'être épié et écouté en temps réel par des gens externes à notre cercle de proches. Comme nous l'avons déjà expliqué précédemment, cette nécessité de la vie privée n'a rien à voir avec le fait d'avoir ou pas « quelque chose à cacher ». L'anonymat garantit une expression sans obstacles et sans autocensure, mais permet aussi de jauger ce qui est exprimé sans le biais d'une réputation à tenir. La posture fallacieuse « je n'ai rien à cacher » sous-entend que seuls les criminels souhaitent se cacher pour ne pas que leur malveillance éclate au grand jour. Il est très important de tordre le cou à un tel pseudo-argument, toujours très actuel : nous avons tous quelque chose à cacher, que ce soit la couleur de nos sous-vêtements ou les secrets de fabrication du plat vedette de notre restaurant étoilé. Aussi bien les individus que les entreprises ont des informations précieuses qu'ils souhaitent garder pour eux. Pour reprendre une phrase que l'on croise parfois,

dire que l'on n'a rien contre la surveillance car on n'a rien à cacher, c'est comme dire qu'on n'a rien contre la censure parce qu'on n'a rien à dire[18].

Quant à la censure et la surveillance des communications justement, les Cypherpunks ne sont pas très confiants vis-à-vis du gouvernement américain. À cette époque, ce dernier promeut le Clipper Chip, un moyen de contrôle technique des échanges téléphoniques permettant de sécuriser les conversations contre diverses intrusions, mais laissant la porte ouverte aux agences de renseignement américaines. Ces dernières seraient donc en mesure d'utiliser ces portes dérobées pour lire les communications des citoyens. Un des Cypherpunks, Matt Blaze, a trouvé des vulnérabilités compromettant le Clipper Chip en 1994, ce qui a accéléré l'abandon de cette technologie[19]. Enfin, lorsque l'on chiffre ses communications et que l'on reste anonyme sur le web, il est possible que ces caractéristiques soient tellement uniques qu'elles en deviennent un moyen de différenciation, voire d'identification. Ainsi, il est important de dissimuler même le fait que l'on cherche l'anonymat et le secret des échanges.

Les Cypherpunks ont été des fondateurs et des figures marquantes de nombreuses entreprises, initiatives et solutions logicielles. Nous avons parlé de PGP, NAI… mentionnons également Open Whisper Systems, l'entreprise qui édite l'application mobile Signal ; l'EFF

18 : Cet argument fallacieux est tellement répandu qu'il existe une page Wikipédia qui lui est dédié : https://fr.wikipedia.org/wiki/Rien_%C3%A0_cacher_(argument)

19 : http://portal.acm.org/citation.cfm?id=191193 C'est également à cette époque que le principe de *warrant canary* a été inventé : il s'agit d'une façon ingénieuse de communiquer au public les demandes gouvernementales de transmission de données utilisateurs. Nous avons déjà parlé des *National Security Letters* très à la mode après la passation du *Patriot Act* ; d'après celles-là, l'entreprise à qui on demande des informations ne peut pas en informer ses clients. Une manière de contourner ce bâillon est de publier un *warrant canary*. Ce dernier précise que pendant une certaine durée (indiquée), l'entreprise n'a pas été visée par une demande gouvernementale de transmettre des données utilisateurs. Si le *canary* est modifié ou retiré, c'est qu'une telle demande a été faite. C'est une analogie avec le canari ou le pinson apporté par les mineurs lorsqu'ils descendaient dans les mines de charbon : si le canari mourait, c'est que l'atmosphère n'était plus respirable. Voir http://io9.gizmodo.com/why-did-they-put-canaries-in-coal-mines-1506887813

(*Electronic Frontier Foundation*), une ONG américaine dont le but est de protéger les droits numériques et de fournir des outils d'auto-défense numérique au grand public : le principe de la CryptoParty, les chiffrofêtes où chacun(e) peut apprendre à se servir des (très) nombreux outils disponibles aujourd'hui et dont la prise en main n'est pas toujours aussi aisée qu'on l'aimerait ; John Gilmore est le créateur de la sous-section « alt. » dans les groupes Usenet dont on a parlé dans le chapitre précédent ; etc.

Retenons deux Cypherpunks notables : Jim Bell et David Chaum. Nous avons déjà évoqué David Chaum. Quant à Jim Bell, il est l'auteur d'un essai célèbre, intitulé *Assassination Politics* et un cas notable de phobie administrative bien des années avant l'ex-secrétaire d'État français au commerce extérieur, Thomas Thévenoud[20]. S'il est vrai que l'on peut se gausser de la phobie administrative, lire *Assassination Politics*[24] est une autre paire de manches. Écrit entre 1995 et 1996, l'essai contient dix grands chapitres et décrit une manière de motiver membres de gouvernements et fonctionnaires dans leur travail quotidien : la prédiction du jour de leur décès. D'abord publié *via* alt.anarchism, l'essai développe deux façons d'implémenter l'idée de base. Ainsi, soit chacun peut ouvrir ce genre de pari de manière publique, soit on choisit d'utiliser des signatures numériques et du chiffrement pour protéger les parieurs. Les paris sont collectés dans une cagnotte commune et les devises sont une quelconque monnaie électronique. La résolution reste la même quelle que soit l'implémentation : le parieur qui devine le jour de décès de la personne cible remporte le montant de la cagnotte. L'idée est que les cibles (membre de gouvernements, hauts fonctionnaires, etc.) se verraient motivés pour

20 : McCullagh, Declan (2001-04-09). «Cypherpunk's Free Speech Defense». Wired. http://archive.wired.com/politics/law/news/2001/04/42909?currentPage=all
Pour rappel, Thomas Thévenoud, membre du gouvernement en 2014, en a démissionné après que ses déboires avec le fisc ont fait les gros titres (http://www.lemonde.fr/politique/article/2014/09/05/comment-valls-a-demissionne-thevenoud_4482850_823448.html). Cette démission est intervenue seulement neuf jours après la nomination de M. Thévenoud qui a évoqué une « phobie administrative » pour justifier le fait qu'il ne payait pas ses impôts.

faire leur travail correctement et ne céderaient pas aux sirènes de la corruption à col blanc si une telle épée de Damoclès était suspendue au-dessus de leurs têtes. Le système décrit par Bell n'interdit en rien à quelqu'un de parier sur le jour du décès et de s'occuper personnellement de ce que la prédiction se réalise. Visiblement, la possibilité d'abus (terrorisme, justiciers de tous genres, lynchage, etc.) et la menace qu'un tel système représenterait pour les minorités n'ont pas effleuré l'esprit de Jim Bell… On peut apprécier, voire adhérer aux idées et positions des Cypherpunks ou en être rebuté. Quoi qu'il en soit, il est facile de comprendre que l'utilisation d'outils informatiques avancés fournissant anonymat et protection du secret des communications va au-delà de la « geekerie » : il s'agit avant tout d'un projet politique.

LES MONNAIES NUMÉRIQUES ALTERNATIVES

En 2016, le mot « blockchain »[21] a été mis à toutes les sauces. Des projets se sont montés visant prétendument à révolutionner chaque aspect de notre vie avec la blockchain, mais se révélant des implémentations bancales de systèmes préexistants. Effet de mode oblige, le leitmotiv « faire du vieux avec du neuf » et le buzz qui en a découlé ont (presque) réussi à vider la technologie de son sens. Ce que l'on a également remarqué, au grand dam des nombreux aficionados du bitcoin, c'est que « blockchain, c'est cool » alors que « bitcoin, c'est sale ». Il s'agit en fait de plus ou moins la même chose et les fondements idéologiques et politiques de la technologie en question sont aux antipodes du buzz médiatique. Petit voyage en territoire de la finance pour comprendre en quoi le bitcoin est, lui aussi, un projet politique comme celui de Cypherpunks.

21: La blockchain est un registre qui permet de stocker et d'échanger des informations de manière fiable et non modifiable. Il s'agit d'une sorte de base de données décentralisée et partagée au sein d'un réseau de pair-à-pair, sans intermédiaire. Une blockchain contient l'historique de tous les échanges effectués entre ses utilisateurs chacun pouvant confirmer la validité de la chaîne. En général, les enregistrements sur la blockchain sont immuables (car chaque participant a une copie de la transaction chez lui). La blockchain constitue ainsi un grand livre comptable partagé, répliqué et infalsifiable.

David Chaum, le Cypherpunk à l'origine des mixnets, est également la première personne à avoir (presque) réussi à créer une monnaie électronique universelle, utilisée dans les années 1990. Il développe en effet un système nommé eCash, qu'il commercialise en 1989 à travers une entreprise nommée DigiCash. Cette dernière présente eCash comme étant surtout un moyen d'effectuer des micropaiements plutôt que comme un moyen de stocker de la valeur à proprement parler. Le design d'eCash est révolutionnaire : il inclut un registre des transactions distribué, les comptes clients sont chiffrés, l'intégrité du système est garantie et capable de prévenir les transactions redondantes, le niveau d'anonymat est relativement haut mais l'authentification des parties est toujours possible, etc. Fondé à Amsterdam, aux Pays-Bas, DigiCash a presque réussi à infléchir la course de l'histoire financière telle qu'on la connaît. En effet, Chaum prend le pari des banques et des institutions financières centralisées : eCash leur est vendu comme un moyen de décliner les devises nationales sous forme électronique ; ces institutions gardent leur rôle central car leurs ordinateurs ne servent qu'à confirmer les transactions. De son côté, le client a accès à des transactions plus transparentes et impliquant moins d'intermédiaires, donc coûtant moins. Et son pari prend plutôt bien : de nombreuses banques achètent des licences d'exploitation d'eCash et testent les micropaiements que cette monnaie permet.

Malgré toutes ces promesses, en 1998, DigiCash fait faillite. Les raisons de ce fiasco ne sont pas claires : certains disent que l'avènement de l'e-commerce pré-bulle dotcom a privilégié les cartes bancaires[25], d'autres qu'il y a eu des problèmes de management chez DigiCash. On peut aussi supposer que les banques n'étaient pas prêtes à laisser se développer un système de paiement limitant leur emprise. Aucun moyen de paiement de l'époque n'arrivait à la cheville d'eCash, mais le besoin d'un tel moyen n'existait pas non plus. Quelle qu'ait été la raison, DigiCash a fermé boutique et Chaum a vendu les brevets. L'avènement des

monnaies électroniques anonymes, décentralisées et sans intermédiaire, a été balayé par les débuts d'une oligopolisation[22] encore plus grande. C'est à partir de 1998 que les fusions de grandes banques commencent, avec la création de Citigroup Inc., l'un des principaux acteurs de la crise financière de 2008. Alors président des Etats-Unis, Bill Clinton amende la législation pour permettre la fusion du conglomérat financier Travelers Group et la banque commerciale Citicorp. Avant ces changements, une telle opération est impossible : les banques commerciales et les banques d'investissements doivent rester séparées. Le résultat de cette fusion, Citigroup Inc., est l'un de ces supermarchés géants de services bancaires et financiers qui n'ont pas hésité à prendre des risques spéculatifs avec les épargnes des clients commerciaux (individus et entreprises). Plutôt que d'assurer la sécurité des épargnes et des crédits, ces monstres banco-financiers ont introduit un système de rente à haut risque : la rente pour eux, le risque pour les clients. On se souvient de la crise de 2008, de la chute presque imminente du système monétaire international et de la paupérisation galopante qui s'en est suivie.

FACE À LA CRISE FINANCIÈRE, LA DÉCENTRALISATION DU BITCOIN ?

La crise financière et la publication de l'article de recherche décrivant le fonctionnement du bitcoin sont presque concomitantes. Est-ce que Satoshi Nakamoto, pseudonyme de l'auteur anonyme du bitcoin, a attendu ce moment-là pour publier son travail ? Nul ne le sait. Étant donné le positionnement politique du bitcoin (décrit par Nakamoto), on peut imaginer que la crise de confiance que représente la crise financière de 2008 est un moment opportun : quelle meilleure illustration pour la position de Nakamoto du pouvoir destructeur certain de la centralisation de l'argent ? Diverses tentatives

22 : Un oligopole est un marché caractérisé par un petit nombre de vendeurs qui se partagent la totalité du marché, face à un grand nombre d'acheteurs.

(que ce soit DigiCash ou des expérimentations au sein de Citicorp avant qu'elle devienne Citigroup Inc.) montrent que le remède à cette centralisation excessive ne viendra pas de l'intérieur non plus.

Ainsi, en 2008, juste un mois après la faillite de la banque Lehman Brothers, Satoshi Nakamoto envoie son article décrivant la monnaie à la liste de diffusion des Cypherpunks. Beaucoup parmi les inscrits sur la liste ont tout simplement survolé et archivé l'e-mail. Pour les Cypherpunks, l'idée de cash électronique anonyme n'est pas nouvelle ; de nombreuses tentatives ont eu lieu mais aucune ne s'est révélée viable. L'implémentation de Nakamoto reprend pratiquement toutes les caractéristiques des tentatives précédentes : le chiffrement asymétrique pour assurer et authentifier le transfert de valeur ainsi que le stockage (une sorte de portefeuille), l'ensemble des règles visant à garantir l'intégrité du système monétaire décentralisé, la possibilité de chacun d'être un nœud dudit système et de pouvoir être garant de son intégrité et de l'utiliser pour des transactions financières. Le but du système de Nakamoto ? Le même que celui de chacune des tentatives précédentes : rendre le modèle de système monétaire actuel inutile et le remplacer à terme, les ordinateurs des individus se substituant aux banques et autres institutions financières.

Le registre des opérations, décentralisé et universel, est la blockchain (aussi parfois appelée en français la « chaîne de blocs »). Chacun peut y vérifier les transactions passées à tout moment. Le système de récompense inhérent au bitcoin (la monnaie elle-même) fournit suffisamment de motivation pour les gestionnaires du registre de continuer à le garder en bonne santé et à jour. Comme d'autres essais de monnaies par le passé, celui proposé par Nakamoto utilise la preuve de travail (« *proof of work* »[23]). Au risque de me faire taper sur les doigts par les spécialistes, disons qu'il s'agit du traitement cryptographique permettant la validation des

23 : Le système hashcash a été créé par Adam Back ; son utilisation première était la lutte contre le spam qui, à l'époque, proposait essentiellement du Viagra et des moyens d'augmentation de la taille de votre pénis.

blocs de transactions. Chaque transaction effectuée entre les utilisateurs est inscrite sur un bloc et vérifiée avant d'être validée par les « mineurs » : il s'agit du « minage ». Les mineurs sont récompensés par l'octroi périodique d'une quantité donnée de bitcoins.

Nakamoto est le pseudonyme d'une personne ou d'un groupe de personnes ; jusqu'à aujourd'hui, nul ne sait qui se cache derrière[24]. Le statut de nouveau venu parmi les Cypherpunks ne contribue pas à soulever les foules. Malgré tout, l'un des Cypherpunks, Hal Finney, développeur principal à PGP Inc. et auteur d'une tentative de création de monnaie électronique, s'y intéresse. Les premières transactions en bitcoin ont ainsi eu lieu entre Nakamoto et Finney aux premiers jours de 2009[25]. Le système se précise et se perfectionne : il est réellement décentralisé, la technologie blockchain permet d'ordonner chronologiquement les transactions et fournit aux mineurs le moyen de confirmer et vérifier chaque transaction à tout moment. Un tel chaînage des opérations reposant sur une validation publique, transparente et décentralisée permet également de s'assurer que nul ne fait de transaction redondante, dépensant ainsi des bitcoins qu'il n'a pas. Bon courage pour créer des « faux billets » dans ce système !

La seule chose que nous n'ayons pas encore abordée, c'est la valeur de cette monnaie électronique. Le système pensé par Nakamoto prévoit une quantité finie de bitcoins. Ces derniers étant la récompense de l'activité de minage, il faut trouver une manière ingénieuse de les distribuer. La quantité de la récompense est ainsi

24 : Ou ceux qui savent se gardent bien d'en parler. D'aucuns suspectent un autre développeur brillant d'être Satoshi Nakamoto : il s'agit de Nick Szabo, le créateur d'une monnaie nommée bit-gold. Même si Nakamoto connaissait l'existence de Szabo et son travail, il n'en fait mention nulle part. Que les deux soient ou non la même personne n'enlève rien à la contribution de Szabo à une réflexion globale et politique de l'importance de la gouvernance financière pour l'ordre sociétal.

25 : Hal Finney est aujourd'hui en état de mort clinique suite au développement fulgurant de la maladie de Charcot. Son corps est conservé, cryogénisé, dans une clinique américaine ; les frais médicaux de conservation jusqu'à l'éventuel réveil pour traitement lorsque celui-ci existera sont assurés en grande partie par les bitcoins minés aux tous débuts de cette monnaie.

divisée par deux tous les quatre ans. En anglais, on appelle cet évènement « *the halvening* » ; le dernier a eu lieu en juillet 2016. D'après ce modèle, chaque récompense de minage pendant les quatre premières années d'existence du bitcoin était de 50 BTC ; elle était de 25 BTC avant le *halvening* de l'été dernier, et elle est désormais de 12,5 BTC pour les trois prochaines années et quelques mois.

UN AUTRE SYSTÈME FINANCIER EST POSSIBLE

Ce système constitue un mécanisme décentralisé de confiance financière. Aucun point de contrôle centralisé n'existe, il est donc difficile (pour ne pas dire impossible) de faire s'écrouler le système. Même si aujourd'hui, avec la nécessité d'avoir des machines très performantes pour miner, le pouvoir de minage est à plus de 50 % concentré dans des « fermes » chinoises, il sera toujours difficile d'arrêter le bitcoin : chaque mineur a une copie du registre distribué (la chaîne de blocs donc). Le bitcoin est ainsi domicilié nulle part et partout à la fois.

La gouvernance du bitcoin provoque également des émules. Son statut juridique provoque des débats (très) vifs : ainsi, certaines juridictions la traitent comme un bien[26] alors que d'autres y font référence en tant que monnaie[27]. Si ce dernier cas venait à être adopté pour de bon, nous serions dans la situation ubuesque de devoir imaginer les mêmes régulations pour le bitcoin que pour n'importe quelle devise nationale et d'établir ses instances dirigeantes. Viser l'exploration spatiale pour 2020 est plus réaliste...

Quel que soit son statut cependant, la question de gouvernance reste entière. Vu sa nature, le bitcoin (ou toute autre cryptomonnaie parmi les quelques milliers existantes[28]) devrait-il être soumis à la décision des mineurs ou bien des développeurs du logiciel ? Les mineurs l'obtiennent mais sans les développeurs, rien n'existerait. Et inversement : les développeurs auraient beau créer un logiciel, sans les gens qui l'utilisent, leur travail n'aurait pas

vraiment de sens. Si l'on pousse cette réflexion plus loin, on peut inclure l'écosystème au sens large dans cette équation. En effet, il n'y a pas que les développeurs et les mineurs ; les créateurs d'applications (portefeuilles, plugins de paiement, etc.) et les places de marché de change sont des acteurs à part entière de cette communauté. Alors, si on a besoin de prendre une décision, qui devrait le faire ? Et comment ? Voter est une option, mais la question de la délégation de confiance se repose. Etc. Décentraliser et supprimer les intermédiaires des transactions financières va ainsi bien au-delà de la question du logiciel : comme dit plus haut, on est face à une question politique fondamentale de gouvernance.

Que ce soit bitcoin, monero, ether, eCash, nous sommes donc face à une multitude de protocoles informatiques qui permettent d'envoyer de la valeur (dont monétaire) d'une personne à une autre et sans aucun intermédiaire. Comme le dit Andreas Antonopoulous[29], ce genre d'interactions est un nouveau système financier, par et pour le peuple. La gouvernance de ces cryptomonnaies est par chacun et par personne à la fois, sans qu'aucune autorité centrale ne s'y mêle. Plus largement, le « cash électronique » que ces cryptomonnaies constituent, est seulement une application parmi d'autres de la technologie blockchain. On voit ainsi apparaître des systèmes de vote, des registres visant à remplacer des actes notariés, des fonds d'investissements, etc. Le futur semble décentralisé.

Avant de poursuivre, un petit exercice de prospective s'impose : le bitcoin remplacera-t-il les monnaies nationales ? Faisons ensemble et rapidement cette expérience intellectuelle.

OUI

Aujourd'hui, de plus en plus de commerçants acceptent les paiements en bitcoin et toujours plus d'associations mettent en place des dons en bitcoin. Les applications sont de plus en plus faciles à utiliser : votre « portefeuille » bitcoin permet de régler une bière dans un bar en plein Paris en flashant un QR code et il y a même des gens qui parviennent à voyager autour du monde pendant

18 mois en n'utilisant d'autre moyen de paiement que le bitcoin[30]. Il est bien évidemment facile de fantasmer sur l'horizon 2020 : nous resterions vautrés dans le luxe résultant des frais d'intermédiaires épargnés pendant que notre frigo intelligent fera les courses en flashant des QR codes comme un grand et que notre toaster préparera non seulement le pain sans gluten mais aussi le café…

Plus réaliste est cependant la masse critique d'utilisateurs du bitcoin : il s'agit de ceux qui n'ont pas accès à des services financiers de base. Pour une personne vivant en Europe occidentale et ayant un travail, un appartement et un ou plusieurs comptes en banque, la question de l'accès aux services financiers élémentaires ne se pose même pas. En revanche, elle se pose avec acuité pour des milliards de gens dans le monde : la moitié de la population, en fait[26]. L'utilisation de téléphones connectés à Internet permet d'envisager une adoption presque fulgurante de services financiers décentralisés par ces personnes. De même, un énorme marché (évalué à 500 milliards USD[31]) existe du côté des transferts d'argent par les émigrants économiques vers leurs pays d'origine. Rien n'est blanc ou noir, mais il y a des chances de bien développer certaines niches et d'introduire le bitcoin comme un véhicule de transfert de choix[32]. Et ça fera du monde, pour le coup. Ajoutons-y des applications gérant la production d'énergie verte (ensoleillement), les voitures autonomes qui feraient du covoiturage pour nous ramener à nos bureaux et les services commerciaux sans intermédiaires, et on est en pleine science-fiction. Mais notre monde n'était-il pas de la science-fiction pour les contemporains de Zola ?

NON

Une monnaie comprend trois piliers fondamentaux : elle est une unité de comptabilité, un moyen d'échange et un stockage de

26 : http://www.mckinsey.com/industries/financial-services/our-insights/counting-the-worlds-unbanked. La Banque mondiale a noté que le nombre a baissé de 2,5 milliards à 2 milliards entre 2011 et 2016 : https://www.weforum.org/agenda/2016/05/2-billion-people-worldwide-are-unbanked-heres-how-to-change-this.

valeur. Le bitcoin n'en est pas encore là. En outre, on peut dénoncer sa nature spéculative[34], ses motivations idéologiques sous-jacentes ou encore la dénaturation de ces dernières dans une visée totalement consumériste. Peut-être que le bitcoin rejoindra les archives poussiéreuses de l'Histoire aux côtés d'eCash et des autres tentatives passées. Comme eCash, il se peut que le buzz blockchain produise un compétiteur que les banques adopteront même s'il est moins performant que le bitcoin, renforçant ainsi l'emprise de ces institutions. Il est facile de payer en bitcoin aujourd'hui, mais on n'arrivera probablement jamais à une masse critique de consommateurs pour autant.

Revenons à nos moutons. Que le bitcoin réussisse à modifier en profondeur et durablement notre système financier actuel est pour l'instant pure spéculation. Il est cependant évident que cette approche des transactions financières rassemble toujours davantage de soutiens et que de plus en plus de gens comprennent qu'il y a autre chose derrière le simple rôle monétaire. De même, on ne peut que constater que darknets et darkwebs sont issus et structurés par des motivations politiques. Des darknets et darkwebs où on peut établir des interactions commerciales *via* des monnaies alternatives, où on peut continuer à apprendre et à créer étayent l'émergence d'un monde parallèle capable d'exister sans forcément se préoccuper de ce qu'il se passe au-dehors. Que l'on adhère ou pas à ces cultures *underground,* les communautés et les pratiques que l'on trouve sur le « darkweb » sont un reflet de notre monde « clair »[27]. Que trouve-t-on alors sur le darkweb le plus populaire, celui où Bernard Debré aurait acheté de la coke avec une carte bancaire ?

27 : Recommandation de lecture : le livre de Jamie Bartlett, *The Dark Net – Inside the Digital Underworld* (2014). Le livre explore le darkweb d'une manière beaucoup plus large, s'intéressant surtout aux pratiques et nettement moins aux aspects techniques. http://www.jamiebartlett.org/the-dark-net/

02

. . . .

VOYAGE EN TERRE D'OIGNONS

Comme nous venons de le voir, il existe une multitude de darknets dont la motivation première est souvent politique. Mais qu'y trouve-t-on réellement ? Aventurons-nous-y en mettant en cause quelques clichés à la vie dure.

COMMENT NE PAS ACCÉDER AU DARKWEB ?

Si vous cherchez une réponse à la question de l'accès au darweb dans votre moteur de recherche favori, vous avez de fortes chances de tomber sur des pépites d'ignorance. Déjà, en français, les notions que nous avons clarifiées plus haut (« deep web », « darknet », « darkweb ») sont utilisées de manière interchangeable, ce qui est une grossière erreur. Brisons les clichés.

On nous apprend sur un site internet[34] que *« les réseaux overlays [étaient] à l'origine isolés du réseau public. De nos jours, les dark nets sont des réseaux connectés à Internet, mais dont l'accès implique l'utilisation de logiciels, protocoles, ports, et configurations généralement non standardisés »*. Voilà donc que les standards ne concernent pas les réseaux overlay ! Il est certain que les technologies déployées par les fournisseurs de téléphonie et utilisées à chaque fois que vous vous servez de Skype ou de votre téléphone fixe, c'est un truc « *non standardisé* »… Par ailleurs, lorsque l'ancêtre des réseaux overlays a été mis en place, il n'y avait pas encore de « *réseau public* ». La vidéo[35] accompagnant

l'article finit de nous convaincre que quelques grosses lacunes sont présentes : il s'agit d'un bric-à-brac d'imagerie gothique et complotiste[28] sur fond de musique tonitruante. La vidéo explique que ce sont les navigateurs web qui indexent du contenu et montre une page noire avec du code dessus pour parler de bitcoin, le tout sur fond de musique dramatique[29]. De quoi glacer le sang, surtout quand on se rend compte que le code « super dangereux » qui est montré est en réalité l'habillage d'une page web…

Avant de passer à une autre perle, arrêtons-nous à deux recommandations de cet article : celle de fermer Tor si vous êtes sur le « web clair » et celle qui veut que l'utilisation du bitcoin soit « *probablement illégale* ». Même si on ne sait pas pourquoi, l'auteur de l'article invite fortement à éviter à tout prix d'utiliser Tor dans le cadre de notre utilisation quotidienne du web. C'est vrai, protéger sa vie privée lorsque l'on visite des pages web, en voilà une idée saugrenue… En fait, utiliser Tor de façon quotidienne n'a rien de bizarre : être anonyme sur le web empêche les sites web visités ainsi que votre fournisseur d'accès Internet de vous pister. Cette recommandation est donc aussi inepte que l'affirmation à propos des bitcoins. En effet, une quantité toujours croissante de commerçants, physiques et en e-commerce, qui introduisent le bitcoin comme moyen de paiement supplémentaire[30] ; de nombreuses associations acceptent les dons en bitcoin car elles récupèrent la totalité du don plutôt que d'en laisser des portions à des intermédiaires bancaires ; et enfin, en France ainsi que dans d'autres pays, on déclare ses avoirs en bitcoin et paye des impôts sur les bénéfices réalisés.

28 : On remarque par ailleurs que les contenus la composant ne portent pas de mention d'auteur : leurs créateurs ne sont donc pas crédités, ce qui constitue un cas potentiel de violation de droits d'auteurs et autres contrefaçons. Les mentions légales du site indiquent en plus que tout contenu sur le site appartient à son administrateur. Du coup, lorsque l'auteur de la vidéo nous raconte que le darknet (sic) permet de trouver plein d'articles contrefaits, on se dit qu'on n'a pas besoin de s'embêter à aller dans le darkweb pour en trouver…

29 : Comme quelqu'un plaisantait sur Twitter récemment, le darkweb n'est pas constitué de pages web dont le fond web est noir.

30 : Regardez par exemple cette carte https://coinmap.org/

Continuons donc notre petite exploration d'inexactitudes. Le web où il faut aller sereinement s'arrête là où commencent les sites web de zombies… Le deep web vraiment profond « *représente plus de 80 % du web, attention, pas en volume mais en concentration de l'information, selon la loi 80/20 de la nature, 20 % d'informations affecte 80 % de notre vie* » ; il s'agit d'un endroit très malfamé mais qui regorge également de solutions à des mystères éternels :

« [Il] est accessible par une modification matérielle : un "système Shell fermé". Ici, ça devient vraiment grave. Cette partie [.]. contient des informations sur le matériel expérimental (Gadolinium grenat de gallium processeurs Quantum électroniques.), mais aussi de plus sombres informations, telles que la "loi 13", les expériences de la deuxième guerre mondiale, et même l'emplacement de l'Atlantide. »[37]

Le cliché le plus drôle pour la fin : pour aller vraiment « *profondément* », il ne faut rien de moins que du « "*falcighol dérivation polymère", c'est tout simplement l'informatique quantique* ». Il s'agit d'un mythe très répandu fondé sur la (dés)infographie[38] qu'on trouverait sur le darkweb, d'après la légende, non seulement les secrets de la Seconde Guerre mais aussi les archives du Vatican[38] (avec le lot habituel des complotistes autour des francs-maçons), les archives des agences du renseignement les plus puissantes au monde[39] ou – très promotion des femmes – la base opérationnelle d'une unité très puissante d'intelligences artificielles féminines[40].

Alors, est-il si difficile d'accéder au darkweb ? Non, pas nécessairement. La question est surtout : êtes-vous suffisamment paranoïaque pour vous y promener de manière sécurisée ? Si vous êtes interloqué par cette question, vous comprendrez, à la fin de ce chapitre (lorsqu'on parlera des façons de se faire prendre) qu'il faut une bonne dose de paranoïa pour penser et prévenir tous les agissements qui pourraient se retourner contre

vous. Nous avons donc choisi de ne pas vous décrire comment procéder techniquement pour visiter des sites en .onion.

Ce qu'il faut comprendre, c'est que ce n'est pas y accéder le plus difficile ; les étapes techniques sont bien documentées et en différentes langues, dont le français, sur le web. De plus, un livre papier peut plus ou moins rapidement devenir obsolète niveau sécurité et numérique. En effet, le point central, c'est votre attitude lors de la navigation. On ne devient pas expert-e en sécurité en une nuit…

LES COINS (PAS SI) SOMBRES DE L'INTERNET

Émergent de cette série de clichés quelques réflexions : quelles ressources trouve-t-on dans le darkweb ? On lit souvent que 90 %, voire 96 % de l'Internet se trouve « sous l'iceberg ». Ailleurs, il est écrit que « *le deep web est plus de 500 fois plus gros que le web indexable* »[41]. Ah, cette propension à la « pifométrie »… Soyons sérieux et tordons le cou à quelques mythes aussi persistants que loufoques et dangereux.

La question des proportions de contenus darkweb *vs.* « web clair » est aussi inutile que mal posée : en la posant, on ne spécifie jamais de quel contenu et de quel darkweb on parle, à quel moment et à quoi on le compare. Il est cependant crucial de comprendre que le contenu est très dynamique, probablement beaucoup plus dynamique que ce que l'on a l'habitude de voir. Ainsi, des sites peuvent disparaître en une après-midi et ne plus revenir ; des sites (notamment marchands comme on le verra plus bas) peuvent renaître et continuer à subsister en version 2, 3, etc. sans égard pour la fermeture par la police du site d'origine. D'autres fois, des sites web peuvent être annoncés comme existant pendant une fenêtre de quelques heures seulement. Le même site web peut être dupliqué et exister en plusieurs exemplaires : ce point est cependant rarement

abordé dans les discussions sur la quantité de contenu. Enfin, avez-vous déjà vu une quantification précise, méthodique et à jour des contenus sur le « web clair » ? Ah, vous non plus ? Il est donc impossible de cartographier avec précision les quantités de ressources existantes dans le darkweb.

Les services cachés de Tor (appelés *Hidden Services*) sont reconnaissables à leur extension .onion ; ce sont les éléments auxquels on ne peut accéder qu'en passant par Tor. Ces services sont nombreux et surtout présents partout dans le monde[43]. D'après le Projet Tor[44], ces nœuds .onion sont un peu moins de cinquante mille. Il s'agit donc des services à partir desquels on peut créer son site, son blog ou son e-commerce sur le darkweb. Ce nombre n'est pas très intéressant car peu informatif. Ce qui est plus intéressant, c'est de comprendre quelle proportion du trafic Tor représente les .onion : d'après le Projet lui-même[45], moins de 5 % du trafic total opéré par Tor concerne les services cachés. Au sein de ces derniers, seulement certains sont liés à une activité manifestement illégale (pédopornographie, violence, drogues). Pas si glamour et morbide le darkweb, en fait.

LE DARKWEB EST-IL SEULEMENT UN REPAIRE DE CRIMINELS ?

Mais revenons aux .onion un peu plus en détail. Il s'agit d'un réceptacle que tout le monde peut créer et au sein duquel peuvent être déployées diverses applications. Le nom d'un .onion (l'équivalent de l'URL des services cachés) contient seize caractères alphanumériques. Ce nom est créé de façon automatique sur la base des paires clé privée/clé publique utilisées. Il est possible de mettre au point des adresses avec de vrais mots (le Facebook caché est par exemple accessible à *facebookcorewwwi.onion*). On peut très bien utiliser les services cachés créés par d'autres. Ainsi, par exemple, lorsqu'on se sert du Facebook caché, on ne le crée pas *ex nihilo*, mais on utilise un service préexistant.

Un .onion peut en effet héberger divers types de services tels qu'un site web, un logiciel de messagerie instantanée[31] ou encore un service d'e-mail. Tous ceux-ci sont nombreux : il y a en effet des sites pédopornographiques et d'autres qui vendent des armes et de la drogue, mais il y a également une foule d'autres services, à commencer par des copies de Wikipédia, des réseaux sociaux et de sites où les lanceurs d'alertes en devenir peuvent publier. Il y a également pléthore de sites d'information sur des sujets divers et variés, de l'évolution du bitcoin à des radios indépendantes diffusant de la musique indé.

Ainsi le darkweb est-il à l'image de la société humaine. Tant qu'il y aura de la violence hors d'Internet, il y en aura aussi bien sur le web clair que sur le darkweb. Si vous pensez qu'il est plus dur de trouver des malfaiteurs en ligne, détrompez-vous. Il est plus facile de débusquer des pédophiles en ligne que de fouiller tous les appartements parisiens en espérant y trouver des criminels. Mes échanges avec divers représentants des forces de l'ordre le confirment : il est plus pratique d'avoir tous ces suspects au même endroit. On parlera plus bas des opérations de police et des enquêtes sur le darkweb, dans le cas de Silk Road notamment.

Qu'y a-t-il donc de si malfaisant dans ce darkweb pas si sexy et pourtant sujet à tant de fantasmes ? Diverses études existent, aucune n'est (ni ne peut être) exhaustive. D'après une étude récente de la société Terbium Labs[45], plus de 50 % des 400 sites étudiés contiennent du contenu légal : des choses aussi quotidiennes que des blogs, des recettes de cuisine, des designers, des discussions sur les dysfonctionnements érectiles,

31 : Ricochet est par exemple un service de messagerie instantanée ; son fonctionnement est décentralisé : il crée un service caché sur l'ordinateur où on l'a installé mais sans créer de .onion. Ensuite, ce service caché permet à un utilisateur d'en trouver d'autres qui sont en ligne et de leur envoyer des messages. C'est totalement transparent : vous, l'utilisateur, ne voyez rien de ces procédures. https://ricochet.im/

etc. Pratiquement 45 % du contenu illégal a trait aux drogues, incluant aussi bien les substances illicites les plus sensationnalistes que des médicaments sur ordonnance (vendus sans elle, évidemment). Cette étude ne trouve pas d'armes mais a catalogué des sites pédopornographiques (3 % du contenu illégal).

Une autre étude couvre plus de 2 700 sites[46] ; les conclusions sont au contraire que presque 57 % de ces sites hébergent une forme d'activité criminelle. Cette dernière étude a de nombreux défauts : elle est extrêmement orientée idéologiquement, à un point tel que l'on se demande parfois si la classification des sites n'est pas volontairement biaisée.

Si un débat public mérite d'avoir lieu quant au rôle du chiffrement et de l'anonymat comme manière de se prémunir de la collecte permanente d'informations de la part d'acteurs privés et publics, le positionnement de cette étude est beaucoup moins nuancé et… scientifique : le leitmotiv aurait pu se résumer à « le chiffrement, c'est le mal ». Une telle vision manichéenne nuit à la qualité de la recherche. Pour ce qui est de la méthodologie, on n'a accès ni aux classifieurs ni aux données ; on ne sait pas combien de ces sites sont des doublons ; il n'y a aucune investigation quant à d'autres caractéristiques telles que l'hébergeur ; etc. La question des doublons est un véritable point de vigilance quand on cherche à savoir ce qu'il y a comme types de sites dans le darkweb : il est usuel d'avoir des doublons pour un site ; dupliquer un site légitime peut par exemple servir d'appât pour certaines escroqueries ou permettre de mieux gérer la charge. Comptabiliser et classifier uniquement des sites en HTTP est également un problème : une partie non négligeable des sites et services utilisent le HTTPS.

Enfin, l'étude fait un cas politique de ses résultats mais a la maladresse de surinterpréter l'usage des .onion d'une part, et de faire l'économie d'une véritable investigation de propriété de ces sites prétendument criminels. Nous le verrons, il est possible de savoir quel hébergeur est impliqué dans le fonctionnement d'un

site, ou encore de connecter des informations du « web clair » aux sites du darkweb. Exemple : cinq sites existent, avec des noms et des couleurs différentes mais vendant plus ou moins la même marchandise. Si on trouve qu'ils sont opérés par le même groupe de personnes, doit-on continuer à les considérer comme cinq sites ou comme un groupe de criminels ?

Cet exemple montre qu'une déclaration simpliste annonçant que « la majeure partie du darkweb est réservée à l'activité criminelle » ne constitue pas un argument valable. Ainsi, un décompte sans contextualisation quant aux opérateurs des services manifestement illégaux n'a aucun intérêt en criminologie.

LE DARKWEB : DU *SACRE DU PRINTEMPS* À LA FESSÉE

Si le contenu que l'on trouve sur le darkweb n'est pas si dangereux que cela, qu'abrite-il alors ? Vous avez des questions ? Il y a Quora sur le « web clair » – et Hidden Answers sur le darkweb. Vous voulez « liker » des photos de chats sur Facebook ? Pas de problèmes, il existe sur le darkweb aussi.

Vous souhaitez lire des sites d'information ? Il y en a également beaucoup, ainsi que divers blogs, et des sites de partis politiques. On trouve énormément de livres, des vieux, des inintéressants, des géniaux, des interdits, en téléchargement ou à l'achat, des clubs de lecture (même si celui du Silk Road original n'y est plus). Il y a des choses aussi idiosyncrasiques que des milliers de pages d'archives sur Igor Stravinsky, le compositeur russe auteur du célèbre ballet *le Sacre du printemps*, ou encore des sites entiers dédiés à des poètes. Un site se revendique des « fondamentalistes anti-Harry Potter » alors que d'autres inventent des histoires avec l'ours Balou de Disney. Une radio vous passe de la « *musique pour faire l'amour* » alors qu'une télé estudiantine se promène dans les tunnels sous une université américaine, comme on a déjà vu des documentaires

caméra à l'épaule suivre des gens dans les catacombes de Paris. On trouve des médicaments habituellement vendus sur ordonnance pouvant permettre à des gens sans couverture médicale suffisante de les acheter moins cher qu'en pharmacie. Il y a même des forums de discussions entièrement dédiés à la fessée…

Quel que soit le thème, il y aura non seulement quelqu'un mais une véritable communauté se passionnant pour celui-là ou un autre. S'il est vrai qu'il y a beaucoup de sites pas très reluisants, il y a également un vivier de cultures alternatives, d'échanges et de créativité qu'il convient de prendre en considération lorsqu'on s'intéresse au darkweb. Il est alors vraiment dommage qu'aucune de ces communautés n'ait fait les grands titres. De nombreuses activités nourrissent des peurs et fantasmes terrifiants. Qu'en est-il donc ?

LES « CHAMBRES ROUGES » : FANTASME OU RÉALITÉ ?

Avez-vous déjà entendu parler des *Red Rooms*, les terrifiantes « chambres rouges » ? On y filmerait des scènes de torture, de viol et des assassinats (pas nécessairement dans cet ordre) en direct. Du streaming gore, en somme. La légende veut que ces *Red Rooms* montrent tour à tour des gladiateurs modernes s'entre-tuer[48], des viols, des meurtres, des « dons » d'organes de la part de personnes non consentantes, etc. C'est un fantasme morbide que tous les nouveaux venus sur des forums tels que Reddit[49] cherchent à assouvir.

Ces *Red Rooms* n'existent pas. Convenons-en, ce n'est pas plus mal. De nombreux internautes et autres YouTubeurs[50] racontent qu'ils en ont vu, que ça existe, etc. mais au final, c'est un peu comme le Père Noël : beaucoup y croient, personne ne l'a jamais vu. Au mois d'août 2015, il y eut un engouement soudain autour des Red Rooms. Quelqu'un avait prétendu l'ouverture de *Bacon Room*[51], une « chambre rouge » où auraient été torturés et assassinés des terroristes de l'organisation État Islamique (EI). Quelqu'un aurait

détenu sept personnes de l'EI en un endroit tenu secret. Le 31 août 2015, ces terroristes auraient été torturés et assassinés, le tout sous l'œil attentif de darkwebonautes. Et gratuitement qui plus est. Quelques minutes avant que le *livestream* (soit le flux d'images diffusé en direct) commence, le site est tombé… Plus tard, un écran affichait un message du FBI indiquant que le site web avait été fermé. Rien ne dit que cette annonce était véridique non plus. On ne sait toujours pas aujourd'hui ce qu'il s'est réellement passé : certains avancent que le site était un « pot de miel » établi par le FBI pour identifier et appréhender des gens cherchant à regarder des assassinats en ligne[51]. Ou était-ce un canular très élaboré ? Ou bien une tentative de propager un quelconque malware à de très nombreuses personnes en même temps[52] ? On ne le saura probablement jamais.

Il est impossible de prouver que quelque chose n'existe pas (n'essayez pas, c'est un coup à se faire très mal à la logique). Analysons plutôt les sites qui disent être des *Red Rooms*. Ils ont plusieurs choses en commun :

- Ils prétendent tous vous montrer du *livestream* de torture et d'assassinats.
- Ils demandent un paiement élevé pour vous laisser voir ce qu'il y a à voir (en bitcoins généralement). Parfois, les transactions sont redirigées vers des navigateurs et services tiers.
- La page d'accueil est généralement bien gore : des images de traces de sang, de cadavres humains, etc. Ces images proviennent de films d'horreur et figurent sur le site en tant que promesse de ce que vous allez trouver une fois le paiement effectué. Parfois, la page d'accueil contient également un formulaire de login.
- On ne vous montre jamais un extrait de ce que vous êtes supposé-e voir une fois le paiement effectué.
- Parfois le site vous demande de télécharger et d'installer « *un logiciel spécial* ».

Il y a fort à parier que nous ayons affaire là à une escroquerie de mauvais goût. Tout d'abord, toute personne qui nous demande de payer une somme importante sans aucune garantie de recevoir ou voir la marchandise peut passer son chemin. C'est du bon sens. Mais regardons le côté un peu plus technique. Tor est lent car, comme nous l'avons expliqué plus haut, le trafic transite par les ordinateurs de bénévoles, de relais en relais. Cette lenteur fait partie de la FAQ du projet[53]. Alors, imaginez le niveau du streaming vidéo *via* cette infrastructure… Et encore, en comparaison avec Freenet et I2P, Tor est rapide. Bon… Admettons que la demande de téléchargement d'un logiciel « *spécial* » supplémentaire résolve ce problème. Nous avons déjà abordé la question du malware. Ici, le risque qu'il s'agisse d'un logiciel vérolé est élevé. Il est fort possible que ce genre de logiciel soit en effet un mouchard quelconque ou un *ransomware*[32]. La prudence est donc de mise.

Enfin, pour justifier la difficulté de trouver une *Red Room* opérationnelle, d'aucuns expliquent que les évènements qui sont censés s'y produire ont lieu dans des endroits interdits[55]. On cite notamment la Corée du Nord. C'est ingénieux et on aurait presque eu envie d'y croire. Mais comment une personne ferait-elle pour, primo, mettre en place un tel business en Corée du Nord ? Deuzio, mettre en place un système de « fourniture de victimes » ? Tertio, avoir un accès à Internet suffisant pour faire du streaming ? La Corée du Nord est une terrible dictature, ses citoyens sont sous une surveillance permanente et l'accès à Internet y est très sévèrement régulé. Passer outre ces limitations relève de l'exploit.

En conclusion, aucune preuve tangible n'existe à ce jour confirmant l'existence de ces « chambres rouges ». Il est difficile et assez dérangeant de savoir que d'aucuns peuvent fantasmer sur la torture et l'assassinat d'autres êtres humains au point d'en faire un mythe persistant, à l'image des *Red Rooms*.

32 : Ce genre de « logiciel spécial » traîne une autre légende urbaine avec lui : celle du Shadow Web, ou web des ombres. D'après la légende urbaine, il s'agit d'un endroit sur Internet (sic) encore plus terrifiant et noir que les Red Rooms et compagnie. Une autre fiction de YouTubeurs tels que Creepypasta et Takedownman.

LA PÉDOPORNOGRAPHIE ET LES *SNUFF MOVIES*

/!\ Malheureusement, il est des sites où la violence, loin d'être un mythe, est tout à fait réelle. Cœurs sensibles, s'abstenir (passez directement à la sous-section suivante donc).

Contrairement à un mythe soigneusement entretenu, on ne « tombe » pas sur les sites pédopornographiques accidentellement. Ces contenus ne sont pas là, au détour d'un Allociné ou de Wikipédia : il faut les chercher spécifiquement pour les trouver. N'en ayant jamais ni cherché ni consulté, la discussion qui suit est fondée sur des informations rendues disponibles par les autorités.

Diverses opérations de police ont permis d'arrêter les créateurs et opérateurs de plusieurs services de pédopornographie. Certains de ceux-là sont pires qu'épouvantables, s'il est encore possible de faire de la gradation dans l'atroce. La pédopornographie classique représente des images d'enfants et d'adolescents dans des positions sexuellement explicites. Une catégorie de la pédopornographie est connue sous le nom H2C ou « Hurt 2 the Core ». Connue sous le sobriquet « hurtcore », ce type de pédopornographie consiste en l'agression brutale d'enfants et la captation vidéo des exactions. Il ne s'agit pas de douleur accidentelle : faire mal aux enfants y est tout à fait intentionnel et prémédité. En 2014, la police australienne a réussi un coup de filet impressionnant[55] en appréhendant Lux et ses acolytes, l'un des réseaux les plus célèbres de hurtcore. Lux (Mathiew Graham de son vrai nom) a été jugé[56] et purge actuellement une peine de prison de quinze ans[57].

D'après les rapports de l'enquête de la police australienne, les divers sites du réseau H2C fonctionnaient comme forums de partage de contenus et d'échanges. On apprend également que si des utilisateurs créaient des contenus originaux (comprendre : leurs propres vidéos d'abus et d'agression d'enfants), ils étaient admis dans une partie cachée du site, une sorte de lounge VIP

du pédophile totalement dérangé. Le producteur le plus célèbre serait Peter Scully, un autre Australien, connu pour avoir créé la série *Daisy's Destruction*[57]. La légende urbaine veut que Daisy soit le prénom d'un bébé… le reste est assez clair, étant donné le contexte. Des disparitions d'enfants en bas âges ont été signalées, mais il n'y a pas de preuve tangible pour confirmer la rumeur. Des films de bébés torturés ont été saisis par la police australienne, certains des enfants ont été sauvés à temps et rendus à leurs familles. Scully aurait également créé une boîte de production, *No Limit Fun*, produisant des contenus sur le thème des agressions sexuelles envers de jeunes enfants, contenus par la suite vendus entre 100 et 10 000 USD[59]. L'Australien a été appréhendé et est actuellement en attente de jugement.

Les *snuff movies* sont une catégorie particulière de films (souvent classés en « porno ») : on est censé y voir un homme ou une femme se faire violer et/ou tuer. Le but annoncé de ces productions est clairement de divertir. Assurer que ce genre de films n'existe pas est délicat : des enregistrements multimédias d'exactions existent, mais plutôt de violences sexuelles que de meurtres. En effet, personne n'a jamais vu de vidéo d'assassinat à visée récréative, et le FBI maintient que ces vidéos sont une légende urbaine[60].

La situation est un peu plus compliquée pour les films d'exactions sexuelles. Il existe un marché pour ces contenus et il est hors du darkweb. Une enquête journalistique par Al-Jazeera English menée au printemps 2016 révèle[61] ainsi qu'en Inde, dans l'État d'Uttar Pradesh, de nombreuses échoppes vendent des DVD montrant de vraies agressions sexuelles. Souvent, les agresseurs utilisent la vidéo comme moyen de pression contre la victime, menaçant de la rendre publique si la personne les dénonce. D'autres fois, ces vidéos sont récupérées sur les téléphones des agresseurs dans des boutiques de réparation et vendues le plus largement possible par les réparateurs, sans que ni

l'auteur de la vidéo ni la victime soient au courant. Outre la vente de DVD, la propagation des vidéos est assurée *via* l'application mobile de messagerie WhatsApp. Ces contenus n'ont clairement pas besoin du darkweb pour circuler et perpétuer *ad nauseam* l'effet toxique et néfaste sur leurs victimes. Enfin, nous avons déjà abordé (voir chapitre 01) le revenge porn et la dissémination, *via* le web, de captations montrant des interactions sexuelles plus ou moins consenties ; ces pratiques sont courantes aux États-Unis et les vidéos sont propagées sur le « web clair » (Facebook, forums estudiantins, etc.).

Pas besoin donc d'imaginer des mises en scène outrancièrement macabres ou de fouiller le darkweb pour trouver des contenus d'une rare violence. Le site DeepDotWeb, un média grand public de l'écosystème darkweb, avait par ailleurs publié un sondage ouvert à ces visiteurs leur demandant de voter pour ou contre une interview avec un gestionnaire de site pédopornographique[62]. Malgré une majorité de « pour » et l'attrait publicitaire évident qu'un tel contenu aurait apporté, le site a décidé de ne pas publier l'entretien. Le directeur de publication a expliqué que les gens ayant voté « contre » ont apporté des arguments plus solides et ont contribué à prendre une décision dans le cadre de ce « *dilemme moral* ». Le fait que ce genre de contenu puisse choquer une partie des visiteurs a pesé dans la discussion[63]. Des contacts ont donc eu lieu entre DeepDotWeb et la BBC, qui a publié un reportage sur la question[64].

DES TUEURS À GAGES : L'HISTOIRE DE BESA MAFIA

D'aucuns ont déjà tenté de trouver un tueur à gages *via* Craiglist, un site de mise en relation très populaire aux États-Unis ; comme vous vous en doutez, l'histoire ne s'est pas bien finie pour le commanditaire en herbe[67]. Il y a eu d'autres cas : un ado qui, n'appréciant pas l'accusation de tentative de viol sur une de ses

camarades de lycée, a mis sa tête à prix (500 USD) sur Facebook[66] ; d'autres se sont tellement émus de constater que des personnes portent de la fourrure qu'ils ont eu recours à Facebook pour chercher un tueur à gages pour régler leur compte aux tortionnaires d'animaux ; manque de chance *(sic)*, le candidat pour le job était un agent du FBI[67].

Comme le darkweb est un sujet mystérieux, il n'est pas surprenant que la légende veuille qu'il regorge de tueurs à gage. Malgré la persistance de divers sites qui prétendent offrir ces services, l'histoire prouve que chacun de ces sites est un scam[33]. Grossièrement, il en existe de deux types : les sites de mise en relation et ceux basés sur la prédiction de la date de la mort. Ceux de la première catégorie, où l'on est censé pouvoir trouver quelqu'un qui assassinerait la personne de notre choix contre paiement, sont assez nombreux et aussi proches de l'escroquerie les uns que les autres. C'htulhu, tout comme Unfriendly Solutions, a rapidement été dénoncé[34] comme un faux[68].

L'autre catégorie de sites d'assassinats reprend l'idée développée par Jim Bell dans *Assassination Politics*. Il existait un site éponyme, nommé *Assassination Market*[69], sur lequel des médias pourtant respectés tels que *Forbes* ont publié des articles et des entretiens[70]. L'objectif de ce site suit l'idée de Bell : une cagnotte en bitcoins collecte les paris des participants sur le jour de la mort d'une personnalité qu'ils souhaiteraient voir partir. Un assassin potentiel peut également participer à la cagnotte et doit par

33 : Scam (personne le faisant : scammeur) est l'activité qui consiste à prétendre vendre des biens ou des services mais ne finalise pas la transaction ou l'utilise à des fins détournées. Par exemple, les gens qui vous disent que vous aurez accès à une *Red Room* seulement après avoir payé ou qui vous demandent d'installer des « *logiciels spéciaux* » pour s'en servir ensuite pour infecter votre ordinateur ou vous voler vos données.

34 : C'est le cas de Deku-Shrub, l'un des modérateurs du subreddit /r/deepweb et expert en sécurité. Voir par exemple http://pirate.london/2016/02/assassination-scams-the-next-generation/ En réponse, il a reçu des menaces dont une vidéo où on voit une voiture brûler en arrière-plan. Deux administrateurs de *Hidden Answers* (l'équivalent de Quora sur le darkweb) ont reçu des menaces similaires après avoir mis en doute la véracité de Besa Mafia.

ailleurs fournir l'adresse de son portefeuille bitcoin pour recevoir la récompense le cas échéant. Des sources indépendantes (médias, etc.) devraient confirmer la mort du sujet, déclenchant le paiement de la récompense. Le site a été fermé en 2014 et ne semble pas avoir rouvert depuis.

La légende urbaine selon laquelle le darkweb regorge de plates-formes de mise en relation avec des tueurs à gages a la vie dure. Mais toute escroquerie finit tôt ou tard exposée au grand jour[71]. En avril 2016, l'un des plus célèbres sites proposant des tueurs à gage, BesaMafia, a été compromis. Ses dessous (base de données, archives e-mails, etc.) ont été donnés en pâture aux darkwebonautes. Découvrons ensemble ce cas intéressant, et même assez drôle.

BesaMafia se présentait comme un service de mise à disposition de tueurs à gages opéré par la mafia albanaise[72]. Les tarifs variaient selon l'option choisie : entre 5 000 et 9 000 USD « *si vous voulez que cela ressemble à un accident* » et jusqu'à 30 000 USD, « *un tarif adapté pour les P.-D.G., les hommes d'affaires, les petites célébrités* ». Besa s'est offert de belles virées marketing sur le « web clair », notamment sur des sites prétendument spécialisés[73]. De nombreuses personnes ont dénoncé la plate-forme comme étant du scam et ont été menacées pour l'avoir fait[35]. Ce qui était intéressant avec BesaMafia, du point de vue du chercheur, est que le site avait adopté certaines caractéristiques commerciales d'un marché de drogues : s'y trouvaient entre autres des chats internes, des FAQ et des ressources autour du bitcoin[36].

35 : Si vous êtes intéressé(e), je vous recommande vivement la lecture – rafraîchissante – de cette interview : http://pirate.london/2016/05/besa-mafia-murder-for-hire-scam- exposed-following-hack/ . Cette personne se disait être l'administrateur du site web.

36 : https://skidpaste.org/xcGcx4JI.txt Il est difficile d'avoir la certitude absolue que ces fichiers sont les vraies archives de BesaMafia, mais il est aussi difficile de s'imaginer que quelqu'un les aurait créés pour nourrir un hoax aussi élaboré.

Le 23 avril 2016 donc, le site BesaMafia a été compromis et ses données publiées[37]. Ce qui en ressort ? Un scam très élaboré ayant réussi à embobiner de vraies personnes qui ont payé du vrai argent. Dans certains e-mails, l'administrateur du site échange avec des représentants de la loi leur donnant des informations sur qui a commandé quel meurtre. Le modèle d'affaires du site favorisait les commentateurs et un fonctionnement du type « réunion Tupperware ». Des candidatures étaient aussi acceptées, fait curieux pour un site qui vous dit qu'il met à disposition des tueurs endurcis de la mafia albanaise. Dans les e-mails, on trouve également des échanges spécifiant le prétendu business d'enfants[74] ; si vous voulez l'enfant pour mendier, ils peuvent vous en trouver « *des moches, issus des familles pauvres, pour 4 000 USD* ». D'après les informations divulguées, il ne semble pas que les gens derrière BesaMafia se soient rendus responsables de mise en danger ou d'atteinte de l'intégrité physique d'autrui. La saga semble continuer avec Dark Mamba, une « *société militaire privée* » comme le site se définit, proposant des tueurs à gages et opérée par l'ancien administrateur de BesaMafia…

EST-IL POSSIBLE D'ACHETER DES ARMES SUR LE DARKWEB ?

Lorsque l'on parle de tueurs à gages, il convient d'aborder rapidement la question de la vente d'armes. Si vous lisez Reddit et le sous-forum /r/deepweb[75], vous avez certainement vu passer de nombreuses questions comme « Où est-ce que je peux acheter un missile nucléaire sur le darkweb ? »[76] La réponse est : nulle part.

Comme avec les tueurs à gage, un nombre non négligeable de scammeurs opère aussi dans ce domaine. On en apprend les hauts faits de manière occasionnelle. Ainsi, alors que sont rédigées

37 : La vente d'armes létales n'est malheureusement pas limitée au darkweb. Voir l'enquête du journal allemand *Der Spiegel* qui a pu identifier le marché *AFG Security* opérant à partir de la Slovaquie et fournissant des armes factices reconverties en armes opérationnelles ; certaines auraient été retrouvées dans le cadre de divers actes terroristes en Europe, dont certains en France http://www.spiegel.de/international/europe/following-the-path-of-the-paris-terror-weapons-a-1083461.html

les dernières lignes du présent ouvrage, un individu, mécontent de s'être fait alléger de quelques bitcoins[77] se plaint sur Reddit et demande une assistance juridique (il faut oser !) car l'arme achetée n'a pas été livrée. (Attention, on ne sait actuellement pas s'il s'agit d'un vrai cas ou d'un canular.) Il est apparu que l'individu (prétendument) escroqué est mineur… En achetant son arme sur un marché quelconque sur le darkweb, il risque d'être accusé de plusieurs infractions dont la tentative de se procurer une arme à feu, d'acheter une arme à feu en ligne en payant avec des cryptomonnaies ou encore de tenter de l'importer aux États-Unis (l'import de ce modèle d'arme en particulier y est interdit depuis 2014). On peut citer aussi d'autres personnes qui s'essaient à l'achat d'armes pour se préparer à une candidature auprès des forces de l'ordre. L'histoire ne dit cependant pas si l'approche a été couronnée de succès...

Malheureusement, de vrais (re)vendeurs d'armes existent également. Les prix sont élevés, alors des « entrepreneurs » s'engouffrent dans la brèche : il existe par exemple un vendeur allemand qui récupère des armes dysfonctionnelles ou inopérantes pour les réparer avant de les revendre[78]. Dans la plupart des cas, ces armes sont bien fonctionnelles ; il s'agit, d'après le reportage, majoritairement de petits calibres, vendus entre 1 000 et 1 500 €, et acheminés à leurs acheteurs par la Poste. Dans ce dernier cas, la personne qui vend n'est pas celle qui gère le site de vente. Des marchés dédiés existent. Il semblerait que pour la période 2013-2015, environ 40 % d'entre eux aient eu une activité de vente d'armes létales. Des marchés existent évidemment qui refusent d'accepter des vendeurs d'armes, souvent pour des raisons morales.

Des opérations de police se déroulent assez régulièrement. On peut citer *Operation Onymous*, une collaboration entre le FBI, Europol et quelques autres agences spécialisées. Ayant pris place à l'automne 2014, l'opération s'est officiellement soldée par la fermeture de centaines de sites de vente de marchandises

illégales ou illicites. Cependant, d'après des données produites par des chercheurs[79], ce succès est largement surestimé : un nombre non négligeable des sites fermés était des scams ou des copies redondantes d'un même site. Il se peut que les vrais sites laissés en place le soient pour servir d'appât. Dans d'autres opérations, les représentants de la police ou du FBI se font passer pour des clients ou parviennent à infiltrer les équipes d'administration des sites web ciblés[80]. Le cas d'Agora, un des marchés où des AK-47 et autres armes à feu étaient en vente, est intéressant : après diverses actions de police, le site a décidé d'interrompre la vente de ces objets[81]. La décision a été motivée par la difficulté et le prix (très) élevé des envois, ainsi que par le nombre important d'escrocs. Ces derniers créent en effet davantage de travail pour les administrateurs et les modérateurs d'un marché, sans que cet effort soit rémunérateur pour autant. Malgré ces obstacles, la vente d'armes létales est toujours d'actualité sur le darkweb. En acheter n'est pas aussi aisé que le veut la légende urbaine du « clic et bim ! J'ai ma Kalachnikov » ; des journalistes allemands[82] avaient pu le constater à leurs dépens lors d'une émission en direct. Ils ont perdu l'équivalent de 800 USD et l'arme n'est jamais parvenue aux journalistes[83].

« CYBERMERCENAIRES » À LOUER

Si les tueurs à gages sont un mythe, les hackers « à louer » et les données volées sont présents dans de nombreux marchés du darkweb. Comme dit plus haut, la proportion de sites proposant ces services à but commercial est faible (moins de 2 % des services répertoriés à chaque étude). Divers sites existent qui mettent en relation clients et exécutants, les plus célèbres étant TheRealDeal Market, dark0de et Trojanforge. On trouve également un grand nombre de forums de discussion, tel que Hell, dont la visée n'est pas commerciale mais où on peut sans problème contacter des utilisateurs se faisant payer pour « rendre service ».

TheRealDeal Market[84] a ouvert en avril 2015 avec une ambition dépassant celle des sites préexistants : il voulait vendre des vulnérabilités 0day[38]. Pour rappel, ces dernières sont des brèches de sécurité dont l'auteur du logiciel n'est pas informé ; ces vulnérabilités constituent donc une faiblesse tant qu'un correctif n'est pas créé[39]. On comprend aisément que ces 0days sont des outils puissants qui le restent tant qu'on n'a pas colmaté la brèche. Mais ne compter que sur la vente de 0days est risqué en termes de modèle d'affaires. Certes, il s'agit de moyens d'attaque puissants qui coûtent cher et sont plutôt rares. En effet, la faiblesse principale du 0day est due au niveau de vulnérabilité : il n'y a aucun moyen de vérifier qu'un 0day l'est vraiment… sauf en ébruitant l'affaire et donc, en poussant les créateurs du logiciel cible à produire des correctifs. Ce qui, logiquement, rend le 0day inopérant. Bien sûr, le temps nécessaire à l'application du correctif[40] peut laisser une marge de manœuvre, mais en réalité il semble que ce ne soit pas l'approche la plus simple si l'on veut entreprendre à grande échelle. La fermeture de WabiSabiLabi, un marché de 0days sur le darkweb lancé en 2007, en est une preuve.

Ainsi, outre les 0days, TheRealDeal affichait le désir de vendre du code source de logiciels malveillants et les services de « cybermercenaires ». Pour mettre du beurre dans les épinards, TheRealDeal propose à peu près tous les produits possibles et imaginables[41]. Outre des services et outils de compromission, on y

38 : En 2012, un 0day fonctionnel pour iOS (le système des téléphones iPhone) pouvait se vendre pour 250 000 USD (http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/). En 2013, le *New York Times* expliquait qu'un 0day avait été acquis par un gouvernement non nommé pour 500 000 USD (http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html).

39 : Gwern Branwen, Nicolas Christin, David Décary-Hétu, Rasmus Munksgaard Andersen, StExo, El Presidente, Anonymous, Daryl Lau, Sohhlz, Delyan Kratunov, Vince Cakic, Van Buskirk, & Whom. *Dark Net Market archives* , 2011-2015, 12 July 2015. Web. https://www.gwern.net/DNM%20archives

40 : Traduction : il faut régulièrement vérifier si des mises à jour de vos logiciels existent et, le cas échéant, les déployer.

41 : Voir l'interview avec les administrateurs : https://www.deepdotweb.com/2015/04/08/therealdeal-dark-net-market-for-code-0days-exploits/ Assez étonnamment, le site interdit la vente de services de *doxing* . Et, comme de très nombreux autres sites d'e-commerce, la pédopornographie est strictement interdite.

trouve, pêle-mêle, de l'aide pour le blanchiment d'argent, du LSD et des données de connexion volées…

L'histoire de TheRealDeal est intéressante car elle montre la dynamique de la vaste communauté darkweb. Peu après son ouverture, le site a fait partie, comme plusieurs autres[85], des cibles d'attaques DDoS plutôt compliquées à endiguer. Les attaques étaient accompagnées de demandes de rançon : soit vous payez 10 BTC et l'attaque s'arrête, soit elle continue. Les administrateurs du TheRealDeal ont décidé qu'il y avait une troisième option : prendre l'attaquant à son propre jeu. Au lieu de céder, ils ont opté pour du phishing : un faux site TheRealDeal a été créé et l'attaquant a été invité à s'y connecter pour, soi-disant, discuter rançon. Il paraît que le piège a fonctionné. L'attaquant s'est connecté, les administrateurs de TheRealDeal ont récupéré ses informations de connexion et ont commencé à essayer de s'enregistrer dans d'autres sites d'e-commerce du darkweb. Il est en effet assez facile de suspecter qu'un concurrent pourrait s'offrir les services d'un « cybermercenaire » pour nuire à plus prospère que lui. L'opération a été couronnée de succès : les informations de connexion ont fonctionné sur un petit site nommé Mr Nice Guy. Les administrateurs de TheRealDeal ont ainsi pu accéder aux échanges[86] entre l'attaquant et l'administrateur de Mr Nice Guy : ce dernier, initialement victime de l'attaquant, a proposé de payer pour que sept grands concurrents soient attaqués. Pendant leur indisponibilité, Mr Nice Guy espérait voir affluer les acheteurs esseulés… Mr Nice Guy a même proposé de faire un *exit scam*[88], une escroquerie qui consiste à disparaître dans la nature avec les dépôts bitcoin de ses clients. La concurrence façon darkweb, c'est dur !

TheRealDeal a disparu pendant quelques jours en juillet 2015, au moment même où Operation Shrouded Horizon menée par le FBI et Europol fermait Dark0de[88]. À sa réouverture, un seul des quatre administrateurs initiaux de TheRealDeal était « *libre* » (ni détenu, ni accusé d'un quelconque délit). Dark0de[89] est également

revenu peu après la fin de l'opération de police. Fondé en 2007 en tant que forum[90], il s'agit d'un des plus anciens et prestigieux forums d'échanges et de mise à disposition de logiciels et de services de compromission. Dark0de, que nous venons de mentionner, est un autre site de « cybermercenaires » d'élite. Connu comme l'un des plus prestigieux forums, le site pratique une sélection *a priori* des nouveaux utilisateurs. Une étude scientifique existe sur ce forum, les chercheurs s'étant intéressés à sa sociologie plutôt qu'aux typologies de logiciels qui circulent[91]. C'est une des seules études qui existent à ce jour traitant du sujet et disposant de vraies données (presque 500 captures d'écran d'échanges et plus de 300 applications, fournies par un ex-membre du forum[92]). Dark0de est créé comme un endroit où le ratio signal sur bruit est élevé. Il veut ainsi échapper aux bavardages sans grand intérêt de HackForum. Depuis le départ, être membre de Dark0de n'est possible que suite à une cooptation. Pour postuler, il est requis de présenter un genre de CV : décrire qui on est, ce que l'on sait faire ainsi que spécifier ses « faits d'armes ». Même après être accepté, un membre n'est qu'au premier niveau des privilèges (sur un total de trois niveaux). D'après l'étude, on peut être le pire troll, l'acceptation se passe facilement si l'on sait y faire et surtout si l'on est recommandé par quelqu'un d'influent sur le forum. De nombreux créateurs de célèbres malwares et autres logiciels vérolés étaient sur Dark0de et ont depuis été arrêtés et jugés ; certains purgent des peines de prison (y compris en Sibérie).

Les données, même si elles couvrent la période 2009-2013, illustrent également l'éclectisme et la structure du modèle d'affaires de Dark0de. On y apprend que le marché n'était pas terrible : il existe un vendeur de services et produits pour deux acheteurs potentiels. Parmi les produits, on trouvait beaucoup de porno, mais presque pas de 0days. Les prix des données récupérées (identifiants pour sites web de rencontres ou des réseaux sociaux, numéros de cartes bancaires, etc.) sont ridicules : par exemple, 140 000 numéros de cartes bancaires vendus 2 000 USD. Comme partout ailleurs

sur les sites à visée commerciale, le sérieux du fournisseur sur Dark0de est primordial et on ne pardonne pas une approche légère du service après-vente. On parlera en de plus amples détails de ces caractéristiques commerciales plus loin dans ce chapitre.

QUI D'AUTRES SE SERT DE MES DONNÉES ?

Outre les TheRealDeal et Dark0de, des forums tels que Trojanforge et Hell mettent à disposition des données volées. La spécificité de Trojanforge est la rétroingénierie[42] de malwares. Le site est assez sélectif quant à ses utilisateurs (comme Dark0de et aussi très probablement pour des raisons de sécurité) et n'accepte de nouveaux venus que s'ils sont cooptés. Hell est, quant à lui, connu comme le site où les données de connexion de 4 millions d'utilisateurs du site de rencontres Adult Friend Finder ont été publiées. Avant de s'appeler Hell, le forum se nommait Olympus Hacking Forum ; malgré le changement de nom, la politique est restée la même : la pédopornographie, les drogues et la violence sont bannies. Outre les données d'Adult Friend Finder, Hell a également attiré l'attention des médias suite à la publication de milliers de documents initialement présentés comme provenant de la compromission d'une autre administration publique américaine. Il s'agissait en réalité de données en provenance d'une autre administration publique américaine[93].

La publication des données d'Adult Friend Finder est un cas d'école illustrant la très mauvaise gestion de l'affaire par l'entreprise, mauvaise gestion que nous avons vue répétée dans le cas Yahoo! par exemple. Ainsi, Adult Friend Finder n'a informé ses utilisateurs de la publication de leurs données sur Hell que presque trois mois plus tard[94]. Entre-temps, une experte en sécurité informatique avait déjà levé le lièvre, sans toutefois nommer

42 : Étude technologique consistant à étudier un objet ou un produit informatique existant, afin d'en déterminer le fonctionnement interne et/ou la méthode de fabrication. En pratique, il s'agit de reconstituer le code source et les algorithmes d'un logiciel malveillant à partir d'une application vérolée.

publiquement le site de rencontres[95]. Les données publiées permettaient d'identifier des gens et de relier leurs identités personnelles et professionnelles à leurs préférences sexuelles : le quinqua blondinet avec de l'embonpoint qui aime à se trouver des partenaires libertines en dehors de son mariage, le community manager proche de la retraite dont les comptes sur sites pour adultes sont également liés aux comptes qu'il gère pour ses clients, etc. On imagine aisément les dégâts qu'un tel manque de communication aurait pu produire…

Diverses entreprises existent depuis quelques années proposant une veille du darkweb pour y détecter la publication de données volées ou personnelles. Dans cette veine, il est intéressant d'observer les réactions étonnées à la déclaration du directeur de la sécurité des SI de Facebook lors du Web Summit 2016 : Facebook rachète des données de connexion disponibles à la vente dans les marchés du darkweb[96]. Il s'agirait en réalité d'une pratique datant de 2013[97]. Ainsi, Facebook rachète toutes sortes de données de connexion compromises pour pouvoir identifier lesquels de ses utilisateurs utilisent des mots de passe faibles. Ces utilisateurs sont par la suite invités à changer leurs mots de passe avec quelque chose de plus complexe et d'unique (ne pas réutiliser le même mot de passe ailleurs). Comment Facebook fait-il cela ? Les listes de paires identifiant/mot de passe sont vendues en clair (non chiffrés). Une fois récupérés, les mots de passe compromis sont transformés par une fonction de hachage que Facebook utilise pour sauvegarder les mots de passe de ses utilisateurs. Le service n'a pas accès à votre mot de passe en clair, mais à une version transformée ; seule cette dernière est stockée. Ainsi, chaque mot de passe racheté sur le darkweb est transformé par la même technique, avant d'être comparé aux mots de passe transformés stockés par Facebook. Si des correspondances apparaissent, cela signifie que les mots de passe de départ sont identiques. Facebook envoie donc un e-mail à l'utilisateur pour l'inviter à changer son mot de passe. Ce genre de vérifications arrive surtout lorsqu'une fuite de données utilisateurs défraie la chronique (et il y en a tout le temps…).

Ce type de pratique ne fait pas l'unanimité parmi les professionnels. Selon certains, c'est une excellente idée : il s'agit, disent-ils en somme, d'assurer une protection supplémentaire à ses utilisateurs[98]. D'après les dires du directeur de la sécurité des SI de Facebook, c'est le cas et, grâce à cette approche, des millions d'utilisateurs ont pu mieux protéger leurs comptes sur le réseau social. D'aucuns ont dénoncé le manque d'éthique de la part de Facebook et consorts achetant des données compromises sur le darkweb[99]. En effet, cela revient à encourager les pratiques de compromission : puisque quelqu'un me les achète, alors j'ai intérêt à en trouver davantage. De plus, rien ne s'oppose à la revente de ces données à d'autres acteurs par le même vendeur. Ce qui est probablement le plus dérangeant, c'est de ne pas savoir ce que Facebook fait des données accompagnant les informations de connexion. Prenons le cas Adult Friend Finder abordé plus haut : outre les identifiants et mots de passe, il y a également les préférences sexuelles des gens concernés…

L'EXCEPTION FRANÇAISE

Avant de nous intéresser plus précisément à la partie e-commerce sur le darkweb, regardons de plus près ce qu'il en est des marchés francophones. On se doute bien qu'ils existent, tout comme existent des marchés russophones, en mandarin simplifié et germanophones. L'exception française persiste même dans le darkweb.

Dans un court article datant de septembre 2016[100], la société de sécurité TrendMicro s'est intéressée à la francophonie sur le darkweb. Contrairement aux marchés nord-américains et australiens, lesquels opèrent de manière très ouverte et sont ainsi accessibles à toutes sortes d'acteurs, les marchés en langue française sont très fermés. Ils sont aux antipodes de leurs collègues anglo-saxons : la création de compte utilisateur est soumise à de nombreuses conditions et étapes sanctionnées par un bout de carte blanche, les opérateurs des services étant aussi très précautionneux. Le marché est petit (les estimations fournies par TrendMicro

parlent d'environ 40 000 personnes impliquées) et se caractérise par la création d'outils *ex nihilo* et sur mesure. Cette dernière caractéristique les différencie notablement des marchés en d'autres langues, souvent également plus grands. Les marchés francophones proposent à la vente des produits spécifiques : des armes mais pas n'importe lesquelles, des kits de suicide/euthanasie[43], des clés maîtresses de la Poste pouvant ouvrir n'importe quelle boîte ainsi que des points de permis et des *ransomwares* « faits maison »[44].

Ces particularismes tiennent pour une grande partie à la législation française. En France, le port d'armes est interdit. Cela ne signifie pas pour autant que des gens n'en possèdent pas. Ainsi, sur les marchés francophones on trouve de petites armes, par exemple des pistolets de la taille et à l'apparence d'un stylo. Ce sont le plus souvent des armes de calibre 22 coûtant dans les 150 €. Si vous voulez quelque chose de plus anodin, disons un couteau qui ressemble à une carte bancaire, c'est seulement 10 €. Bien sûr, et malheureusement, on trouve également des armes plus classiques.

Quant aux *ransomwares* identifiés sur les marchés francophones, leurs particularités réside dans le fait qu'ils sont conçus « sur mesure » pour un public parlant français (avec des fôtes et des Majuscules élisant Domicile à des endroits Curieux au sein d'une phrase, mais passons…). Les rançons varient entre 100 et 300 € payables en bitcoins ou – exception française oblige – en cartes PCS que l'on peut trouver dans le tabac le plus proche… Même si la majorité des logiciels malveillants utilisés sont acquis sur les marchés anglo-saxons, il est toujours possible de se

43 : La pratique semble en fait plutôt exceptionnelle : l'article de TrendMicro précise que des détails la concernant sont assez rares et tournent autour de plus ou moins les mêmes individus. Dans au moins l'un des cas, la demande concernait l'achat d'un tel kit pour « suicider » quelqu'un, soit un signal assez clair que l'acheteur souhaite commettre un meurtre.

44 : Rappelons ici que le *ramsomware* (aussi appelé rançongiciel en français) est un logiciel malveillant qui bloque l'accès aux fichiers contenus sur votre ordinateur et demande une rançon pour vous laisser y accéder du nouveau. Certains ransomwares provoquent l'arrêt complet de l'ordinateur et l'impossibilité de le rallumer tant que la rançon n'est pas payée. La hauteur de celle-ci peut varier (voir chapitre 01).

procurer des logiciels développés par des Français tels que le RAT DarkComet[101] dont le développement a été arrêté en 2012[45].

D'autres biens et services sont également en vente : apparemment, on propose un moyen de ne pas perdre de points de permis. Ainsi des vendeurs mettent-ils à disposition de numéros de permis à utiliser si vous recevez une amende. On peut dire aussi que d'aucuns semblent inspirés pour offrir un moyen de collecte de fonds (*crowdfunding*) qui pourraient, par exemple, servir à financer la recherche sur le cancer. Le *French Dark Net*, un réseau de forum et de marchés qui proposait également des paris autour de l'Euro 2016 de foot[46], a commencé à proposer du crowdfunding pour des causes caritatives en août 2016. On n'arrête pas le progrès !

Dans les pages précédentes, nous avons passé en revue ce que l'on trouve et ce que l'on ne trouve pas sur le darkweb. Alors qu'une bonne partie des services existants recouvre des usages plutôt classiques, nous constatons que ce qui attire surtout l'attention, c'est l'activité commerciale. Mais dans quelle mesure est-elle le centre du darkweb ?[47]

45 : Un RAT (ou Remote Access Tool, soit un outil d'administration à distance) est un logiciel permettant la prise de contrôle à distance d'une machine et ne doit pas être confondu avec un virus. Le RAT a des utilisations légitimes (gestion à distance d'un serveur, dépannage à distance) mais peut également être détourné à des fins malveillantes. La raison de l'arrêt du développement du RAT DarkComet est une crise morale survenue après l'identification du logiciel dans ce qui s'est révélé être une attaque par le régime syrien contre certains de ses citoyens https://www.undernews.fr/reseau-securite/darkcomet-lauteur-annonce-la-fin-definitive-du-developpement-du-rat.html

46 : Cette pratique n'a pas été préalablement validée par l'ARJEL (Autorité de Régulation des Jeux En Ligne), l'administration publique française qui régule les jeux en ligne.

47 : Précisons que la notion de produits licites/illicites est difficile à pleinement inclure ici. D'une part parce que l'auteure n'est pas juriste, et encore moins juge, pour définir si un produit ou un service enfreint la loi en vigueur. D'autre part, parce qu'il est très complexe de définir la légalité d'une marchandise et qui plus est, à travers différentes juridictions. Ainsi, dans tout ce bric-à-brac où l'on vend tant de choses, qu'est-ce qui rend ces objets et services illicites ? Divers paramètres doivent être considérés : la nature du produit, la juridiction de son vendeur et celle de son acheteur, etc. Une marchandise peut être légale là où est situé son vendeur, mais pas chez l'acheteur. Le cas des armes est assez explicite. Mais encore : si vous vendez des cartes Pokémon ou des albums Panini collector dans votre boutique, vous ne faites rien d'illégal : la marchandise est légale. Mais déclarez-vous vos gains aux institutions pertinentes pour autant ? Si non, vous commettez très probablement une violation.

L'E-COMMERCE FAÇON DARKWEB

On n'y trouvera guère les designs clinquants des sites e-commerce traditionnels du web clair. À la place, on verra des sites de places de marché assez spartiates, avec une structure et des fonctionnalités très semblables : une barre latérale permet de naviguer au sein des diverses catégories de produits ; une fois que l'on a choisi une catégorie, on peut filtrer par type de produit ou par vendeur. Les différences entre sites viennent donc des vendeurs et leurs offres. Si vous êtes sur un site qui vous permet de créer un compte, le processus est le même que partout ailleurs : un identifiant et un mot de passe sont nécessaires ; parfois, un CAPTCHA est également présent et dans certains cas, un code PIN supplémentaire peut être fourni pour confirmer l'inscription. Dans les cas où vous devez être introduit, l'inscription se passe *via* un lien référent.

Une fois l'inscription faite, il faut y connecter un portefeuille bitcoin[48]. Puisque les transactions par bitcoin sont pseudo-anonymes (on y reviendra), il sera possible de remonter jusqu'à vous. Pour s'en prémunir, des « mixeurs » (appelés *tumblers* en anglais) existent. Il s'agit de l'équivalent des transactions bancaires passant par plusieurs comptes écrans : le « mixeur » permet de faire une sorte de cagnotte où plusieurs personnes vont mettre des bitcoins. Ainsi, lorsque le paiement est fait, pour des champignons hallucinogènes par exemple, il émane du compte « mixeur » et non pas du portefeuille bitcoin de l'acheteur. Les frais d'un tel service sont très bas (entre 1 et 3 %) et permettent d'améliorer notablement l'anonymat des transactions. Il y a eu des propositions[101] visant à criminaliser l'usage de ces « mixeurs », leur fonctionnement étant

48: D'après un rapport d'Europol, environ 40 % de tous les paiement définis comme « cybercriminels » sont faits en bitcoin (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015) ; les données ne se concentrent pas seulement sur les marchés du darkweb. Comme nous l'avons dit ailleurs dans ces pages, l'utilisation de bitcoin rencontre de plus en plus d'activités légales. Enfin, d'autres cryptomonnaies telles que Monero font leur entrée sur les marchés du darkweb (le plus grand, Alphabay, a par exemple comptabilisé 2 % des transactions en décembre 2016 en Monero : https://bitcoinmagazine.com/articles/alphabay-comments-on-bitcoin-congestion-monero-adoption-and-zcash-possibilities-1482345512/).

considéré comme facilitateur pour le blanchiment d'argent et le terrorisme. Ces propositions n'ont pas abouti, notamment parce que la contribution des « mixeurs » au financement du terrorisme a été considérée comme « *relativement limitée* »[102]. De nouvelles voix s'élèvent cependant, appelant à introduire des règles plus strictes quant aux opérateurs et créateurs de « mixeurs »[103]. L'utilisation d'un « mixeur » est considérée comme une manière d'identifier les scammeurs (voir p. 280). Il est clair qu'acheter des produits sur le darkweb est nettement plus risqué que sur un site d'e-commerce classique. Et si vous voulez acheter des marchandises ou des services potentiellement illégaux (armes, drogues, etc.), il est un peu délicat d'aller se plaindre d'avoir été victime d'escroquerie. Ainsi, si vous voyez des annonces de ventes directes, c'est-à-dire sans passer par des « mixeurs », c'est qu'il s'agit très probablement d'un scam.

En général, les sites plutôt dignes de confiance se distinguent par la présence d'un compte dit *escrow*. Autrement dit, c'est une sorte de mise sous séquestre temporaire des fonds, le temps de s'assurer que l'acheteur a bien reçu son achat. L'*escrow* est habituellement géré par trois personnes : le vendeur, l'acheteur et une tierce personne, un modérateur par exemple, qui peut prendre un petit pourcentage du total[49] comme rémunération pour le temps et l'attention portée à la transaction. Normalement, deux des trois personnes suffisent pour débloquer la transaction ; parfois, l'autorisation des trois est requise. Encore une fois donc, donner la possibilité aux visiteurs d'utiliser ce genre de système est signe de sérieux. Des cas d'*exit scam* arrivent où des gens disparaissent avec la cagnotte, mais ceux-là sont très vite décriés et discrédités.

Ceci nous ramène au plus important : la réputation. Il existe de plus en plus de sites spécialisés présentant des statistiques sur les divers marchés. Vous pouvez y voir en temps réel si un site est en ligne et quelle est son appréciation globale. Par ailleurs, divers forums, aussi bien sur le web clair que sur le darkweb, contiennent

49 : Les frais sont de 0,2 à 2%, parfois des gourmands vont jusqu'à 5 % ; de grosses transactions peuvent demander davantage.

des tonnes d'avis clients. Chaque vendeur ainsi que l'équipe de chaque place de marché veillent à la satisfaction client, beaucoup plus que sur beaucoup de sites d'e-commerce traditionnels. La compétition est virulente, comme vous l'avez lu plus haut, et il y a de nombreux escrocs. L'idée fondamentale est : si vous voulez vraiment faire de l'argent de façon honnête, vous avez intérêt à être impeccable. Certes, les délais de livraison peuvent être plus longs, mais les gens en sont conscients. Si vous n'êtes pas content-e, il est inutile de vociférer, comme on le voit souvent sur les réseaux sociaux, en espérant qu'on vous remboursera ou qu'on vous enverra un nouveau produit gratuitement. Vous pouvez le faire, mais le résultat ne sera pas concluant et, le plus souvent, on vous répondra que c'est votre faute, notamment lorsque le vendeur est bien noté. D'ailleurs, de nombreux marchés et sites accessoires publient des guides destinés aux inexpérimentés et aux nouveaux venus (qu'ils soient vendeurs ou clients potentiels).

Nous avons vu que la concurrence est rude dans le darkweb. Votre e-commerce peut être attaqué par des « cybermercenaires » payés par un concurrent. Un concurrent peut décider de casser les prix. Un autre peut avoir un meilleur *branding*, une meilleure communication de marque, ou proposer des fonctionnalités que vous n'avez pas ou un meilleur support, etc. Si ce sont des règles du jeu relativement communes, il faut voir que la taille de la base de prospects et de clients est beaucoup plus réduite et que les techniques habituelles du marketing sont inopérantes. Disons qu'il n'est pas possible de mettre un Google Analytics pour voir quels référents vous amènent des clients ou pour vous aider à établir les célèbres tunnels de conversion[50]. Il arrive

50 : Pour rappel, Google Analytics est l'un des outils préférés du marketing : il s'agit d'un bout de code en javascript, associé à un identifiant unique, qui vous fournit des informations sur les visiteurs de votre site web et leurs comportements. Il en est de même avec le service AdSense (concerne l'interaction de vos visiteurs avec les pubs que vous affichez sur votre site web). Si on voulait vraiment chipoter, des centaines de sites existent dont l'occupation principale est les paris en ligne ; ces sites ont des connexions darkweb ←-→ web clair qui, comme c'est l'habitude de Google Analytics, sont très bavardes. En y regardant de plus près, une bonne centaine de ces sites côté darkweb ont le même opérateur (et souvent, propriétaire). Pour plus d'informations sur la notion de marketing de tunnel (encore appelé « entonnoir ») de conversion, consulter : http://glossaire.infowebmaster.fr/tunnel-de-conversion .

assez fréquemment que des sites de *phishing* soient aussi là pour escroquer les nouveaux venus. Divers sites spécialisés tiennent donc à jour des listes indiquant les sites faisant du *phishing*. Certains sites d'informations proposent carrément des outils pour vérifier que l'.onion sur lequel on s'apprête à passer commande n'est pas un site d'hameçonnage.

UN ÉCOSYSTÈME DYNAMIQUE ET COMPLEXE

On le voit bien, les marchés du darkweb forment un écosystème très dynamique et assez unique en termes de structure et de modes de fonctionnement. Aussi surprenant que cela puisse paraître, le risque (très) élevé associé à l'e-commerce du darkweb n'est pas un obstacle à sa prospérité. On le voit clairement : vous ne pouvez vous en prendre qu'à vous-même si vous vous faites avoir, cela signifie que vous n'avez pas bien étudié le vendeur ; les forces de l'ordre nationales ou étrangères peuvent s'être infiltrées ; le marché peut être fermé ou compromis n'importe quand, la police ou l'attaquant emportant les bitcoins contenus dans les *escrows* ; il est difficile de trouver une autorité centrale auprès de laquelle se plaindre si on n'est pas content(e). Une relation de confiance du même type que celle que l'on entretient avec son boulanger n'est pas tout à fait possible sur le darkweb puisque votre vendeur préféré peut disparaître du jour au lendemain. Et malgré tout, ces marchés prospèrent.

Nous parlerons de Silk Road en détail plus bas, mais prenons son exemple pour illustrer le propos. Peu avant sa fermeture, au sommet de sa gloire, le site comptait près de 4000 vendeurs et plus de 150000 clients. On parle d'une situation où les parties sont toutes anonymes et où le commerce concerne en bonne partie des substances illégales souvent envoyées d'un pays à un autre. Cependant, la confiance en Silk Road était énorme : Atlantis, un marché concurrent, n'a pas réussi à le détrôner malgré une campagne publicitaire agressive (rien à voir avec les pubs à la

télé !). Silk Road avait tout pour lui : une base clients, un forum très animé, des systèmes de messagerie interne et des *escrows* de qualité. Si on y regarde de plus près et que l'on suit les palanquées de discussions Reddit, forums, blogs, sites dédiés, etc., on se rend rapidement compte que chaque scammeur est dénoncé rapidement. Il en est de même pour la sécurité de chaque place de marché : il y a une discussion permanente des caractéristiques perçues et réelles, avec sa dose habituelle de trolling et blagues pourries. Il y a des gestes commerciaux forts lorsqu'un gros problème survient ; ainsi, par exemple, l'administrateur de Silk Road 2 avait réagi à une compromission du site datant de février 2014 en promettant de rembourser les vendeurs lésés. Excellente réputation et sécurité éprouvée sont les meilleurs indicateurs de confiance dans un écosystème où l'anonymat est la règle et la prise de risque élevée.

Enfin, point significatif : il existe une ligne rouge très claire respectée par une majorité de personnes. Sur de nombreux marchés, la présence ou la mise en vente de contenus pédopornographiques sont explicitement interdites, voire bannies. Les ressources qui collectent les liens en .onion (telles que le Hidden Wiki) ne sont pas non plus très friandes de ces contenus. Nous l'avons déjà dit, on ne « tombe » pas sur de la pédopornographie au détour d'un clic...

L'EXCEPTION FRANÇAISE, BIS

Comme nous l'avons vu plus haut, les vendeurs francophones se distinguent par des offres originales et une taille relativement modeste de la communauté. Leur manière de faire des affaires a également quelques spécificités[105].Les gens sont très paranos, davantage que sur les marchés anglo-saxons. La peur d'une infiltration par la police est également très forte. Ainsi, si le chiffrement des communications internes à un site est fortement recommandé partout ailleurs, tout le monde ne s'en sert pas ; en revanche, les francophones y sont très attachés. Par ailleurs, l'inscription se fait le plus souvent seulement par cooptation. Un membre du site

spécialisé DarkMarkets.co[106] a récemment tenté de s'inscrire… peine perdue ! La personne se plaint de ne pas pouvoir librement créer un compte sur l'une des places de marché françaises : il faut déjà avoir un compte sur un forum précis ; mais sans cooptation, pas d'inscription sur le forum en question.De plus, ce n'est pas parce que vous avez réussi que vous devenez tout de suite un membre actif avec des privilèges. Des systèmes de réputations et de « karma » existent pour établir le niveau de confiance en chaque membre. Il vous faut donc un « score réputationnel » minimum pour devenir « membre actif » par exemple. Suivant ce « score », vous pourrez ensuite être admis en tant que « membre de confiance », « modérateur » ou « administrateur ». Pour résumer, plus votre « score réputationnel » est élevé, moins on vous considère comme un policier sous couverture. Ce système rappelle celui du forum de « cybermercenaires » d'élite Dark0de dont nous avons brièvement parlé précédemment (voir page 285).

Des marchés et autres sites peuvent apparaître et disparaître pour réapparaître de manière aléatoire, et la réputation est essentielle. On voit des « cabales » se monter pour dénigrer une personne si l'on estime qu'elle a fait preuve de malhonnêteté[107]. Ainsi, un administrateur peut se lancer, sur le forum de son site e-commerce, dans le lynchage carabiné à l'encontre d'un concurrent ou même créer des opérations pour voler les sommes tenues dans les *escrows* du concurrent. Pour les nouveaux venus, il est ainsi difficile de naviguer. Une autre spécificité française est l'existence d'autoshops. Nous l'avons vu, chez les Anglo-Saxons, les vendeurs sont listés sur le(s) place(s) de marché de leur choix. Du côté francophone, un forum peut avoir une place de marché associée mais un vendeur peut également opter pour un site e-commerce personnel (autoshop).

Finalement, les autoshops sont privilégiés, et le vendeur peut utiliser les forums pour en faire la pub. Les transactions sont donc directes, sans la possibilité de recourir à un administrateur de place de marché, ce qui augmente les opportunités d'escroquerie.

Par conséquent, pour s'assurer de la bonne gestion de l'argent, les *escrows* sont de rigueur, tout comme chez les Anglo-Saxons. Les frais sont plus élevés (5 à 7 %) et très souvent, la somme totale que l'on peut y consigner est limitée. Vu la fréquence des transactions, on peut facilement arriver à la limite dont on vient de parler ; dans un cas pareil, il faut attendre que les opérations précédentes libèrent la place. Vous imaginez bien que peu de gens ont cette patience. Chez les Français, il y a donc une autre spécificité : les *escrows* semi-automatiques hébergés par de tierces parties et permettant de poursuivre les transactions sans délais. Enfin, le recours aux autoshops a suscité la création de nouveaux services : les fournisseurs d'hébergement et d'infogérance. C'est logique, n'est-ce pas. Côté anglo-saxon, une quantité non négligeable d'.onion est hébergée par un fournisseur appelé Freedom Hosting II. Côté français, pour moins de 1 BTC, vous avez quelqu'un qui s'occupe de créer, déployer et maintenir votre auto-shop. Elle est pas belle la vie ?

Comme on n'arrête pas le progrès, aux côtés des annonces de vente de logiciels vérolés et de la marijuana, on peut tomber sur… une annonce de recrutement de rédacteur de fiches e-commerce[108]. Ce n'est pas commun. Ainsi, Liberty-Markket recherche « *un membre H/F, avec une bonne orthographe et maitrisant l'art de la mis en page* » (la citation est reproduite sans correction). Au-delà du côté anecdotique et quelque peu drolatique d'une telle fiche de poste, celle-ci révèle une évolution vers une professionnalisation du milieu.

SUR LA ROUTE DE LA SOIE

Silk Road était la place de marché la plus célèbre du darkweb[51]. À l'été 2011, une publicité se propage sur les forums du darkweb :

51 : Encore une fois, on ne parle que du darkweb propulsé par les services cachés Tor. Par ailleurs, on n'aborde pas sur ces pages les écosystèmes russes et chinois non plus. Nous avons également omis de parler de *carding*, soit la fraude à la carte bancaire : il s'agit d'un pan entier de délits avec leurs spécificités, sujet certes intéressant, mais susceptible de grandement diluer notre thématique principale.

un marché où on peut trouver de tout, aussi bien de la cocaïne que des livres, des bijoux faits main, des cigarettes, des œuvres d'art d'artistes indépendants, des vêtements, etc. Les drogues étant plus vendeuses que les bouquins, ces derniers n'ont jamais fait les gros titres. Pourtant, des interdictions très claires existent alors à propos de ce qu'on peut vendre ou pas. Ainsi, sont prohibés des produits et services pouvant blesser quelqu'un (armes), des annonces de tueurs à gages, de la pédopornographie. L'interdiction va même plus loin et inclut tout produit ou objet dont la création a impliqué la remise en cause de l'intégrité physique d'un autre humain. Silk Road est, jusqu'à aujourd'hui, la seule occurrence pour ce type de commerce : une communauté et une popularité hors pair, un positionnement politique clair, assumé et provocateur, un succès commercial inattendu :

« L'État fait son possible pour contrôler chaque aspect de notre vie. Ainsi, Silk Road est un endroit où il est possible de vivre sa vie comme chacun l'entend. »

Le site lui-même n'est pas « géré » par un administrateur (malgré le pseudonyme « SR Admin » d'un des utilisateurs), mais de manière collégiale. Après un an d'existence fructueuse, l'administrateur du site annonce un changement : son identité se sépare en deux. D'une part, l'individu, avec son pseudonyme habituel, de l'autre, le gestionnaire de Silk Road représentant l'identité communautaire et collégiale de l'administration. Ce dernier est la véritable légende de Silk Road et, pour ainsi dire, sa valeur ajoutée. Ainsi, à partir du 5 février 2012, l'administrateur du site s'appelle Dread Pirate Roberts, communément appelé DPR. La référence du nom est significative : DPR est une figure du livre *The Princess Bride*. Il s'agit d'un hors-la-loi à la Robin des Bois, un gentil qui aide les faibles et protège les vulnérables. La spécificité du caractère romanesque de Dread Pirate Roberts est dans son identité : il est anonyme, certes, mais surtout « il » n'est pas un seul homme. Il s'agit d'une identité multiple, fluide, personnifiée par une série d'individus qui en endossent le costume, la réputation

et la responsabilité afférente. Il s'agit donc d'un archétype original de l'idée qui ne peut être arrêtée car elle ne dépend pas d'une personne donnée pour survivre. Le positionnement politique de Silk Road, avec le personnage de DPR comme administrateur, définit donc le site non seulement comme une place de marché mais aussi comme un mouvement politique à part entière. Ainsi, le but de DPR est de voir de nouvelles interactions se créer entre les individus :

"I'd like to take a moment to share with you what the Silk Road is and how you can make the most of your time here. Let's start with the name. The original Silk Road was an old-world trade network that connected Asia, Africa and Europe. It played a huge role in connecting the economies and cultures of these continents and promoted peace and prosperity through trade agreements. It is my hope that this modern Silk Road can do the same thing, by providing a framework for trading partners to come together for mutual gain in a safe and secure way."

« Je souhaite prendre quelques minutes pour partager avec vous ce qu'est Silk Road et comment vous pouvez en tirer le meilleur bénéfice. Commençons par le nom. La Route de la Soie est un ancien réseau commercial connectant l'Asie, l'Afrique et l'Europe. Il a joué un rôle significatif en mettant en relation les économies de ces continents et en promouvant la paix et la prospérité *via* des accords de commerce. J'espère que cette Route de la Soie moderne peut en faire de même, en créant un cadre permettant à des partenaires commerciaux de se rencontrer pour leur bénéfice mutuel et de manière sûre et sécurisée. »
(NDLR : il s'agit du message d'accueil que l'utilisateur nouvellement inscrit recevait.)

La « War on Drugs », la « guerre contre les drogues » américaine, est souvent dénoncée comme un cas de violation de droits fondamentaux[109] et comme étant encore plus violente que la guerre contre le terrorisme. Silk Road se veut un endroit où tout commerce peut avoir lieu. Partant du postulat que l'on n'empêchera pas

les trafics tant qu'il y aura de la demande, autant que les échanges soient les plus pacifiques possible. L'existence de Silk Road n'est donc pas qu'un marché de drogues :

"*What we're doing isn't about scoring drugs or sticking it to the man, it's about standing up for our rights as human beings and refusing to submit when we've done no wrong. Silk Road is a vehicle for that message. All else is secondary.*"

« Ce que nous faisons n'est pas décider quelle est la meilleure drogue ou la fournir aux gens de gré ou de force. Il s'agit de défendre nos droits d'êtres humains et de refuser de nous soumettre quand nous n'avons rien fait de mal. Silk Road est un véhicule pour ce message. Tout le reste est secondaire. »
(NDLR : Extrait d'échanges sur le forum de Silk Road.)

On touche là à l'idéologie anarchiste. Les fondamentaux des Cypherpunks sont également pleinement revendiqués et implémentés à travers DPR et Silk Road :

"To grow into a force to be reckoned with that can challenge the powers that be and at last give people the option to choose freedom over tyranny."

« Pour devenir une force reconnue qui peut défier les puissances qui sont et enfin donner aux gens la possibilité de choisir la liberté plutôt que la tyrannie. »
(NDLR : Extrait d'échanges sur le forum de Silk Road.)

Le site continue à prospérer. DPR prend entre 8 et 15 % des transactions s'effectuant sur Silk Road. Les estimations veulent qu'en deux ans et demi d'existence, le site ait facilité 1,2 million de transactions valant au total 9,5 millions BTC. L'attention politique attire alors l'attention médiatique – et le FBI. Les recherches commencent et un jour, un post datant de 2011 écrit par un utilisateur surnommé *altoid* est retrouvé sur un forum[110] ; il demande si quelqu'un connaît Silk Road et des commentaires sur la

qualité de ce qui s'y vend. En octobre 2011, un autre post du même « altoid », sur un autre forum, raconte une histoire différente : la personne cherche un spécialiste technique du bitcoin donnant son e-mail de contact, *rossulbricht at gmail dot com*. Google fournit des informations confirmant que l'adresse e-mail est enregistrée au nom d'une personne nommée Ross Ulbricht et en fournissant la photo de profil de la personne. Parmi les vidéos YouTube associées à l'utilisateur[111], nombreuses sont celles qui montrent des contenus en lien avec l'école économique autrichienne, sujet cher à Dread Pirate Roberts. Plus tard, un article anonyme publié[112] dans le journal indépendant *Austin Cut*, édité dans la ville natale d'Ulbricht, présente le montage de Silk Road comme une simulation économique d'une alternative à la lutte contre les drogues et contre la « War on Drugs » à la fois. Enfin, une question sur le forum d'entraide StackOverflow montre qu'Ulbricht a des difficultés techniques avec les services cachés de Tor[113]. Rien de concret donc mais un faisceau de minces indices. À partir de ce moment-là, les choses deviennent beaucoup moins claires. Lors d'une prétendue fouille de routine à la frontière entre Canada et États-Unis, les autorités saisissent neuf cartes d'identité portant toutes une photo de Ross Ulbricht mais affichant un nom différent. L'adresse d'expédition est celle d'Ulbricht à San Francisco. Quant à savoir comment, peu après, le FBI a mis la main sur les serveurs situés dans différents pays et hébergeant les services de Silk Road[52], c'est encore moins clair. Personne, du côté de Silk Road, n'était au courant que le FBI étudiait les données récupérées à partir de ces machines et y trouvait des correspondances pour certains des indices mentionnés plus hauts. Parmi les informations retrouvées sur ces serveurs, certaines concernaient des messages indiquant que DPR aurait commandité un assassinat.

52 : D'après certains chercheurs, le FBI aurait introduit des logiciels espions permettant de remonter à l'adresse IP réelle du site et ainsi, de localiser les emplacements des serveurs https://www.nikcub.com/posts/analyzing-fbi-explanation-silk-road/

Un jour de 2013, les gens se réveillent en constatant que Silk Road est fermé. En octobre, un procès-verbal[114] est publié accusant un jeune homme du nom de Ross Ulbricht d'être le fondateur et l'administrateur principal du site. Les gens sont choqués, non seulement à cause de l'identification publique de la personne, mais aussi en raison d'une mention de tentative d'assassinat. Ulbricht est le garçon d'une famille de classe moyenne, diplômé d'un master scientifique, belle gueule. L'idée de DPR, l'anarchiste passionné qui interdit tout produit issu de violences sur autrui sur la place de marché Silk Road, commanditant un assassinat est vraiment bizarre ; pour beaucoup de gens, les profils ne correspondent pas du tout.

Comme si ces rebondissements rocambolesques ne suffisaient pas, DPR aurait commandité plusieurs assassinats. Après l'identification des serveurs, le FBI infiltre Silk Road (Opération Marco Polo). L'un des administrateurs, sous le pseudonyme de *chronic-pain*, se retrouve à devoir espionner pour la police. DPR aurait payé 80 000 USD pour un premier assassinat, le prétendu tueur à gage étant en réalité un agent du FBI[115]. C'est à ce moment-là qu'un faux assassinat aurait été monté par le FBI. Dans le deuxième assassinat pour lequel DPR aurait déboursé 150 000 USD[116], le rôle du FBI est moins évident. Lors des premiers procès, Ulbricht a été accusé de pas moins de six tentatives de meurtres[117], mais ces charges ont par la suite été entièrement retirées du dossier[118]. Fait curieux, on retrouve dans cette histoire le même agent spécial du FBI que celui ayant participé à l'opération transformant Sabu de LulzSec en mouchard.

Depuis, le darkweb n'a plus jamais été le même. Les poursuites à l'encontre de Ross Ulbricht se sont transformées en une condamnation à la perpétuité[119]. Sa famille continue à le soutenir et à tenter de faire diminuer sa peine de prison ; le souvenir de la passion politique de DPR pousse même certains à qualifier la condamnation de « punition politique » et à considérer Ulbricht comme un

prisonnier politique[120]. Certains des agents du FBI ont profité de la manne et volé des centaines de milliers de dollars (sous forme de bitcoins)[121] ; il s'agit d'ailleurs de certains des agents ayant mis en scène le faux meurtre dont on a brièvement parlé plus haut. Un mois après la fermeture de Silk Road, la version 2 était en ligne, mais a été infiltrée dès le départ et fermée peu après. Le confident de DPR, un homme portant le pseudonyme de « Variety Jones », a également été appréhendé et jugé[122]. Aucun des marchés actuels n'a la même fière allure politique que le Silk Road d'origine et son Dread Pirate Roberts.

03

CACHÉ COMME UN SECRET ÉVENTÉ

Si le darkweb, c'est aussi secret et caché, comment se fait-on prendre ? Assez facilement en fait. L'erreur principale de beaucoup est d'imaginer que puisqu'ils utilisent un logiciel qui protège l'anonymat, rien ne peut leur arriver. Grossière erreur : cela revient à commettre le crime parfait, de manière récurrente, en essayant d'anticiper les tentatives de vous en empêcher d'un adversaire disposant souvent de beaucoup plus de moyens, financiers et humains, que vous (FBI, police). Et aucun logiciel ne vous protège de vos propres erreurs. En effet, comme mentionné plus haut, on ne devient pas expert en sécurité en une nuit. Analysons ensemble les diverses manières qu'il y a de compromettre des activités que l'on pense bien cachées.

ANONYMAT VS. SÉCURITÉ

Tor protège votre anonymat. Mais comment est-on anonyme ? Comment se fond-on dans la foule ? En ne se faisant pas remarquer. Dans la protection de l'anonymat, la notion d'homogénéité a donc un rôle prépondérant. Parvenir à véritablement cacher ce qu'on cache est difficile. Si, globalement, les autres se font traquer par les trackers pub, alors se fondre dans la foule veut dire se faire traquer aussi (quitte à renvoyer de fausses informations) de la même façon que si tout le monde a un téléphone mobile ou un compte Facebook, ne pas en avoir vous rend différent, donc

discernable. Cependant, faire comme tout le monde veut aussi dire commettre les mêmes erreurs liées à la sécurité. Le Graal serait donc d'être indiscernable en apparence tout en étant irréprochable d'un point de vue sécurité et en ne renvoyant que des informations fausses. Une gageure.

Admettons qu'en utilisant le navigateur Tor, on soit suffisamment anonyme pour se fondre dans une masse de quelques centaines ou quelques milliers d'individus. *Quid* de la sécurité ? « Être en sécurité » est une notion aussi extensible que générale. Comment Tor assure-t-il notre sécurité ? La réponse est : plutôt mal. L'un des problèmes est l'homogénéité. Utiliser le même navigateur que tout le monde vous uniformise et peut vous aider à ne pas vous faire remarquer ; mais si l'utilisation de ce navigateur est ponctuelle, cet évènement est remarquable et suffit à vous séparer du lot. Il en est de même si vous n'utilisez que ce navigateur. Pire encore, si l'un de ces utilisateurs homogènes est vulnérable, tous le sont parce qu'ils partagent tous les mêmes caractéristiques. Comme nous l'avons vu précédemment, un hacker (bon ou mauvais, c'est sans importance) aime à se faire des nœuds au cerveau et à trouver des approches originales. L'homogénéité en informatique, c'est comme dans la nature : le manque de diversité crée des faiblesses.

Prenons un cas concret : une alerte à la bombe à l'université américaine Harvard[53]. Le 16 décembre 2013, un e-mail anonyme signale la présence d'un engin explosif à l'université[122]. C'est fâcheux, nous sommes en pleine semaine d'examens. Moins de 24 heures après, le FBI arrête un étudiant[123] : le garçon, étudiant à Harvard, aurait aimé ne pas aller aux examens, alors il s'est dit qu'une alerte à la bombe serait une bonne façon de se débarrasser de cette corvée. Raté.

53 : On pourrait évoquer d'autres menaces, sur le sol français ; les cas de *swatting*, ou encore les canulars téléphoniques, ne manquent pas, mais en France, on n'a pas accès aux procès-verbaux. Il est donc difficile de décortiquer des faits – et fonder une réflexion sur de pures spéculations n'est pas des plus heureux.

Alors, comment s'est-il fait avoir ? Comme un bleu : il a utilisé le wifi de la bibliothèque de Harvard. Analysons le cas tout en retenant qu'il ne s'agit pas de cautionner les actions de la personne mais d'expliquer en quoi être anonyme ne signifie pas (toujours) être en sécurité.

Le but de l'étudiant (nommé Eldo Kim) était d'éviter de passer l'examen planifié le 16 décembre. Pour compromettre la tenue de l'examen, Kim décide donc de faire évacuer le bâtiment où se tient l'épreuve. Et comme il n'est pas à court de bonnes idées, il décide de s'en charger tout seul comme un grand.

Donc, ce matin du 16 décembre 2013, Kim va à la bibliothèque de Harvard, se crée un e-mail avec le service *GuerillaMail.com*, télécharge le navigateur Tor et, à 8 h 30, envoie à l'administration :

"shrapnel bombs placed in:science center
sever hall
emerson hall
thayer hall
2/4. guess correctly.
be quick for they will go off soon"

« Des bombes ont été placées dans les bâtiments suivants :
le Science center
le Sever hall
l'Emerson hall
le Thayer hall
2/4. Devinez correctement.
Ne perdez pas de temps, car elles vont bientôt exploser. »

L'étudiant ferme ensuite son ordinateur mais ne l'éteint pas, se dirige vers la salle d'examen comme si de rien n'était et attend que l'administration ferme le site pour raison de sécurité. D'après le procès-verbal[125] dressé par l'agent du FBI l'ayant appréhendé, l'étudiant a écrit « *bombe à shrapnels* » parce que « *ça sonnait plus dangereux* ». De plus, le choix du « *2/4. Devinez correctement* »

a été fait pour forcer l'administration à fermer les quatre salles ce qui allongerait le temps de fouille, donc le temps de fermeture du site, donc le temps avant le début de l'examen fatidique.

L'exécutant ne doit pas être fan des films de braquage tels qu'*Ocean's Eleven*. Il saute les étapes principales : planification, surveillance de la cible et élaboration d'un plan de sortie. La planification et la surveillance de la cible sont bâclées. L'étudiant est visiblement mal informé : aux États-Unis, la procédure standard requiert que les fouilles de plusieurs sites où une alerte à la bombe est signalée se fassent en parallèle et non pas en séquentiel. Fouiller une salle prend donc autant de temps que d'en fouiller quatre. C'est logique : risquer qu'une bombe explose juste parce qu'on n'a pas eu le temps d'arriver à la pièce piégée n'est pas une option raisonnable. Pour l'allongement des délais, c'est raté. Quant au plan de sortie, il n'existe tout simplement pas. Apparemment l'étudiant ne s'est jamais posé la question de ce qu'il se passerait s'il se retrouvait en interrogatoire avec un vrai agent du FBI, c'est-à-dire une personne dont le boulot consiste également à employer diverses techniques pour vous faire avouer des méfaits.

Mais attendez un peu, l'étudiant a quand même utilisé Tor : comment a-t-il pu se faire prendre ? Nous voici donc au cœur du problème qui fait se confronter anonymat et sécurité. L'étudiant est allé avec son ordinateur personnel à la bibliothèque universitaire. Se connecter au wifi lui a permis de télécharger le navigateur Tor et de se créer un compte e-mail sur GuerillaMail.com. Le service *GuerillaMail.com* ne cache pas l'adresse IP, d'où le besoin de l'utiliser *via* un outil qui assure l'anonymat. Tor est donc le choix idéal. Oui, mais pour se connecter au wifi de la bibliothèque, il a dû utiliser ses véritables identifiants, donc fournir de quoi s'identifier et s'authentifier. Ce réseau est lourdement supervisé par le service informatique de l'université, et les informations de connexion sont conservées pour des temps plus ou moins longs. Donc, Kim s'est connecté au wifi, puis a ouvert le navigateur Tor, action parfaitement visible et identifiable si vous

surveillez le trafic. Ainsi, lorsque, par la suite le FBI, a cherché l'origine de l'e-mail disséminant la fausse alerte à la bombe, il a été possible non seulement de savoir que quelqu'un a utilisé Tor, mais aussi de déterminer précisément qui l'a utilisé.

Comment en est-on arrivé à fouiller du côté de la bibliothèque ? Il y a une alerte à la bombe un jour de grands examens à Harvard, et on ne trouve rien. Il n'est pas nécessaire de sortir du MIT pour se douter qu'il y aura une enquête. La question principale est donc : à qui profite l'interruption ? Eh bien, à plein d'étudiants qui auraient dû se trouver en salle d'examen ce matin-là, peut-être à des pions qui se seraient réveillés trop tard et auraient été en retard ou encore à un professeur qui se serait mal préparé pour l'examen ou aurait été pris d'une soudaine crise de procrastination le poussant à ne pas vouloir corriger des copies. Les étudiants sont en général les suspects n° 1 dans ce cas. En outre, les enquêteurs ont l'e-mail à leur disposition : d'où provient-il ? L'adresse IP d'envoi n'est pas facilement traçable car l'expéditeur a utilisé un moyen d'offuscation, le plus probablement Tor. Cette supposition est confirmée lorsque l'en-tête de l'e-mail envoyé à l'administration est examiné : l'en-tête contient des traces indiquant que le navigateur utilisé est le navigateur Tor. Ce dernier « masque » votre activité en ligne, mais ne masque pas le fait que vous l'utilisez.

Une fois tous ces éléments rassemblés, vérifier dans les informations de connexion au réseau universitaire si quelqu'un s'est connecté à Tor est relativement simple : les adresses IP de l'université sont connues ainsi que les adresses IP des nœuds d'entrée de Tor. Limiter ensuite les recherches aux connexions au réseau faites par des étudiants le matin du 16 décembre a vite fait ressortir un nom : celui du coupable. Eldo Kim a été l'une des seules personnes à se connecter à Tor ce matin-là. On ne sait pas s'il a regardé du porno ou des vidéos de chats avant d'envoyer son e-mail canular (l'anonymat de sa navigation est préservé), mais on sait que ses activités convergent vers une action potentiellement délictueuse. Et comme son plan de sortie n'existe pas, il avoue tout dès le début

de l'interrogatoire. Il faut admettre que, stratégiquement parlant, l'étudiant a réussi : il n'a pas eu à passer l'examen, et il n'aura plus à en passer. Il a été condamné et exclu de l'université…

En quoi ce cas a-t-il trait à notre discussion sur homogénéité et sécurité ? Avant d'évoquer OPSEC, c'est-à-dire la création d'un modèle de menaces, l'évaluation des problèmes liés au facteur humain et leur gestion, réfléchissons à la question suivante : s'il y avait eu des centaines de personnes connectées à Tor ce matin-là (plus grande homogénéité), l'étudiant se serait-il fait prendre ? Peut-être que oui, peut-être que non, il est difficile de spéculer sur un enchaînement de « et si ». Ce qu'il faut voir ici, c'est que le dénominateur commun de beaucoup (peut-être de toutes) de ces personnes aurait été le navigateur Tor. On est en pleine homogénéité : un navigateur, toujours le même, avec des failles plus ou moins connues et des utilisateurs plus ou moins précautionneux. Utiliser Tor aurait probablement suffi à dissimuler ces agissements aux yeux de l'administration universitaire, mais se cacher d'une structure avec les capacités du FBI, c'est une autre histoire ! Ce dernier[54] ne s'arrête pas à une adresse IP non traçable ; il existe de nombreuses façons de découvrir qui est derrière une activité en faisant fi de l'adresse IP utilisée.

En outre, il ne faut pas oublier que toute activité laisse des traces : qu'il y ait deux cents étudiants ou même deux mille connectés à Tor à partir de la bibliothèque universitaire ce matin-là, combien parmi eux sauraient effacer les traces de navigation laissées sur leurs ordinateurs ? Notre étudiant a utilisé le navigateur Tor directement à partir de son ordinateur et non pas

54 : En fait, le FBI n'est pas le seul acteur de sécurité et sûreté intervenu sur ce cas : suite à la réception de l'e-mail canular, l'administration universitaire a fait appel au FBI, au Bureau of Alcohol, Tobacco, Firearms and Explosives (une administration spéciale dédiée à tout ce qui est armes et engins et substances explosives), au Secret Service (agence gouvernementale dépendante du département de la Sécurité intérieure des États-Unis), à la police du département de Cambridge, à la police de la ville de Boston et aux pompiers de Cambridge. Bref, une palanquée de gens dont le travail est d'arrêter des délinquants, qu'ils soient des petites frappes ou des membres du grand banditisme.

en utilisant la distribution Tails, qui s'exécute à partir d'une clé USB et permet l'effacement de nombreuses traces une fois la clé débranchée. Le navigateur Tor nettoie, lui aussi, ses traces[127] mais uniquement lorsque vous fermez tous les onglets ouverts et fermez le navigateur lui-même[55]. Pour ne laisser pratiquement aucune trace sur l'ordinateur personnel, il aurait fallu fermer le navigateur entre chaque action (création de compte e-mail ; envoi de l'e-mail canular ; etc.), éteindre l'ordinateur, le laisser refroidir, etc. Notre étudiant procrastinateur a donc deux graves délits à son compte : le premier étant de vouloir jouer à faire (très) peur pour son propre bénéfice personnel et l'autre est que l'exécution du canular a été faite de manière peu scrupuleuse.

Ce que ce cas montre – en dehors de toute considération morale quant à la motivation de l'étudiant –, c'est qu'un outil technique ne fait pas tout. L'anonymat, notamment celui fourni par une (plus ou moins bonne) homogénéité de l'outil, n'est efficace que dans le cas où ce que l'on souhaite protéger est le contenu d'une communication. Dans ce cas, l'anonymat est par exemple la probabilité égale qu'un message ou un contenu soit écrit par n'importe lequel d'une multitude d'auteurs. Si j'ai une cagoule au milieu d'une foule de gens non cagoulés, mon visage ne sera ni discernable ni identifiable ; je peux être à peu près n'importe qui de sexe féminin et de taille moyenne. Mais si je suis la seule personne à porter une cagoule, mon visage ne sera toujours ni discernable ni identifiable mais il y a fort à parier que je me ferai remarquer immédiatement…

Pour conclure cet exemple, on peut dire que la préparation et la planification sont indispensables si vous voulez préserver votre anonymat et votre sécurité informatique[56] : c'est l'OPSEC.

55 : On simplifie. C'est un peu plus compliqué que ça : ces traces sont liées au fonctionnement normal du système d'exploitation.

56 : Et même, elles ne peuvent rien contre quelqu'un qui vous en veut personnellement. Avec un accès à vos machines, du temps et des ressources à disposition, la probabilité que vos secrets se retrouvent divulgués est importante. En outre, les tentatives de compromission de Tor par des représentants de la police est une activité connue.

L'OPSEC, KÉZACO ?

Rappelons les bases : les services cachés cachent également l'adresse IP de leur opérateur et ne permettent pas de détecter l'endroit où il se trouve (géographiquement). Cependant, la technologie, même la plus performante, ne peut rien pour améliorer le facteur humain. Un exemple simple : si un service caché publie très largement du contenu sur une tranche horaire donnée, on peut en déduire dans quelle partie du monde se trouvent ses administrateurs.

Nous l'avons déjà vu, on n'est jamais assez prudent (ou paranoïaque, comme aiment à le dire beaucoup de spécialistes de sécurité). Le sobriquet PEBKC ou PEBKAC, abréviation de « *problem exists between keyboard and chair* » (« le problème se situe entre le clavier et la chaise ») est une image adaptée. Lorsqu'on fait de la sécurité (y compris informatique), il est primordial d'évaluer les menaces et vulnérabilités liées à une activité donnée. Dit ainsi, c'est banal : nous pratiquons une évaluation de sécurité opérationnelle dans la plupart de nos actions de manière quotidienne. Lorsque vous traversez la rue, vous vous assurez qu'aucune voiture ne risque de vous renverser ; lorsque vous faites les courses, vous jetez un œil à la date de péremption ou encore aux ingrédients pour vous assurer qu'aucun n'est un allergène potentiel pour vous. On peut continuer cette liste à l'envi.

L'approche que nous adoptons dans chacun de ces gestes est connue comme OPSEC, ou « sécurité des opérations ». Le terme étant surtout utilisé par les professionnels de sécurité et défense, reprenons leur définition : « Processus *via* lequel on refuse de divulguer de l'information critique à des adversaires potentiels. » Lorsque nous partons en vacances, nous essayons d'éviter de laisser trop de fenêtres ouvertes ou accessibles afin de ne pas faciliter les choses aux voleurs qui voudraient s'introduire chez nous. Dans le cadre de votre travail, surtout si l'on détient une information stratégique pour le développement de l'entreprise, on évitera de laisser notre ordinateur allumé, non-protégé et sans surveillance dans le train pendant que nous irons prendre un café à la voiture-bar. De même, on évitera de ramasser

une clé USB que quelqu'un semble avoir perdue pour la brancher directement sur son ordinateur voir à qui elle appartient : c'est une manière classique d'introduire des logiciels espions et de potentiellement s'arroger le contrôle de votre ordinateur à distance. L'information critique qui vous appartient est toujours investie du même pouvoir : si elle est mal protégée, elle peut permettre à un acteur malveillant de prendre l'avantage et de vous créer des ennuis. L'approche holistique conduisant à une hygiène opérationnelle qui réduit les risques est donc traduite dans notre cas par l'idiome « avoir une bonne OPSEC ».

S'agissant de gestes quotidiens, l'effort cognitif est négligeable : toutes les vérifications que l'on fait sont tellement habituelles qu'on ne se rend même pas compte qu'on les exécute. Lorsqu'il s'agit d'assurer la sécurité d'envois de drogue à des clients qui font leurs courses sur Silk Road, les exigences en matière d'OPSEC sont un peu plus poussées. Ainsi, lorsque le député Debré s'exclame, offusqué, avoir reçu ses champignons hallucinogènes dans une enveloppe tout ce qu'il y a de plus banal par la Poste, on voit que le vendeur fait preuve de bon sens : envoi qui ressemble à n'importe quel autre (donc, n'attire pas l'attention), transitant par les voies habituelles (La Poste). Cela ne veut pas pour autant dire que le vendeur a correctement et continuellement pris le soin de faire un modèle des risques.

En effet, lorsque l'on parle de faire un modèle de menaces, on pense aux cinq principes fondamentaux de l'OPSEC :

1 – identifier votre information critique ;
2 – analyser les menaces qui pèsent sur vous ;
3 – analyser vos propres vulnérabilités ;
4 – évaluer les risques ;
5 – employer des mesures de protection appropriées.

Rien que de très logique.

Avec la médiatisation du darkweb et les activités illégales qui y circulent, les forces de l'ordre interviennent plus régulièrement.

Des sources nous ont ainsi confirmé que la police française avait son portefeuille bitcoin où étaient stockés les bitcoins saisis. De nombreux criminels ont déjà été arrêtés et jugés, que ce soit pour vente de substances illégales (drogues, médicaments interdits) ou pour pédopornographie. On y apprend (presque) à chaque fois que l'OPSEC de ces gens était mauvaise. Des erreurs humaines aident la police à les appréhender. On peut s'en réjouir car, s'il est quelque peu pitoyable de se faire prendre pour fausse alerte à la bombe, il est tout à fait rassurant de savoir que les erreurs humaines permettent aussi d'appréhender de véritables criminels. Ces erreurs ne sont pas aussi caricaturales qu'une étiquette rouge « DROGUES » sur une enveloppe blanche, mais traduisent des niveaux de connaissance limités, un manque de préparation et une mauvaise « hygiène » numérique. Le petit florilège qui suit invite également à réfléchir à l'impact des (parfois trop) grandes libertés dont jouissent certains services de police et de renseignement dans leurs tentatives de démasquer des criminels, ou supposés tels, et de la possible instrumentalisation de prérogatives censées au départ outiller une lutte légitime contre la délinquance.

LES VULNÉRABILITÉS DES SERVICES CACHÉS

Lorsque vous mettez en place votre site *via* les services cachés de Tor, vous pouvez commettre des erreurs d'ordre technique, en laissant par exemple paraître les adresses IP réelles[127], ou lister plus ou moins clairement tous les sites hébergés sur le même .onion. Sarah Jamie Lewis, une chercheuse canadienne, a créé OnionScan, un outil qui explore les services cachés à la recherche de vulnérabilités. L'intérêt d'un tel service est que, comme nous l'avons déjà précisé au début de ce chapitre, seule une partie des .onion hébergent des sites dont l'activité est illégale ou illicite. Certains marchés du darkweb, étant donné les sommes en jeu et les enquêtes continues de la part de divers services de sécurité, innovent constamment en matière de sécurité[128].

Grâce à ces recherches, on sait par exemple que 25 % des services cachés[129] sont vulnérables au niveau de leurs données d'hébergement. Cela fait un quart d'environ 15 000 adresses .onion ayant été scannées, dont 11 000 ayant été actives pendant plusieurs heures… en bref : il s'agit de beaucoup de sites. La vulnérabilité fournit diverses informations quant aux sites hébergés sur un même service ; la moitié de ces services vulnérables sont hébergés par Freedom Hosting II… Avec ces informations, il est possible de creuser et parvenir à « dé-anonymiser » les sites, donc à remonter à leurs opérateurs.

Mais arrêtons-nous là, ou nous allons nous perdre dans ce labyrinthe de technicité. Le point important est de savoir que toujours plus d'outils existent qui permettent d'explorer ce paysage et d'en apprendre beaucoup sur les sites, même lorsque ceux-là se croient invulnérables. Cette observation vaut aussi bien pour les sites ayant une activité (manifestement) illégale que pour ceux dont le but est de fournir un espace d'expression à ceux qui n'en ont pas dans leurs pays. Cette discussion nous amène directement à la vulnérabilité inhérente à la confiance en des tiers.

LA CONFIANCE PAR PROCURATION

C'est probablement enfoncer des portes ouvertes que de dire qu'on ne peut pas vivre en société sans déléguer une partie de nos activités à des tiers de confiance. Et le plus souvent, ils en sont dignes. C'est lorsqu'il y a compromission que les choses peuvent mal tourner.

Avec la prolifération des utilisateurs et des utilisations, de nouveaux fournisseurs de services apparaissent : hébergement, clients de messagerie instantanée, d'e-mails, etc. Rien de révolutionnaire de ce côté : la situation est similaire à ce dont vous avez besoin pour avoir la même chose sur le « web clair ». Nous avons parlé de l'hébergement des services plus haut et des vulnérabilités identifiées

qui s'y rattachent. L'hébergeur Freedom Hosting II est un bon exemple de tiers de confiance ici. Malgré ses déboires précédents, il continue à assurer l'hébergement d'environ 20 % des sites stables du darkweb. Au début de son existence, Freedom Hosting (FH) était LE service d'hébergement. En 2011, il était déjà une cible d'Anonymous (Operation Darknet) ; les Anons ciblaient les sites de pédopornographie hébergés chez FH. Et l'opération réussit, Anonymous ayant compromis Lolita City, l'un des sites pédopornographiques les plus importants à l'époque. L'attaque a également permis de récupérer de l'information sur plus de 1 500 utilisateurs du site qu'Anonymous a rendu publique. Lors d'#OpPedoChat en 2012[130], Anonymous a continué ses efforts en réussissant à compromettre d'autres sites et à rendre publiques d'autres informations sur leurs utilisateurs. Début 2017, le successeur de FH, Freedom Hosting II, s'est vu compromis par une personne ou un groupe de personnes se revendiquant d'Anonymous. Le résultat est une coquette collection de fichiers de ~80 Go où on trouve littéralement de tout : des clés privées stockées sur les serveurs de FH2, des mails, des informations sur les services hébergés. La motivation de cette compromission est, d'après le message de l'attaquant, « *aucune tolérance pour la pédopornographie* ». Or, en explorant les services hébergés par FH2, l'attaquant s'est rendu compte que pratiquement la moitié de ceux-là constituait une forme de pédopornographie[131].

En 2013, il est découvert que le navigateur Tor a été victime d'une attaque de la part du FBI[57]. On le verra par la suite, le FBI, et les services de police plus généralement, ont recours à des opérations de compromission dont le statut légal est discutable[58].

57 : L'attaque, avec nom de code EgotisticalGiraffe, a été révélée par Snowden : https://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document Le FBI a reconnu : http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

58 : En France, la gendarmerie et la police opèrent dans le cadre d'enquêtes judiciaires. Si un juge d'instruction est impliqué, des actions offensives peuvent être ordonnées mais sont menées sous contrôle dudit juge. Ce suivi ne semble pas être de mise chez les Anglo-Saxons.

La vulnérabilité permet de communiquer les adresses MAC (identifiant une machine) et IP des utilisateurs aux attaquants. Le problème posé par cette approche, en dehors des libertés prises avec la loi, c'est que FH hébergeait une quantité non négligeable de sites, ainsi que TorMail, le service e-mail Tor[132]. Ainsi, en compromettant l'hébergeur, le FBI et les services de police impliqués dans cette opération ont également pu obtenir des informations sur la messagerie et ses utilisateurs, ce qui dépasse la lutte contre la pédopornographie.

La compromission de TorMail a donc motivé beaucoup d'utilisateurs souhaitant l'anonymat et la sécurité des communications à chercher des fournisseurs d'e-mail hébergés hors des États-Unis et de l'Union européenne. C'est ainsi qu'on a vu émerger SAFe-mail, une entreprise israélienne. Ses utilisateurs comptaient non seulement des vendeurs de substances illicites et des scammeurs bitcoin, mais également des journalistes. Runa Sandvik, experte infosec et actuellement directrice sécurité des SI au *New York Times*, a analysé[133] les rapports, visiblement pacifiques, entre l'entreprise et les divers services de sécurité tels que le FBI. Il est apparu que l'entreprise « *n'était pas au courant d'activité criminelle* » ayant lieu *via* son service e-mail ; de même, la société collabore avec les autorités israéliennes si une demande en émane. Comment les communications hébergées par SAFe-mail sont-elles chiffrées (bout en bout ou point à point) ? Ce n'est pas très clair… Enfin, l'entreprise reconnaît avoir reçu des ordres émanant de cours israéliennes mais provenant d'États étrangers. Le tiers de confiance n'a dans ce cas pas vraiment l'air digne de confiance…

INFILTRATION ET SURVEILLANCE, NŒUD GORDIEN

Le monde numérique (dont le darkweb) est une image du monde hors-ligne. Les forces de l'ordre se sont adaptées et ont acquis des compétences supplémentaires et parfois spécifiques, permettant de mener des enquêtes en ligne et notamment sur le

darkweb. Comme Tor donne la même puissance d'anonymat à tout le monde, les infiltrations sont donc possibles. De nombreuses opérations sont connues et ont permis d'appréhender des acheteurs d'armes[59] et de poisons[60]. Les infiltrations par des agents spéciaux et autres policiers dans les marchés darkweb vendant des armes ont été tellement intenses qu'Agora, l'e-commerce d'armes le plus prospère, avait tout simplement cessé d'accepter ces produits à la vente[134]. Un agent peut aussi se faire passer pour un client et acheter des armes. Dans certains cas, les vendeurs peuvent y avoir laissé des empreintes digitales[135]… On se souvient de Silk Road 2, héritier du défunt Silk Road, apparu à peine un mois[136] après que le FBI a procédé à l'arrestation de Ross Ulbricht et que le site a été désactivé. Silk Road 2 a eu une durée de vie très limitée : l'équipe de gestionnaires du site a été infiltrée par un agent du FBI dès le départ. Il a été possible de parvenir à son fondateur, Blake Benthall, grâce à des informations récoltées pendant l'infiltration et enrichies par la suite avec des détails disponibles sur des sites à accès public[137].

Avant de débattre, exemples à l'appui, du bien-fondé éthique de certains agissements des forces de l'ordre, rappelons les étapes d'une procédure judiciaire pénale en France. Un délit ou un crime doit tout d'abord avoir été constaté. Il s'agira d'une infraction punie par la loi selon le Code pénal. La phase dite policière peut être menée par tout représentant de la police, de la gendarmerie ou des douanes. L'objectif de cette phase sera la constitution des preuves

59 : https://motherboard.vice.com/read/dark-web-guns-bust-over-a-dozen-arrested-in-undercover-operation Dans ce cas, de l'information blanche a permis à des enquêteurs indépendants de découvrir le vendeur et le site d'e-commerce concernés. Voir les explications de Gwern sur Reddit : https://www.reddit.com/r/DarkNetMarkets/comments/35ytiw/17_arrests_due_to_flipped_agora_seller_weaponsguy/

60 : Une opération est décrite ici : http://www.tampabay.com/news/courts/criminal/labelle-man-accused-of-selling-toxin-in-death-plot/2162117 . D'autres cas de tentatives d'achat de poisons se sont soldés par les arrestations des clients : http://www.independent.ie/irish-news/courts/man-ordered-enough-deadly-poison-on-the-dark-web-to-kill-1400-people-court-hears-31392729.html ; http://nypost.com/2015/01/20/man-charged-with-trying-to-buy-deadly-poison-on-dark-web/ ; http://www.dailymail.co.uk/news/article-3030368/16-year-old-boy-admits-trying-buy-killer-poison-30-times-deadlier-ricin-undercover-officers-Dark-Web.html

de l'infraction : soit par le biais d'investigations (les forces de l'ordre en font en permanence pour justement détecter ce genre de faits), soit par le biais d'une saisie (par une victime ou par le procureur de la République). On ne parlera pas des modalités en détails, mais précisons que son objectif principal est de dépasser le stade du simple soupçon : pour que procédure pénale il y ait, le délit doit être caractérisé. Dans les cas complexes ou graves, la phase policière peut être étendue à l'instruction judiciaire. Dans ce cas, l'enquêteur en charge est un juge d'instruction. Ce dernier est indépendant du parquet, a des pouvoirs très étendus et peut notamment autoriser des écoutes, de la géolocalisation, des intrusions dans des systèmes informatiques, etc. L'objectif de ces opérations peut ainsi être de démanteler un réseau de délinquants. Un juge d'instruction peut également décider d'une détention provisoire s'il estime avoir suffisamment d'éléments à charge ; c'est à ce moment qu'un suspect devient mis en examen justement. Dès que le juge d'instruction termine son travail, il prend ce que l'on appelle une ordonnance de règlement : il est déchargé de l'enquête ; l'ordonnance décide de la suite de la procédure.

Ainsi une procédure pénale est-elle un travail complexe et souvent de longue haleine. On le devine aisément : pour prétendre décrire un délit caractérisé, il faut recueillir ce que l'on appelle des preuves pénales. C'est pour ce faire que l'instruction comprend des situations où les activités des délinquants potentiels peuvent se poursuivre pendant un temps.

De nombreux cas de compromission suite à des attaques informatiques sont connus. Mais si l'infiltration est une activité légale, les attaques informatiques le sont beaucoup moins. Ceci est également vrai dans le cas d'attaques menées par le FBI et des agences de police. Dans le cas de la compromission du navigateur Tor évoquée dans la sous-section précédente, des sites pédopornographiques ont été fermés et des utilisateurs potentiels repérés. Il reste que les outils utilisés par nombre de personnes pour se cacher d'un (souvent leur)

gouvernement peu démocratique ont également été compromis. Diverses opérations ont permis d'(ab)user des mêmes méthodes que celles utilisées par des hackers malveillants souhaitant s'emparer de données personnelles laissées sur des sites de rencontres. Dans un cas, des chercheurs américains ont découvert et décrit une vulnérabilité dans Tor permettant de découvrir les adresses IP de marchés du darkweb et de leurs utilisateurs ; le FBI a envoyé une mise en demeure à l'université forçant les chercheurs à transmettre les données recueillies[138]. Ces approches soulèvent de nombreuses questions éthiques et politiques. Discutons brièvement du cas le plus récent : la fermeture du site pédopornographique PlayPen.

Après la fermeture de divers sites pédopornographiques (suite à des opérations dont on a parlé plus haut), PlayPen est devenu le nouveau roi du domaine. Son nom annonce la couleur (*playpen* signifie « lit à barreaux » en anglais) ; de ce que l'on sait, plus de 200 000 utilisateurs échangeaient, et des images de violence sur enfants, et des conseils pour ne pas se faire prendre. Une agence opérant pour un pays inconnu, mais qui n'est pas les États-Unis, a réussi à introduire un logiciel vérolé chez les administrateurs de PlayPen : cliquer sur le lien vers une vidéo permettait de diriger le trafic du site hors de Tor[139]. Cette compromission a été faite en décembre 2014. Le renseignement a été fourni au FBI et en février 2015, les serveurs ont été saisis. C'est là où l'histoire diverge d'opérations similaires passées (Silk Road…) : le site n'a pas été fermé, mais a vu se déployer un outil de monitoring du trafic créé et opéré par le FBI[140]. En quelques mois seulement, le FBI a mis la main sur plus de 1 300 adresses IP et autres informations permettant d'identifier les visiteurs et utilisateurs de PlayPen. Des procès ont été intentés à des Américains et deux sont déjà en attente de jugement[141].

Si l'on ne peut que se réjouir du fait que des criminels aient été identifiés et mis derrière les barreaux, à bien y regarder le cas PlayPen est très inquiétant. Le FBI a laissé le site opérant pendant au moins deux semaines, sous son contrôle. Pendant ce temps,

des milliers d'images pédopornographiques ont été téléchargées et téléversées ; ces agissements doivent être punis, et l'institution pénalement responsable pour les avoir autorisés est bien le FBI[142]. Nous sommes donc face à deux questionnements de taille : l'un est de l'ordre éthique, l'autre d'ordre démocratique. En effet, on peut s'interroger sur le compromis qui consiste à laisser des gens produire et télécharger des contenus illégaux pour recueillir des preuves contre eux. Dans ce cas, si l'on prend la procédure d'enquête judiciaire en France, un juge permet la propagation d'images pédo-pornographiques. Actuellement, il ne semble pas y avoir de réponse univoque à cette question, chacun risque de prendre la position la plus en phase avec son propre système de valeurs morales, mais il apparaît important de se poser ses questions et d'y réfléchir à plusieurs. Typiquement, on peut évoquer le compromis selon lequel laisser quelques délinquants faire pendant un petit moment est moins grave que ne pas avoir de quoi les mettre derrière les barreaux pour un petit moment : le bilan global est donc positif.

L'autre questionnement qui transpire de cette discussion est d'ordre démocratique. Pour permettre le recueil de données dans le cadre de l'enquête PlayPen, le FBI a bénéficié de l'autorisation d'un juge. La demande formulée auprès de celui-ci est cependant très vague et générale. Le résultat des courses dépasse largement le cas PlayPen : l'autorisation d'un juge à une demande très vague permet au FBI d'effectuer autant d'intrusions que l'agence le souhaite, sans avoir à communiquer les cibles ni à respecter les frontières nationales. Le FBI n'a jamais publié d'informations à propos du fonctionnement de leur(s) outil(s) d'intrusion non plus. Des associations de défense des droits numériques telles que l'EFF avaient saisi la justice pour se prononcer sur le dépassement de prérogatives et l'intrusion massive dans les ordinateurs de centaines de personnes. Dans un de ces procès qui s'est conclu très récemment, les accusations contre l'un des justiciables ont été totalement abandonnées : poursuivre les procédures judiciaires exigeait que le FBI rende public le code source du programme ayant servi à compromettre

les connexions anonymisées des internautes accusés. Le FBI a donc choisi d'abandonner toutes les poursuites dans le cadre du procès pour participation aux activités du site pédopornographique PlayPen plutôt que de rendre public l'*exploit* ayant servi à s'introduire dans les ordinateurs des suspects[61].

Les cours américaines sont ainsi face à un précédent légal de taille : alors que certaines reconnaissent l'incapacité de la constitution américaine à protéger ce que l'on fait avec notre ordinateur personnel[143] (ce qui crée de la jurisprudence favorable aux agissements du FBI), la plupart ne sont pas en mesure de résoudre le problème technico-judiciaire. La jurisprudence évoquée à l'instant signifie qu'une agence gouvernementale américaine n'a pas besoin de l'autorisation d'un juge pour s'introduire dans l'ordinateur d'un individu. C'est inquiétant, mais l'histoire devient encore plus terrifiante quand on imagine que cela pourrait très bien arriver chez nous : le FBI pouvant s'introduire dans mon et votre ordinateur, un juge français saura-t-il faire régner la loi française si l'on s'en offusquait ?

INFORMATION BLANCHE

En France, la communauté du renseignement utilise l'idiome « information blanche » pour désigner toute information accessible publiquement de façon ouverte. Les Anglo-Saxons l'appellent l'OSINT, abréviation d'« *open source intelligence* », ou « renseignement/information issu(e) de sources ouvertes ». Par exemple, vos tweets sont souvent géolocalisés : on peut ainsi savoir que tel jour des vacances, vous avez pris une photo devant la Tour Eiffel. Nul n'a besoin d'accéder à de l'information privée (vous questionner dans le cadre d'une enquête criminelle par exemple) pour savoir que tel jour à telle heure vous vous trouviez très probablement à Paris, pas loin de la place du Trocadéro. Comme mentionné plus haut, tout ou presque tout ce que l'on fait laisse des traces.

61 : Au total, 135 personnes sont poursuivies pénalement. https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/

Un exemple célèbre de traces probantes ayant mené à l'arrestation de suspect opérant dans le darkweb est l'identification de Ross Ulbricht. Un inspecteur des impôts, Gary Alford, a par exemple[144] cherché les mentions les plus vieilles de Silk Road. Il a ainsi trouvé de vieilles annonces dans des forums qui liaient Ross Ulbricht à la création (présumée) de Silk Road[145]. Avec de la persévérance et une assiduité exemplaire sur les forums prônant la légalisation du cannabis, l'enquêteur indépendant, connu sous le pseudonyme La Moustache, a permis[146] de connecter l'un des principaux gestionnaires de Silk Road, Thomas Clark, plus connu sous le nom de Variety Jones. Cette identification a mené à son arrestation et sa mise en examen[147]. Dans cette même optique, le cas d'un vendeur de cannabis à succès sur Silk Road, Agora, Abraxas et AlphaBay est intéressant ; son nom d'utilisateur est alors « caliconnect » ou une variante assez facilement reconnaissable. L'élément qui a permis de formuler des accusations précises à l'encontre de Burchard est… la découverte de la tentative vaniteuse de Burchard de protéger le nom en déposant la marque « caliconnect » ! Les registres sont publics, donc il est très simple de voir le véritable nom de la personne ayant déposé la marque. Les enquêteurs ont pu remonter les pistes, retrouver des commentaires de clients sur Reddit et autres forums où ils donnaient leur avis sur la marchandise de Burchard. Et il y en a eu des avis clients ! Caliconnect était dans le Top 20 des vendeurs sur Silk Road (parmi 4 000 au total, c'est une position enviable dans ce monde-là) et les estimations portaient ses gains à plus d'un million de dollars.

BEAUCOUP DES RÉPONSES, ENCORE PLUS DE QUESTIONS

Ce que cette discussion autour de l'OPSEC, l'anonymat et la sécurité montre, c'est qu'il est illusoire de penser que l'utilisation d'un outil technique se suffit à elle-même pour satisfaire à des exigences très différentes et distinctes. Plus encore, ce que l'on apprend en étudiant les darkwebs, c'est qu'il est impossible de dis-

socier la motivation politique de ces espaces. Il est indiscutable que certaines activités touchent à ce que l'on définit d'habitude comme des activités criminelles. Cependant, le paysage est largement plus nuancé : doit-on considérer qu'une utilisation revendiquant la désobéissance civile est forcément criminelle ?

En outre, la manière de compter et de quantifier les choses a une incidence politique. Vu que de nombreux sites peuvent être et sont opérés à partir d'un même service, le volume d'activités potentiellement illicites se retrouve largement réduit. Si, par exemple, cinq places de marché vendant des drogues sont opérées par le même service caché, donc le même cartel, est-on face à cinq sites ou à un cartel ?

Poussons notre réflexion plus loin : on pourrait se demander quel est le rôle des institutions censées faire respecter la loi. Sommes-nous prêts à donner carte blanche à la police, la gendarmerie, au FBI et autres pour (ab)user d'approches et d'outils au nom de notre protection ? Il est beaucoup question de laisser des portes dérobées dans les applications chiffrées pour que les forces de l'ordre puissent accéder aux communications à tout moment s'il y a une suspicion. Cela reviendrait-il à dire que la présomption d'innocence se transforme en présomption de culpabilité ? De gros titres défraient régulièrement la chronique et nous sommes tous conscients qu'on peut démocratiquement élire un dictateur. Dans un tel cas, quelle différence y aurait-il entre les systèmes de règles criminelles et ceux établis par des systèmes autoritaires ? Au final, on serait dans une situation intenable où les principes démocratiques fondamentaux de notre société sont remis en cause et travestis par des lois scélérates. On revient donc à l'éternelle question de savoir qui surveillera les surveillants et assurera que non seulement l'ordre mais aussi les principes démocratiques sont préservés.

CONCLUSION

Nous voilà à la fin de notre petite exploration. Que peut-on dire en nous quittant sur le pas de cette porte ?

Que notre relation avec le numérique se complexifie. Qu'elle prend des formes de plus en plus intimes aussi. Que nous sommes à une étape fascinante de cette hybridation où certains se font implanter des puces RFID (radio-identification) pour « s'augmenter » tandis que d'autres font la rétro-ingénierie de leurs pacemakers pour savoir ce qui se cache dans la technologie qui permet à leur cœur de battre. Que ce soit un objet physique « intelligent » ou un réseau social, la connexion à Internet est devenue une extension de nous-mêmes.

Il y a quelques années, on pouvait défendre avec force que la technologie est fondamentalement neutre et que son impact dépend de l'usage qui en est fait. Aujourd'hui, la délégation de pouvoir à des outils numériques et autres objets connectés, tous plus complexes et fermés les uns des autres, devient un terrain de jeu d'ingénieurs sociaux. Permettre et encourager l'innovation se transforme en gadgétisation à tout prix ; pour survivre dans un environnement industriel très concurrentiel, on fait donc l'impasse sur les fondamentaux.

Comment donc avoir confiance en quelque objet ou service numérique dont on ignore tout et dont la valeur et l'éthique ne sont garanties que par le discours commercial qui l'accompagne ? Telle était la question à laquelle cet ouvrage tentait de répondre, en prenant comme grille de lecture la malveillance connectée qui semble s'intensifier plus vite que le barrage qu'on peut y faire. En explorant des faces cachées, c'est surtout la complexité de notre rapport au numérique qui est apparue. Ce rapport est à l'image de ce qui nous entoure : rien n'est blanc ou noir, rien ne justifie de traiter le « cyber » de cyberdélinquance comme une circonstance aggravante et rien ne justifie de sous-estimer l'ampleur des enjeux pour tout un chacun. Le traitement du sujet qui en est fait dans cet ouvrage est aussi à l'image de notre rapport au numérique : multicouches, multifacettes, plus ou moins compréhensible, plus ou moins drôle.

L'angle de la sécurité est donc important dans ce contexte. La menace et la confiance sont, pour reprendre un cliché, les deux faces d'une même monnaie. Ce qui fait le lien entre les deux est la sécurité : il s'agit de s'assurer que la menace n'existe plus ou a été suffisamment réduite pour pouvoir de nouveau se sentir en confiance. Et c'est pourquoi la sécurité est un objet à part, dual, difficile à traduire : elle est à la fois une réalité et un sentiment.

Sa réalité (mathématique, technique) se traduit en des algorithmes de chiffrement, en protection contre les logiciels malveillants, en modèles de menaces et autres contre-mesures. On peut monter en compétences et continuer à accélérer la course, comme Alice et la Reine Rouge, voire parfois avoir un mouvement d'avance. Le sentiment de sécurité est cependant ce qui complique cette tâche de manière considérable : la perception que chacun de nous a de ce qui constitue un risque et de ce qui est digne de confiance varie entre les individus. On peut très bien se sentir en confiance alors qu'une menace persiste (pour peu qu'on l'ignore) – et inversement, on peut se sentir en danger alors qu'on est techniquement plutôt bien protégé.

Et puisqu'on en est à parler de ressenti, rappelons la réalité de cette tension entre sécurité et protection. Après tout ce que nous avons dit jusque-là, il semble de plus en plus évident que « sécurité contre vie privée » est une fausse opposition. On le voit par exemple dans l'inaptitude d'une surveillance généralisée de nos vies numérico-charnelles à en assurer la sécurité. On peut dire que ces gesticulations sécuritaires permettent de renforcer le sentiment de sécurité. La question est de nouveau dans la facilité déconcertante de faire passer ce sentiment pour une réalité. À force de se dire que des mesures sont prises, on oublie que la menace évolue.

C'est à ce moment qu'on doit se rappeler que la douche appartient à ceux qui chantent faux et que pour que cela continue, on ne doit pas permettre une infantilisation de nos usages ni des compromis avec notre sécurité qui cachent le fait que le vrai travail de mise en réalité n'est pas fait. Pour pouvoir continuer à chanter (faux) sous la douche, vous et moi devons garder en tête les enjeux de confiance à l'heure du numérique et en devenir des acteurs.

REMERCIEMENTS DE L'AUTEUR

Commencer ce livre a été difficile. Le finir a aussi été difficile mais pas pour les mêmes raisons : il y a tellement de choses à dire qu'on ne sait pas par où commencer. Et une fois qu'on a commencé, on sait encore moins où s'arrêter.

Si j'ai su, maladroitement et à coups de blagues pas toujours très drôles, faire en sorte que ce livre voie le jour, c'est grâce à un environnement bienveillant et porteur. Oui, c'est une manière quelque peu pompeuse de dire : les zami-e-s, je vous adore !

Merci à Stéphane Bortzmeyer d'avoir fait confiance à mes tribulations numériques et à ma capacité de les raconter. La préface a su cristalliser, avec la simplicité et la sincérité qu'on te connaît, Bortz, les doutes, questionnements et enjeux abordés (et bien sûr, merci pour le fou rire Marianas Web !).

Merci à ceux qui ont vu les brouillons boiteux, qui ont relevé des erreurs, des contradictions, des insuffisances ou encore baissé l'intensité d'excès occasionnels de lulz. À Benoît pour ses retours détaillés et pointilleux ; à Jef Mathiot pour « les darquenettes » et pour le label *Approved by @TouitTouit* ; à Éric F. pour les suggestions et critiques constructives ; à Tris Acatrinei parce qu'à l'Est, on est têtues et c'est très bien aussi ; à Stéphanie Chaptal pour sa présence rassurante et enrichissante ; à Marc Rees pour être qui il est, surtout au FIC ; à Me Ronan Hardouin, le meilleur avocat du monde, d'avoir évité un petit désastre ; à Sniperovitch et Ivan pour l'ode de vie saveur couscous ; à J. pour la musique et la mauvaise foi phénoménale ; à Olive pour

l'ambition ; à Emmanuel pour le soutien moral ; à ceux que je n'ai pas nommés, qui se reconnaîtront, et dont la présence a été une source constante de ~~trolls~~ rires, de connaissances, de questions et autres jeux de mots douteux à pas d'heure.

Merci infiniment aux gens qui ont pris le temps, à travers leur fenêtre, de nous laisser entrevoir une dimension différente et complémentaire des enjeux du numérique : vxroot pour les conseils ; Benoît pour son « tome 42 » sur le vote électronique ; toi, qui te reconnaîtras, pour qui le réseau, c'est un jeu ; Olivier Tesquet pour le regard critique sur ceux dont tu suis les faits d'armes depuis si longtemps ; à Maxime Vaudano pour le travail exemplaire sur les Panama Papers et tant d'autres sujets ; à ceux dont les propos n'ont pas pu être inclus pour des raisons de sécurité (eh oui).

Merci à Maëva Journo et Agnès Busière, les jeunes femmes qui, chez Larousse, ont voulu cet ouvrage au moins autant que j'ai pris plaisir à l'écrire. Merci à Émilie Choupin pour la relecture et à Damien Payet pour les éléments graphiques. Votre patience, bonne humeur et curiosité ont été déterminantes (et pas seulement à cause de l'actualité galopante). Ma fierté et une des grandes réussites de ce livre seraient que vous changiez vos mots de passe régulièrement…

Bon, en faisant ce livre, j'ai appris à l'insu de mon plein gré qu'il faut savoir s'arrêter. J'espère qu'on aura d'autres occasions de reprendre ce chemin et de visiter ces espaces entremêlés comme si on revenait dans la maison de notre enfance : avec affection et sans peur.

SOURCES

* * *

AVANT-PROPOS

https://www.franceculture.fr/emissions/la-vie-numerique/banlieue-deep-web-et dark-net-meme-combat

00. LES MYTHES D'INTERNET

http://www.snopes.com/quotes/internet.asp

Françoise Levie, *L'homme qui voulait classer le monde*. Paul Otlet et le Mundaneum, Les Impressions nouvelles, 2006.

http://archive.org/stream/OtletTraitDocumentationUgent#page/n555/mode/1up

https://interstices.info/jcms/c_16645/louis-pouzin-la-tete-dans-les-reseaux

Slava Gerovitch, *From Newspeak to Cyberspeak: A History of Soviet Cybernetics*, MIT Press, 2002.

https://twitter.com/jjarmoc/status/789637654711267328

http://dylan.tweney.com/2001/09/26/internet-emerges-as-the-most-reliable-way-to-communicate/

http://www.businessinsider.fr/internet-est-reellement-controle-par-14-personnes-qui-detiennent-7-cles-secretes/

http://motherboard.vice.com/fr/read/le-controle-dinternet-est-entre-les-mains-de-14-personnes?utm_source=mbfrtw

http://www.icann.org/tr/french.html

http://www.businessinsider.fr/internet-est-reellement-controle-par-14-personnes-qui-detiennent-7-cles-secretes/

https://www.ietf.org/

https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7444/show/securiser-les-communications-sur-internet-de-bout-en-bout-avec-le-protocole-dane.html

http://www.bortzmeyer.org/les-quatorze-qui-controlent-tout.html

http://www.slate.fr/story/122943/video-internet-cia-jeu-video-controler-esprits

01. LE CÔTÉ OBSCUR DE LA FORCE : PIRATAGES ET MALVEILLANCE CONNECTÉE

https://nvd.nist.gov/visualizations/cwe-over-time
https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu
https://blog.qualys.com/ssllabs/2013/10/31/apple-enabled-beast-mitigations-in-os-x-109-mavericks
https://blog.qualys.com/ssllabs/2013/09/10/is-beast-still-a-threat ; https://threatpost.com/apple-turns-on-safari-beast-attack-nitigation-by-default-in-os-x-navericks/102804/
http://www.codenomicon.com/news/pressrelease/2014/04/09/codenomicon_advising_internet_community_on_serious_internet_vulnerability_dubbed_heartbleed.html
http://heartbleed.com/
https://krebsonsecurity.com/2013/08/firefox-zero-day-used-in-child-porn-hunt/
https://www.exploit-db.com/
https://www.nextinpact.com/news/101344-mysql-chercheur-devoile-deux-failles-0-day-critiques.htm
http://www.zdnet.fr/actualites/et-si-l-iot-etait-une-mine-pour-la-securite-informatique-39840136.htm ; http://www.zdnet.fr/actualites/shodan-un-moteur-de-recherche-reve-pour-cybercriminels-et-les-responsables-iot-39842658.htm
http://www.zerodayinitiative.com/about/
http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/
https://arstechnica.co.uk/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/
https://www.zerodium.com/ios9.html
http://www.zdnet.fr/actualites/la-nsa-achete-des-vulnerabilites-y-compris-en-france-legalement-39794121.htm ; Vupen a fini par fermer ses bureaux en France. Pour se faire une idée des prix, en 2012, une 0day se vendait entre 5 000 et 250 000 dollars.
Pour une description détaillée, même si elle commence à dater un peu, voir Ablon L., Libicki M. C., & Golay A. A., Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, Rand Corporation, 2014. http://www.rand.org/pubs/research_reports/RR610.html
https://www.youtube.com/watch?v=b1iyQFcBCsI
http://www.zdnet.fr/actualites/comment-corriger-la-derniere-faille-0-day-de-linux-et-android-39831500.htm
http://www.vox.com/2016/8/24/12615258/nsa-security-breach-hoard
https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/
https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/
Bellovin S. M., Blaze M., Clark S., & Landau S. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet, Nw. J. Tech. & Intell. Prop., 12, i, 2014.
https://www.nextinpact.com/news/101945-au-journal-officiel-fichier-biometrique-60-millions-gens-honnetes.htm
http://blog.erratasec.com/2015/05/this-is-how-we-get-ants.html
http://www.liberation.fr/futurs/2017/02/21/le-megafichier-etendu-au-pas-de-charge_1549968
https://medium.com/@espringe/amazon-s-customer-service-backdoor-be375b3428c4#.jvpbvwsj9
http://money.cnn.com/2016/04/22/technology/facebook-twitter-phishing-scams/

Voir ces exemples : https://heimdalsecurity.com/blog/wp-content/uploads/Phishing-example-Amazon-Prime-22-12-2015.png (Amazon Premier); le Trésor public français https://www.francebleu.fr/infos/economie-social/le-tresor-public-met-en-garde-contre-des-faux-mails-de-remboursements-d-impots-1452595387 ; http://www.rtl.fr/culture/futur/une-nouvelle-arnaque-au-phishing-sur-gmail-comment-s-en-proteger-7786848043 (Gmail); http://www.rtl.fr/actu/conso/faux-mails-de-l-assurance-maladie-comment-se-proteger-du-phishing-7773820806 (Assurance maladie en France) ; https://particulier.edf.fr/fr/accueil/aide-et-contact/aide/arnaque-et-phishing.html (EDF); etc.

http://www.zonebourse.com/VINCI-4725/actualite/Vinci-Un-canular-a-18-en-7-minutes-23443531/

https://twitter.com/FranckMorelZB/status/801099935080910848

http://www.liberation.fr/futurs/2011/03/07/le-ministere-de-l-economie-et-des-finances-victime-d-une-attaque-informatique_719808

https://www.ssi.gouv.fr/particulier/principales-menaces/espionnage/attaque-par-hameconnage-cible-spearfishing/

https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/

https://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

https://bits.blogs.nytimes.com/2014/08/22/android-phones-hit-by-ransomware/?smid=pl-share

https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/

https://blog.barkly.com/phishing-statistics-2016

http://phishme.com/phishing-ransomware-threats-soared-q1-2016/

http://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/

http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/

http://www.lemonde.fr/les-decodeurs/article/2016/12/30/espionnage-pendant-la-presidentielle-ce-que-les-etats-unis-reprochent-a-moscou_5055689_4355770.html ; http://www.lepoint.fr/monde/la-russie-a-t-elle-vraiment-hacke-l-election-americaine-30-12-2016-2093683_24.php

http://www.chicagotribune.com/news/local/politics/ct-illinois-republican-party-email-hack-met-1212-20161211-story.html

Voir par exemple cette actu http://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html

https://threatconnect.com/blog/state-board-election-rabbit-hole/

https://chronopay.com/blog/2016/09/15/chronopay-pomogaet-king-servers-com/

http://www.reuters.com/article/us-usa-cyber-democrats-reconstruct-idUSKCN10E09H

https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

http://www.threatgeek.com/2016/06/dnc_update.html

https://wikileaks.org/podesta-emails/emailid/34899

https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

https://www.slideshare.net/MaliciaRogue/contes-legendesru-net16mars2015
http://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221
https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national
https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/
https://www.us-cert.gov/sites/default/files/publications/JAR-16-20296A.csv
http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/
https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
http://de.reuters.com/article/deutschland-russland-cyberangriff-idDEKCN0Y41D2
https://twitter.com/RidT/status/751325844002529280
https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.senat.fr/compte-rendu-commissions/20170130/etr.htm ; Social Media and Fake News in the 2016 Election http://web.stanford.edu/~gentzkow/research/fakenews.pdf
https://medium.com/@maliciarogue/la-bulle-algorithmique-cache-la-for%C3%AAt-des-int%C3%A9r%C3%AAts-financiers-c5626cffa66#.p8o3xp96p ; https://reflets.info/comment-la-cybersecurite-pourrait-sinviter-a-la-presidentielle-de-2017/
https://www.nytimes.com/2016/11/25/us/politics/hacking-russia-election-fears-barack-obama-donald-trump.html?_r=0
https://www.schneier.com/crypto-gram/archives/2000/0515.html#1
http://googlepublicpolicy.blogspot.co.uk/2012/07/breaking-borders-for-free-expression.html
http://www.slate.com/blogs/future_tense/2012/07/25/finspy_trojan_from_gamma_group_may_have_been_used_against_bahraini_activists_says_report_.html
https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/
http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html
https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/
https://privacyinternational.atavist.com/theireyesonme
http://reseau.echelon.free.fr/reseau.echelon/satellites.htm
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1
http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html
https://www.justice.gov/archive/ll/highlights.htm
https://www.wired.com/2010/08/nsl-gag-order-lifted/
http://www.washingtontimes.com/news/2004/may/28/20040528-122605-9267r/?page=all
https://www.technologyreview.com/s/405707/the-total-information-awareness-project-lives-on/
http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html
http://www.nysd.uscourts.gov/rulings/04CV2614_Opinion_092904.pdf
http://www.aclu.org/safefree/nationalsecurityletters/31580prs20070906.html
https://web.archive.org/web/20071106074840/http://www.aclu.org/safefree/nationalsecurityletters/31580prs20070906.html
https://www.techdirt.com/articles/20150427/11042430811/nsas-st ellar-wind-program-

was-almost-completely-useless-hidden-fisa-court-nsa-fbi.shtml
http://www.democrats.com/bush-impeachment-poll-2
http://www.pbs.org/wgbh/frontline/film/united-states-of-secrets/transcript/
https://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court#Criticism
Les révélations de The Intercept https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ ; résumé en français http://www.france24.com/fr/20140520-nsa-bahamas-portable-ecoute-enregistrement-shebab-terrorisme-paradis-fiscal-espionnage-snowden
http://www.afr.com/p/technology/interview_transcript_former_head_51yP0Cu1AQGUCs7WAC9ZVN
http://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html?_r=1
http://www.nytimes.com/2014/09/13/world/middleeast/elite-israeli-officers-decry-treatment-of-palestinians.html?_r=0
http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html
https://mic.com/articles/50459/8-whistleblowers-charged-with-violating-the-espionage-act-under-obama#.9rAHcsE6b
http://www.politifact.com/punditfact/statements/2014/jan/10/jake-tapper/cnns-tapper-obama-has-used-espionage-act-more-all-/
http://www.defenseone.com/business/2013/07/obama-whistleblower-witchhunt-wont-work-DOD/67598/
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security voir en français : http://www.lemonde.fr/technologies/article/2013/09/05/cybersurveillance-la-nsa-a-contourne-les-garde-fous-qui-protegent-les-donnees_3472159_651865.html
https://citizenlab.org/2013/07/planet-blue-coat-redux/
https://www.netsweeper.com/products/content-filtering/
https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan/#1969f49a4434
https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/
http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
https://www.tbb.org.tr/en/banks-and-banking-sector-information/statistical-reports/20
https://www.forbes.com/sites/thomasbrewster/2016/05/31/ability-unlimited-spy-system-ulin-ss7/#3c13a96063fa ; https://www.forbes.com/sites/thomasbrewster/2016/02/11/nypd-stingrays-all-over-new-york/#13e981d82d84
http://www.interceptors.com/ability-script.pdf
http://www.wassenaar.org/
http://www.international.gc.ca/controls-controles/report-rapports/2015.aspx?lang=eng
http://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2022475
http://www.timesofisrael.com/israeli-government-okayed-sale-of-spyware-that-exploits-iphones/
https://blog.imirhil.fr/2017/02/21/logiciel-libre-gouvernance-ethique.html
http://www3.epa.gov/otaq/cert/documents/vw-nov-caa-09-18-15.pdf
http://www.bloomberg.com/news/articles/2015-09-19/vw-clean-diesel-scheme-exposed-as-u-s-weighs-criminal-charges
http://www.volkswagenag.com/content/vwcorp/info_center/en/news/2015/09/Ad_hoc_US.html
http://www3.epa.gov/otaq/standards/light-duty/tier2stds.htm
http://www.dieselforum.org/about-clean-diesel/what-is-clean-diesel-

http://www.theicct.org/sites/default/files/publications/ICCT_PEMS-study_diesel-cars_20141013.pdf
http://www.nytimes.com/2015/09/21/business/international/volkswagen-chief-apologizes-for-breach-of-trust-after-recall.html
https://www.wired.com/2015/09/epa-opposes-rules-couldve-exposed-vws-cheating/
http://www.lemagit.fr/tribune/Laffaire -Volkswagen-Un-plaidoyer-pour-le -logiciel-libre ;
http://www.toolinux.com/L-affaire-Volkswagen
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/
http://www.pcworld.com/article/3012220/security/internet-connected-hello-barbie-doll-can-be-hacked.html
http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/
http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/
https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/
https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#57668e47e426
http://www.theregister.co.uk/2016/10/25/medsec_vs_st_jude_indy_pentester_report_lands/
http://www.vocativ.com/358530/smart-dildo-company-sued-for-tracking-users-habits/
http://observatoire-du-vote.eu/?page_id=38
http://oumph.free.fr/textes/vote_electronique_issy.html
http://cdst.revues.org/326
https://www.vice.com/fr/article/ce-hackeur-canadien-divulgue-les-infos-personnelles-des-racistes-d-internet
http://rue89.nouvelobs.com/2014/08/14/vengeance-dun-pseudo-hacker-contre-rue89-vire-tragique-254205
http://www.leparisien.fr/yvelines-78/mantes-la-ville-une-elue-d-opposition-victime-d-un-swatting-12-03-2015-4597789.php
http://www.europalestine.com/spip.php?article10749 ; http://www.ujfp.org/spip.php?article3966
https://www.nextinpact.com/news/98208-les-sanctions-contre-revenge-porn-portees-a-deux-ans-prison-et-60-000-euros-d-amende.htm
http://europe.newsweek.com/revenge-porn-italy-tiziana-cantone-nightclub-rape-video-499292?rm=eu

02. LES BONS, LES BRUTES ET LES ANONYMOUS

https://fr.wikipedia.org/wiki/Leet_speak
https://encyclopediadramatica.se/Main_Page
https://events.ccc.de
http://www.bbc.com/news/technology-10554538
https://fr.wikipedia.org/wiki/Steven_Levy
http://blog.historyofphonephreaking.org/
http://www.2600.com/
https://fr.wikipedia.org/wiki/Hackers
http://www.cs.indiana.edu/docproject/bdgtti/bdgtti_toc.html#SEC57
http://www.cs.indiana.edu/docproject/bdgtti/bdgtti_8.html
https://w2.eff.org/Net_culture/Net_info/EFF_Net_Guide/EEGTTI_HTML/eeg_91.html
news:alt.fan.warlord
Voir par exemple page 391 de The Johns Hopkins Guide to Digital Media
ou https://en.wikipedia.org/wiki/Netochka_Nezvanova_(author).
http://www.weirdcrap.com/recreational/bricefq1.htm

http://www.catb.org/jargon/html/B/B1FF.html
http://www.wired.com/ 1994/OS/alt.tes/class
https://www.youtube.com/watch?v=RFjU8bZR19A
https://www.youtube.com/watch?v=DNO6G4ApJQY
http://www.rsr.ch/#/la-1ere/programmes/on-en-parle/3058588-le-troll-la-bete-noire-du-net.html
http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1972
http://blog.wired.com/27bstroke6/2008/01/anonymous-attac.html
https://upload.wikimedia.org/wikipedia/commons/7/73/Message_to_Scientology.ogv
http://www.motherjones.com/mojo/2008/09/sarah-palins-secret-emails
http://sunshinereview.org/index.php/Alaska_Public_Records_Act
http://machinist.salon.com/blog/2008/09/15/palin_emails/
http://arstechnica.com/tech-policy/2008/09/palins-e-mail-habits-come-under-fire/
http://www.motherjones.com/politics/2011/06/sarah-palin-email-saga
https://www.wired.com/2008/09/palin-e-mail-ha/
http://gawker.com/5051193/sarah-palins-personal-emails
https://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked
http://www.slate.com/articles/technology/technology/2008/09/hacking_sarah_palin.html
http://www.memphisflyer.com/JacksonBaker/archives/2013/07/25/david-kernell-is-out-from-under
http://thephoenix.com/Boston/News/70055-Photos-Guy-Fawkes-Day/
http://blogs.mediapart.fr/edition/club-acte-2/article/110211/les-sociabilites-neuves-des-communautes-dinformation
http://knowyourmeme.com/memes/it-s-over-9000
http://blogs.suntimes.com/oprah/2008/09/oprah_winfrey_goes_after_inter.html
http://ireport.cnn.com/docs/DOC-93559 ; https://www.reddit.com/r/funny/comments/72g7t/oprah_gets_trolled_by_anonymous_oprah_vs_over/
http://www.liberation.fr/ecrans/2010/09/20/pedobear-la-chasse-a-l-ours-est-ouverte_954765
http://knowyourmeme.com/memes/events/over-9000-penises
http://www.liberation.fr/ecrans/2009/07/22/la-pedophilie-sur-internet-encore-instrumentalisee_958768?page=article
http://www.guardian.co.uk/media/2012/jun/12/how-to-deal-with-trolls
http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fnews.ninemsn.com.au%2Ftechnology%2F827036%2Finternet-underground-takes-on-iran
http://www.abc.net.au/news/stories/2009/09/10/2681642.htm
http://news.bbc.co.uk/2/hi/uk_news/8061979.stm
http://legifrance.gouv.fr/affichTexte.do;?cidTexte=JORFTEXT000021573619&dateTexte=vig
http://www.liberation.fr/france-archive/2009/04/10/le-ps-ruse-et-coince-hadopi-a-l-assemblee_559240
https://yro.slashdot.org/story/04/07/27/129219/patriot-act-used-to-enforce-copyright-law ; https://www.techdirt.com/articles/20100129/0630057974.shtml
http://www.indiantelevision.com/aac/y2k10/aac589.php
https://torrentfreak.com/anti-piracy-outfit-threatens-to-dos-uncooperative-torrent-sites-100905/
http://www.theregister.co.uk/2010/09/20/4chan_ddos_mpaa_riaa/
https://torrentfreak.com/images/mpaaddos.jpg
http://torrentfreak.com/4chan-to-ddos-riaa-next-is-this-the-protest-of-the-future-100919/
http://www.pandasecurity.com/mediacenter/news/4chan-users-organize-ddos-against-mpaa/
http://techcrunch.com/2010/09/19/riaa-attack/

https://torrentfreak.com/4chan-to-ddos-riaa-next-is-this-the-protest-of-the-future-100919/
http://www.slyck.com/story2040_Your_Quick_Reference_Guide_to_Current_US_BitTorrent_Lawsuits
http://www.theregister.co.uk/2009/05/12/davenport_lyons_acs_law/
https://web.archive.org/web/20110721060833/http://www.t3.com/news/law-firm-hands-out-thousands-of-fines-to-suspected-digital-pirates?=42559
http://news.bbc.co.uk/1/hi/technology/8481790.stm
https://web.archive.org/web/20091216055249/http://beingthreatened.yolasite.com:80/press-index.php
http://www.lawgazette.co.uk/opinion/letters/which-hunt
http://www.bbc.co.uk/news/technology-12275913
http://torrentfreak.com/wrongfully-accused-of-file-sharing-file-for-harassment-100831/
https://web.archive.org/web/20160129200458/http://www.parliament.the-stationery-office.co.uk/pa/ld200910/ldhansrd/text/100126-0003.htm
http://www.theregister.co.uk/2010/09/22/acs_4chan/
http://arstechnica.com/tech-policy/news/2010/09/amounts-to-blackmail-inside-a-p2p-settlement-letter-factory.ars
http://www.wired.co.uk/news/archive/2010-09/27/leaked-emails-fuel-anti-piracy-scandal
http://www.guardian.co.uk/technology/blog/2010/oct/01/acslaw-filesharing-accused
http://www.which.co.uk/news/2009/07/more-innocent-consumers-accused-of-file-sharing--179504
http://www.bbc.co.uk/newsbeat/article/11430299/my-details-appeared-on-porn-list
https://torrentfreak.com/acslaw-gay-porn-letters-target-pensioners-married-men-100925/
http://www.theregister.co.uk/2008/04/08/church_of_scientology_contacts_wikileaks/
https://www.wikileaks.org/wiki/Sarah_Palin_Yahoo_account_2008
http://www.imdb.com/title/tt1799148/
http://www.wired.com/threatlevel/2010/06/leak/
https://web.archive.org/web/20100722020415/http://www.aolnews.com/nation/article/wikileaks-snitch-hacker-adrian-lamo-faces-wrath-of-his-peers/19562042
http://213.251.145.96/cablegate.html
https://en.wikipedia.org/wiki/Reactions_to_the_United_States_diplomatic_cables_leak
http://www.bbc.co.uk/news/technology-11935539
http://www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=1&partner=rss&emc=rss
http://www.theatlantic.com/technology/archive/2010/12/wikileaks-exposes-internets-dissent-tax-not-nerd-supremacy/68397/
https://fr.wikipedia.org/wiki/R%C3%A9volution_am%C3%A9ricaine
Commander X. Behind The Mask: An Inside Look At Anonymous. Lulu.com
http://www.washingtonpost.com/wp-dyn/content/article/2011/01/25/AR2011012502918.html
http://www.cbc.ca/news/canada/story/2012/03/15/f-online-protest.html
http://switch.sjsu.edu/web/v4n2/stefan/
http://english.aljazeera.net/indepth/features/2011/01/20111614145839362.html
https://userscripts.org/scripts/show/94122
http://cryptoanarchy.org/wiki/Telecomix
https://www.youtube.com/watch?v=bilJ7lZtutQ
http://www.theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388/
http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars
http://english.aljazeera.net/indepth/opinion/2011/03/20113981026464808.html
https://www.nextinpact.com/archive/63924-sony-pictures-lulzsec-piratage-mots-de-passe-vol-donnees.htm
http://www.tnr.com/blog/the-study/89997/hacking-fun-more-profit
http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars
http://www.independent.co.uk/news/world/americas/who-are-the-group-behind-this-weeks-cia-hack-2298430.html ; http://www.pcmag.com/article2/0,2817,2387219,00.asp
http://www.wired.com/threatlevel/2011/05/lulzsec/
http://www.guardian.co.uk/technology/blog/2011/jun/24/lulzsec-site-down-hacker-jester ; http://www.computerandvideogames.com/308986/lulzsec-hacked-by-anti-hacking-group/
http://www.thesmokinggun.com/documents/internet/hackers-who-tried-sink-lulz-boat-071289 ; http://sanfrancisco.ibtimes.com/articles/169577/20110625/lulzsec-sails-into-sunset-as-teamp0ison-terrorizes-internet-antisec-anti-security-anonymous-hacker.htm ; http://www.guardian.co.uk/technology/2011/jun/24/lulzsec-irc-leak-the-full-record
http://www.nytimes.com/2010/12/04/world/europe/04domain.html
http://risky.biz/forum/why-we-secretly-love-lulzsec
http://www.passwordrandom.com/most-popular-passwords
http://owni.fr/2011/06/08/sur-les-traces-de-lulz-security-les-hackers-invisibles/
http://uk.ibtimes.com/articles/167639/20110622/lulzsec-lulz-security-anonymous-operation-anti-security-anti-sec-hacked-cleary-ryan-arrest-attack.htm
http://www.bbc.co.uk/news/technology-13912836
Inutile de faire un catalogue à la Prévert des attaques perpétrées dans le cadre de l'opération AntiSec : https://en.wikipedia.org/wiki/Operation_AntiSec
https://twitter.com/atopiary/status/94225773896015872
http://www.nytimes.com/2014/04/24/world/fbi-informant-is-tied-to-cyberattacks-abroad.html
https://fr.wikipedia.org/wiki/Quatri%C3%A8me_pouvoir
https://www.theguardian.com/world/blog/2010/dec/03/julian-assange-wikileaks
https://www.theguardian.com/news/datablog/2010/nov/29/wikileaks-cables-data#data
http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikilleaks-qosmos-amesys-libye-syrie/
http://cryptome.org/0002/ja-conspiracies.pdf
http://www.hyperorg.com/blogger/2010/12/05/truth-is-not-enough/
https://zunguzungu.wordpress.com/2010/11/29/julian-assange-and-the-computer-conspiracy-%E2%80%9Cto-destroy-this-invisible-government%E2%80%9D/ pour une analyse très complète.
http://gawker.com/5773533/julian-assange-my-enemies-are-all-jews-and-sissies
http://www.slate.com/blogs/the_slatest/2016/07/25/what_wikileaks_might_have_meant_by_that_anti_semitic_tweet.html
https://www.rt.com/tags/the-julian-assange-show/
https://twitter.com/wikileaks/status/756206619860561920
http://rue89.nouvelobs.com/2016/07/22/wikileaks-menace-creer-twitter-apres-quun-troll-a-ete-banni-264749
http://www.newyorker.com/magazine/2010/06/07/no-secrets
https://voicerepublic.com/talks/reports-from-the-front L'intervention en question, par Jacob Appelbaum, est à partir de 73 min 30 sec.
http://www.telerama.fr/monde/alan-rusbridger-du-guardian-wikileaks-a-instaure-un-

nouveau-type-de-rapports-entre-journalisme-et-technologie,65785.php
http://owni.fr/2011/08/23/les-confusions-dun-dissident-de-wikileaks/
http://www.telerama.fr/medias/le-cinquieme-pouvoir-le-film-sur-wikileaks-est-il-conforme-a-la-realite-des-faits,105860.php
http://www.telerama.fr/medias/wikileaks-regle-ses-comptes-dans-un-documentaire,103930.php
Voir pour davantage de détails et des entretiens, l'e-book d'Olivier Tesquet publié en 2011 sur l'histoire de WikiLeaks http://shop.owni.fr/fr/41-la-veritable-histoire-de-wikileaks.html
https://twitter.com/YourAnonNews/status/256194158971215872
http://pastebin.com/Juxb5M26
https://twitter.com/wikileaks/status/758781081072046080?ref_src=twsrc%5Etfw]
https://twitter.com/cyberrights/status/758390450009104385
https://wikileaks.org/akp-emails/
http://www.reuters.com/article/us-turkey-security-wikileaks-idUSKCN1000H1 ; http://www.numerama.com/politique/183868-la-turquie-bloque-wikileaks-pour-tenter-de-limiter-les-revelations.html
https://twitter.com/wikileaks/status/755657280406822912
https://twitter.com/dasecho/status/755758522416128000
https://twitter.com/ragipsoylu/status/755513149663707137
https://twitter.com/ragipsoylu/status/755511448407801856
https://wikileaks.org/akp-emails/?q=&mfrom=akparti.org. tr&mto=&title=&notitle=&date_from=&date_to=&nofrom=&noto=&count=50&sort=0#searchresult
https://wikileaks.org/akp-emails/emailid/31401
https://medium.com/@crymora/when-leaking-turns-into-dumping-61efcd20c96a#.ehbczztez
https://glomardisclosure.com/2016/07/26/the-who-and-how-of-the-akp-hack-dump-and-wikileaks-release
http://www.huffingtonpost.com/zeynep-tufekci/wikileaks-erdogan-emails_b_11158792.html
https://twitter.com/zeynep/status/757712462925926401
https://twitter.com/zeynep/status/757754939640799234
https://twitter.com/zeynep/status/757750555015979008
https://twitter.com/misterlast/status/757754961191137280
https://bontchev.nlcv.bas.bg/index.html
https://github.com/bontchev/wlscrape/blob/master/malware.md
https://wikileaks.org/podesta-emails/
http://www.politifact.com/global-news/statements/2016/oct/16/mike-pence/did-qatar-promise-clinton-foundation-1-million-fiv/
http://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html?smid=tw-nytimes&smtyp=cur&_r=0
http://www.lemonde.fr/pixels/article/2016/07/25/le-parti-democrate-voit-la-main-de-la-russie-derriere-la-publication-d-e-mails-par-wikileaks_4974501_4408996.html
http://rue89.nouvelobs.com/2016/10/31/maintenant-e-mails-clinton-entre-photos-bites-265545
https://twitter.com/RogerJStoneJr/status/782443074874138624

157 : http://www.telegraph.co.uk/news/uknews/law-and-order/11039528/Jui-lien-Assange-suffering-heart-condition-after-two-year-embassy-confinement-it-is-claimed.html ; http://www.ibtimes.co.uk/medical-woes-julian-assange-exhaustion-pain-likely-deteriorating-mental-state-1581689
http://www.nbcnews.com/politics/2016-election/wikileaks-fuels-conspiracy-theories-about-dnc-staffer-s-death-n627401
https://www.bloomberg.com/news/articles/2016-10-11/how-julian-assange-turned-

wikileaks-into-trump-s-best-friend
160 : http://tempsreel.nouvelobs.com/rue89/rue89-politique/20161004.RUE3976/pour-ses-10-ans-wikileaks-fait-une-conference-et-zero-revelation.html
https://twitter.com/KFILE/status/775110996071424001?ref_src=twsrc%5Etfw]
http://www.bloomberg.com/politics/articles/2016-10-08/clinton-refuses-to-disavow-hacked-excerpts-from-paid-speeches ;
https://www.washingtonpost.com/news/post-politics/wp/2016/10/11/clinton-campaign-chairman-says-fbi-probing-criminal-hack-of-his-email/?postshare=3211476278016159&tid=ss_mail
https://fr.scribd.com/document/28385794/Us-Intel-Wikileaks
http://www.salon.com/2010/12/15/manning_3/
http://www.nytimes.com/2010/10/24/world/24assange.html?pagewanted=all
http://www.washingtonpost.com/wp-dyn/content/article/2010/11/30/AR2010113001095.html
http://www.huffingtonpost.com/2010/12/07/fox-news-bob-beckel-calls_n_793467.html
http://www.guardian.co.uk/media/2010/dec/17/julian-assange-sweden
http://www.bbc.co.uk/news/world-us-canada-11856122
http://media.washingtonpost.com/wp-srv/politics/documents/Dept_of_State_Assange_letter.pdf
https://www.bloomberg.com/news/articles/2016-10-11/how-julian-assange-turned-wikileaks-into-trump-s-best-friend
http://pastebin.com/Juxb5M26
http://www.nytimes.com/2016/08/08/opinion/can-we-trust-julian-assange-and-wikileaks.html

03. LE DARKNET : DES MOTS ET DES MAUX

http://lci.tf1.fr/france/societe/bernard-debre-lr-en-guerre-contre-la-vente-de-drogues-sur-internet-8755720.html
https://web.archive.org/web/20150325025545/http://darknet.se/about-darknet/
http://www.cs.virginia.edu/~cs757/slidespdf/757-09-overlay.pdf
https://freenetproject.org/
http://msl1.mit.edu/ESD10/docs/darknet5.pdf
https://fr.wikipedia.org/wiki/Gestion_des_droits_num%C3%A9riques
Darknet: Hollywood's War Against the Digital Generation (JD Lasica, 2005) en parle en des termes plus accessibles. Voir http://www.m21editions.com/fr/darknet.shtml
https://www.torproject.org/
https://www.torproject.org/docs/faq#HideExits
Roger Dingledine, Nick Mathewson, Paul Syverson «Tor: The Second-Generation Onion Router» http://www.onion-router.net/Publications/tor-design.pdf
http://www.themonthly.com.au/issue/2011/march/1324265093/robert-manne/cypherpunk-revolutionary
https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
Chaum, D. L. (1981). «Untraceable electronic mail, return addresses, and digital pseudonyms». Communications of the ACM. 24 (2): 84–90. doi:10.1145/358549.358563.
Chaum, David (1983). «Blind signatures for untraceable payments». Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203. doi:10.1007/978-1-4757-0602-4_18.
https://fr.wikipedia.org/wiki/Crypto_Wars#.C3.88re_de_l.27ordinateur_personnel
Zimmermann, Philip (1995). "PGP Source Code and Internals". MIT Press. ISBN 0-262-24039-4.
https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg
http://www.nytimes.com/2015/11/17/us/after-paris-attacks-cia-director-rekindles-

debate-over-surveillance.html?ref=world&_r=0
https://nonblocking.info/liberte-egalite-tcpip/
https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000032655328&cidTexte=LEGITEXT000006071154
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id
http://www.activism.net/cypherpunk/manifesto.html , Eric Hughes, 1993.
McCullagh, Declan (2001-04-09). «Cypherpunk's Free Speech Defense». Wired.
http://www.forbes.com/forbes/1999/1101/6411390a.html
https://www.bloomberg.com/news/articles/2015-09-17/bitcoin-is-officially-a-commodity-according-to-u-s-regulator
http://blogs.wsj.com/digits/2015/10/22/eu-rules-bitcoin-is-a-currency-not-a-commodity-virtually/
https://www.cryptocoincharts.info/coins/info
https://theinternetofmoney.org
http://www.forbes.com/sites/laurashin/2016/07/14/this-man-traveled-around-the-world-for-18-months-spending-only-bitcoin/#10a2b9c6261e
https://www.saveonsend.com/blog/western-union-money-transfer/
https://www.saveonsend.com/blog/bitcoin-money-transfer/
https://web.archive.org/web/20131210164404/http://www.nytimes.com/2013/11/27/opinion/much-ado-about-bitcoin.html?_r=0
http://www.papergeek.fr/dark-web-et-deep-web-quelles-differences-et-comment-y-acceder-2963
https://www.youtube.com/watch?v=r0l2FPRoGp8
http://Citazine.fr/article/jour-j-ai-plonge-dans-deep-web
https://i.imgur.com/vvXru.png
http://junkee.com/the-best-unsolved-mysteries-on-the-internet/35874/3
https://www.youtube.com/watch?v=KztcytZSB-Q
http://searchformarianasweb.tumblr.com/
http://www.papergeek.fr/dark-web-et-deep-web-quelles-differences-et-comment-y-acceder-2963
https://torflow.uncharted.software/#?ML=18.017578125,42.94033923363181,3
https://metrics.torproject.org/hidserv-rend-relayed-cells.html
https://research.torproject.org/techreports/extrapolating-hidserv-stats-2015-01-31.pdf
https://terbiumlabs.com/darkwebstudy.html
http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085
http://thebotnet.com/guides-and-tutorials/49828-how-to-access-the-hidden-wiki/ ;
http://wordswithmeaning.org/special-you-know-nothing-of-the-internet-exploring-the-deep-web-confessions-from-an-investigator/
https://www.reddit.com/r/deepweb/comments/3iayfx/are_red_rooms_real/
https://www.youtube.com/watch?v=aDvRZw9EMWo ; un YouTubeur nommé CreepyPasta en est également très friand.
https://www.reddit.com/r/deepweb/comments/3irkmp/isis_redroom_megathread/
https://www.reddit.com/r/deepweb/comments/3ittf5/was_isis_redroom_a_honeypot/
https://www.reddit.com/r/deepweb/comments/3j0cz5/psa_do_not_go_to_that_new_isis_redroom_site_the/
https://www.torproject.org/docs/faq#WhySlow
Une discussion intéressante et sensée dans cette vidéo : https://youtu.be/K47o2EgUIJU
http://www.abc.net.au/7.30/content/2015/s4300786.htm
http://www.theage.com.au/victoria/melbourne-hurtcore-paedophile-master-matthew-

graham-pleads-guilty-20150908-gjht6d.html
http://www.theage.com.au/victoria/how-matthew-david-grahams-hurtcore-paedophile-habit-began-on-the-dark-web-20150908-gjhz43.html ; https://www.deepdotweb.com/2016/03/23/child-porn-website-admin-matthew-david-graham-jailed-15-years/
http://www.theage.com.au/victoria/australias-throwaway-children-20150903-gje3fq.html
http://www.9news.com.au/national/2015/03/16/02/19/tracking-the-australian-man-allegedly-responsible-for-horrific-child-sexual-abuse
http://www.snopes.com/horrors/madmen/snuff.asp
http://www.aljazeera.com/indepth/features/2016/10/dark-trade-rape-videos-sale-india-161023124250022.html
https://www.deepdotweb.com/2014/04/02/poll-should-we-publish-an-interview-with-a-pedo-site-owner/
https://www.deepdotweb.com/clarification-cancelled-interview/
http://www.bbc.com/news/technology-27885502
http://www.dailydot.com/crime/iowa-woman-craigslist-killer-father-schmidt/
http://www.cbsnews.com/news/facebook-murder-for-hire-plot-pa-teen-corey-adams-admits-he-used-site-to-go-after-rape-accuser/
http://abcnews.go.com/US/ohio-facebook-murder-fur-hire-plot/story?id=15765843
http://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/
https://en.wikipedia.org/wiki/Assassination_market
http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/
Pour le trafic d'êtres humains, voir par exemple ce billet de Deku-Shrub http://pirate.london/2015/11/human-hunting-on-the-internet-also-not-a-real-thing/
https://en.wikipedia.org/wiki/Albanian_mafia#Besa
http://www.hire-a-hitman.com/hire-a-hitman/
https://allthingsvice.com/2016/05/18/ugly-kids-are-cheaper-the-besa-files/
Si vous vous y intéressez, mais ne savez pas trop qui raconte des choses sensées, une personne-ressource précieuse est Deku-shrub https://www.reddit.com/user/Deku-shrub
https://www.reddit.com/r/deepweb/comments/4d70hh/how_to_improve_rdeepweb/
https://np.reddit.com/r/legaladvice/comments/5lpdd8/scammed_out_of_firearm_purchase/
http://motherboard.vice.com/blog/darknet-touring-the-hidden-internets-illegal-markets
http://motherboard.vice.com/read/the-fbis-deep-web-raid-seized-a-bunch-of-fake-sites
http://www.afp.gov.au/media-centre/news/afp/2015/may/four-australians-charged-in-international-illegal-firearm-sting?source=rss
https://www.deepdotweb.com/2015/07/07/agora-market-to-stop-listing-lethal-weapons/
http://www.focus.de/kultur/kino_tv/tv-kolumne-beckmann-beckmann-will-kalaschnikow-im-darknet-kaufen-doch-das-experiment-geht-schief_id_5542330.html
https://www.deepdotweb.com/2016/05/20/german-tv-show-gets-scammed-trying-buy-ak47-darknet/
https://www.deepdotweb.com/marketplace-directory/listing/therealdeal-market ;
https://www.reddit.com/user/TheRealDealMarket
https://www.reddit.com/r/BlackBank/comments/359oym/blackbank_service_under_ddos/
http://www.deepdotweb.com/2015/05/31/meet-the-market-admin-who-was-responsible-for-the-ddos-attacks/
http://www.deepdotweb.com/wp-content/uploads/2015/05/exit2.png

https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down/cyber-criminal-forum-taken-down ; voir aussi https://www.malwaretech.com/2015/07/darkode-returns-following-internationa.html
https://darkode.cc//
Une histoire détaillée https://www.deepdotweb.com/2015/07/20/darkode-extended-background-story/
B. Dupont, A.-M. Côté, C. Savine et D. Décary-Hétu (2016), "The ecology of trust among hackers", Global Crime, DOI: 10.1080/17440572.2016.1157480
https://twitter.com/Xylit0l
https://krebsonsecurity.com/2015/06/opms-database-for-sale-nope-it-came-from-another-us-gov/
http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/ ; déclaration du site compromis : http://ffn.com/security-updates/
https://teksecurityblog.com/hacked-how-safe-is-your-data-on-adult-social-sites/
https://www.cnet.com/news/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/
https://nakedsecurity.sophos.com/2016/11/11/facebook-is-buying-up-stolen-passwords-on-the-black-market/
http://www.informationsecuritybuzz.com/expert-comments/facebook-buying-back-stolen-passwords-dark-web/
http://www.csoonline.com/article/3142404/security/security-experts-divided-on-ethics-of-facebooks-password-purchases.html
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf
http://www.darkcomet-rat.com/
http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480
https://www.ctc.usma.edu/posts/financing-terror-bit-by-bit
https://www.baselgovernance.org/news/global-conference-countering-money-laundering-and-digital-currencies
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf
https://darknetmarkets.co/french-deep-web-market/
https://www.deepdotweb.com/marketplace-directory/listing/french-dark-net/
http://blog.trendmicro.com/trendlabs-security-intelligence/the-french-dark-net-is-looking-for-grammar-police/
http://www.vocativ.com/393689/war-on-drugs-human-rights-violation/
http://www.shroomery.org/forums/showflat.php/Number/13860995
https://www.youtube.com/user/ohyeaross
http://austincut.com/2012/01/silk-road-a-vicious-blow-to-the-war-on-drugs/
http://stackoverflow.com/questions/15445285/how-can-i-connect-to-a-tor-hidden-service-using-curl-in-php
https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf
http://arstechnica.com/tech-policy/2013/10/feds-silkroad-boss-paid-80000-for-snitchs-murder-and-torture/
Les échanges ayant mené à cette prétendue commande d'assassinat : http://arstechnica.com/tech-policy/2015/02/the-hitman-scam-dread-pirate-roberts-bizarre-murder-for-hire-attempts/
https://www.theguardian.com/technology/2013/nov/21/silk-road-founder-held-without-bail
http://www.dailydot.com/crime/silk-road-murder-cha rges-ross-ulbricht/
https://www.wired.com/2016/10/judges-question-ulbrichts-life-sentence-silk-road-appeal/
https://www.deepdotweb.com/2017/01/08/ross-ulbricht-legal-defense-fund-hacked/

http://arstechnica.com/tech-policy/2016/02/prosecutors-say-corrupt-silk-road-agent-has-co-conspirators-at-large/ ; http://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/
http://arstechnica.com/tech-policy/2016/09/exclusive-our-thai-prison-interview-with-an-alleged-top-advisor-to-silk-road/
http://www.thecrimson.com/article/2013/12/16/unconfirmed-reports-explosives-four-buildings/
http://www.thecrimson.com/article/2013/12/17/student-charged-bomb-threat/
http://cbsboston.files.wordpress.com/2013/12/kimeldoharvard.pdf
https://research.torproject.org/techreports/tbb-forensic-analysis-2013-06-28.pdf
https://motherboard.vice.com/read/this-researcher-is-hunting-down-ip-addresses-of-dark-web-sites
https://motherboard.vice.com/read/some-dark-web-markets-have-better-user-security-than-gmail-instagram
https://mascherari.press/onionscan-report-this-one-weird-trick-can-reveal-information-from-25-of-the-dark-web-2/
http://www.wired.co.uk/article/anonymous-targets-paedophiles
https://www.deepdotweb.com/2017/02/09/anonymous-hacks-freedom-hosting-ii-bringing-almost-20-active-darknet-sites/
https://www.wired.com/2014/01/tormail/
http://www.forbes.com/sites/runasandvik/2014/01/31/the-email-service-the-dark-web-is-actually-using/#402044448410
http://motherboard.vice.com/read/the-dark-webs-biggest-market-is-going-to-stop-selling-guns
http://motherboard.vice.com/read/tip-if-youre-selling-guns-on-the-dark-web-dont-get-your-prints-on-them
http://arstechnica.com/business/2013/11/just-a-month-after-shutdown-silk-road-2-0-emerges/
http://arstechnica.com/tech-policy/2014/11/silk-road-2-0-infiltrated-from-the-start-sold-8m-per-month-in-drugs/
https://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds Ces données ont permis d'inculper un Écossais http://www.edinburghnews.scotsman.com/news/crime/fbi-helps-catch-edinburgh-man-selling-drugs-on-dark-web-1-4139454
https://motherboard.vice.com/read/how-the-fbi-identified-suspects-behind-the-dark-webs-largest-child-porn-site-playpen
http://www.wired.com/2009/04/fbi-spyware-pro/
http://www.reuters.com/article/us-usa-crime-childporn-idUSKCN0PI2CH20150708
http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting
https://www.eff.org/deeplinks/2016/06/federal-court-fourth-amendment-does-not-protect-your-home-computer
http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html
https://motherboard.vice.com/read/the-google-search-that-took-down-ross-ulbricht
http://antilop.cc/sr/#jones
https://motherboard.vice.com/read/fbi-says-suspected-silk-road-architect-variety-jones-has-been-arrested

TABLE DES MATIÈRES

* * *

Avant-propos, *par Stéphane Bortzmeyer* 7
Les mythes d'Internet 11

Le côté obscur de la force :
piratages et malveillance connectée 27
Comment se fait-on pirater ? 29
L'éternelle tension entre protéger et respecter 83
La question de la confiance à l'heure du numérique . . 111

La figure du hacker :
les bons, les brutes et les Anonymous. 135
50 nuances de hacker 137
Du troll à l'hacktiviste 147
Le lanceur d'alerte : traître ou justicier ? 193

Le darkweb : des mots et des maux 235
Où est le darkweb ? 237
Voyage en terre d'oignons. 267
Caché comme un secret éventé 307

Conclusion 327
Remerciements de l'auteur 331
Sources. 333

LISTE DES ENTRETIENS

* * *

« Vxroot »,
expert sécurité informatique 49

Benoît Sibaud,
expert vote électronique et Internet 119

Anonyme,
expert réseaux et télécommunications 149

Maxime Vaudano,
journaliste au *Monde* et datajournaliste
pour Les Décodeurs 195

Olivier Tesquet,
journaliste à *Télérama* (Wikileaks) 223

ISBN : 978-2-03-593666-0

* * *

* * *

Dépôt légal : mai 2017
318882/01-11034295-avril 2017