Avant-propos

« D'après Stanford[1], en 2030, on aura 130 milliards d'objets qui seront connectés à Internet. Même ma main, vos cœurs sans doute, tout sera connecté. Quel est le cadre de la gouvernance ? Quelle est la politique publique qui réglementera cela ? »[2] En posant ces questions lors de la « réunion gouvernementale de haut niveau » rassemblant de nombreux responsables des gouvernements dans le cadre du 55e Congrès de l'ICANN, Fadi Chehadé, directeur de cette institution, résume une partie des problématiques abordées dans cet ouvrage. La déclaration du président de la puissante *Internet Corporation for Assigned Names and Numbers* permet, en effet, de rappeler l'importance des négociations actuellement en cours au niveau mondial entre gouvernements, organisations intergouvernementales et institutions internationales autour de la question de la gouvernance d'Internet. L'ICANN, qui assume depuis sa création en 1998 la fonction essentielle et stratégique de gestionnaire des noms de domaines et de l'adressage électronique sur Internet, est une organisation de droit privé. Elle est néanmoins assujettie aux tribunaux et à la Chambre de Commerce des États-Unis et dépend de ce fait du gouvernement américain. En 2014, les États-Unis ont accepté d'initier un processus de transition ouvrant la voie à l'internationalisation de l'ICANN et donc, en partie, de la gouvernance d'Internet. Internationalisation ou privatisation ? La résolution de cette alternative, qui reste une source de conflits en l'état actuel des négociations, conditionne l'avenir d'Internet. Ces tractations entre États, acteurs privés, communautés d'utilisateurs et organisations internationales au sujet de l'évolution

1. Stanford University. Université américaine privée, située au cœur de la Silicon Valley au sud de San Francisco. En 1968, l'Université de Stanford fut reliée à l'Université de Los Angeles (UCLA) et l'Université d'Utah grâce au premier réseau informatique délocalisé qui prit le nom d'ARPANET et préfigurait la création d'Internet.

2. Fadi Chehadé, directeur de l'*Internet Corporation for Assigned Names and Numbers* (ICANN). 55e Congrès de l'ICANN, Marrakech, 7 mars 2016.

de la juridiction internationale encadrant le développement du réseau mondial révèlent à quel point la gouvernance d'Internet est une question géopolitique de premier plan. Tandis que ces négociations se déroulaient au plus haut niveau, l'ampleur des cyberattaques qui ont touché en mai et juin 2017 des centaines de pays et d'institutions à travers le monde, et un nombre bien plus considérable encore de particuliers, a soudainement fait passer au premier plan un type de conflit et de criminalité d'un genre nouveau ayant pour théâtre le cyberespace. Parallèlement au débat sur le statut futur de l'ICANN, le phénomène du *Darknet*, dénomination englobant l'ensemble des réseaux cryptés, privés ou alternatifs sur Internet, pose d'une autre manière la question de la gouvernance et du contrôle du réseau, à travers le prisme de la cybersécurité et de la préservation de l'anonymat et de la liberté des utilisateurs d'Internet, autre débat, non moins essentiel, qui a pris une acuité particulière depuis les révélations d'Edward Snowden. Parce que les darknets – il est plus exact de parler de « réseaux cachés » au pluriel – participent à un développement anarchique du réseau mondial qui échappe en grande partie au contrôle des États et de l'ICANN, et parce que c'est au cœur de ces nouveaux territoires virtuels que s'échangent les outils des guerres et attaques informatiques à venir, cet ouvrage sera consacré à l'histoire et à la géopolitique du darknet (ou des darknets). Il conviendra donc, pour commencer, de définir les termes utilisés, en commençant par darknet et darknets, un pluriel pour désigner les différents réseaux privés ou cryptés, à l'instar de Tor (*The Onion Router*), I2P ou Freenet, et un singulier pour englober la totalité du phénomène de « l'Internet caché ». Le glissement du pluriel au singulier résume en lui-même une quinzaine d'années d'évolution et le passage des premiers réseaux d'échanges pair à pair (P2P) à une véritable nébuleuse de réseaux parallèles, évolution dont il sera largement question dans cet ouvrage. On s'efforcera donc ici de différencier les différents espaces qui constituent aujourd'hui le « réseau des réseaux » – « web surfacique », « web profond » ou « réseaux cachés » –, d'expliquer quelques notions essentielles telles que la neutralité du réseau et de mettre en lumière le rôle des acteurs de la gouvernance d'Internet, comme l'ICANN. Nous aborderons ensuite la généalogie du phénomène des darknets, replacée dans l'historique d'Internet et des transformations du cyberespace. On tâchera d'analyser quelles cultures sont liées à la constitution des communautés et espaces qui constituent ces nouveaux territoires virtuels et, pour finir, les implications sécuritaires, géopolitiques et économiques de cette nouvelle (r)évolution de l'univers du numérique que nous avons pris la liberté de baptiser « Internet 3.0 »[3]. Nous espérons que cet essai pourra éclairer au moins partiellement le lecteur sur les enjeux essentiels d'une transformation de la société de communication qui pourrait bouleverser dans un proche avenir aussi bien les usages du numérique que les politiques publiques et, bien sûr, notre vie quotidienne.

3. En distinguant bien cette expression de « web 3.0 » qui qualifie l'« Internet des objets ».

Introduction

Le 17 octobre 2011, le groupe Anonymous lançait une « opération darknet », révélant l'existence d'une quarantaine de sites pédophiles abrités sur le réseau Tor[1]. Les comptes de 1 626 utilisateurs de ces sites furent mis en ligne et l'opération conduisit à la fermeture des sites visés, mais inquiéta les autorités quant à la capacité de groupes tels que les Anonymous à interférer sérieusement avec les opérations de police en cours dans ce type de cas. L'affaire contribua aussi à accréditer et à populariser l'idée qu'il existerait un « Internet profond » donnant asile aux activités les plus illégales, sous le couvert d'une vaste zone de non-droit virtuelle. Le démantèlement par le FBI, un an et demi plus tard, en août 2013, d'un vaste réseau de pédopornographie sur le réseau Tor, puis l'arrestation en octobre de la même année de Ross Ulbricht, accusé d'administrer Silk Road, un site de vente en ligne de produits stupéfiants, contribuèrent à alimenter la légende noire. Le darknet a dès lors franchi le seuil de la confidentialité pour passer du stade de la rumeur à celui de phénomène de société, au point de frapper jusqu'à l'imagination du ministre de l'Intérieur Bernard Cazeneuve qui n'hésitait pas à affirmer, en mars 2016, dans un contexte politique marqué par une vague d'attentats meurtriers et par l'état d'urgence : « Ceux qui nous frappent utilisent le darknet et des messages chiffrés. » Phénomène jusqu'alors encore peu connu, l'existence de réseaux cachés tels que Tor, « le routeur en oignon »[2], accédait à ce moment à une petite notoriété médiatique.

En 2016, Sir David Omand, ancien directeur du GCHQ[3], faisait le constat suivant dans les pages du *World Policy Journal* [OMA 16] : « Le darknet est le lieu où la majeure partie des activités criminelles en ligne sont commises, à l'abri de

1. http://www.humanite.fr/medias/un-reseau-de-plus-de-1500-%C2%AB-pedophiles-%C2%BB-demantele-par-anonymous-482267.

2. Attribuant aux sites et utilisateurs connectés au réseau Tor des adresses en .onion en lieu et place des classiques .com ou .fr.

3. *Government Communications Headquarters* (GCHQ).

toute sanction. Sur le darknet, l'anonymat est la règle, et l'identité ou la localisation des utilisateurs peuvent être dissimulées, même aux yeux de la plus efficace des polices et des services de renseignement. » Tout en employant le singulier, David Omand prenait cependant soin de restituer au terme darknet sa singularité multiple, qui renvoie à un agrégat disparate de lieux virtuels, puisqu'il existe en réalité autant de darknets que de réseaux cryptés ou privés. « Le darknet est une collection de réseaux et de technologies employés pour partager du contenu numérique », expliquaient en 2003 Peter Biddle, Paul England, Marcus Peinado et Bryan Willman, usuellement considérés comme les premiers à avoir employé l'expression dans un article publié en 2003. « Le darknet n'est pas un réseau physiquement séparé, mais des applications et une couche de protocoles superposée à des réseaux existants. » [BID 03] Les quatre auteurs incluaient dans la dénomination de darknets, déjà mise au pluriel, les réseaux pair à pair (P2P), les systèmes d'échanges protégés par clés et jusqu'aux messageries électroniques, forums privés ou *newsgroups*[4]. Dès 2003, les quatre chercheurs prévoyaient l'irrémédiable expansion du phénomène [BID 03] : « Nous prévoyons que l'efficacité du darknet en tant que mécanisme de distribution se heurtera à quelques obstacles à court terme, mais dans l'absolu, le génie du darknet ne pourra pas être remis dans sa lampe. »

En 2003, Biddle, England, Peinado et Willman associaient l'idée de darknet exclusivement aux réseaux de distribution illégale de contenu sous licence. Le problème qui se posait donc à ce moment-là, synthétisé dans l'étude des quatre ingénieurs, se limitait encore au téléchargement illégal et à la menace représentée par ce phénomène en expansion pour l'industrie culturelle. Mais si l'on peut relier l'origine du concept de darknet au développement des réseaux de téléchargement illégal, l'expression renvoie aussi à une culture spécifique liée aux évolutions technologiques marquant le tournant des XX^e^ et XXI^e^ siècles. Le 8 février 1996, le président américain Bill Clinton signait le Telecommunications Act, accompagné du Communications Decency Act. Cette initiative représentait une étape historique dans le processus de libéralisation des télécommunications et des services en ligne tels qu'Internet. Le Telecommunications Act remplaçait le vieux Communication Act établi en 1934, en tentant de prendre en compte les évolutions radicales connues par la société américaine au cours des années 1960, 1970 et 1980. L'idée essentielle de la loi était de favoriser le développement de la compétition dans le domaine des

4. Le *Network News Transfer Protocol* (NNTP) est un protocole réseau désigné par des URL commençant par news://. Par exemple, le système en réseau Usenet, inventé en 1979, est organisé autour du principe de groupes de discussion (*newsgroups*) hiérarchisés en fonction de différentes thématiques, auxquels un utilisateur peut s'abonner selon ses préférences. Les *newsgroups* permettent l'échange d'articles, voire dans certains cas de fichiers image, audio ou vidéo.

télécommunications et de faciliter l'entrée de grands groupes privés dans un secteur initialement dominé par l'American Telephone & Telegraph Corporation. Initialement destiné à promouvoir l'ouverture du marché des télécommunications à de multiples groupes, le Telecommunications Act entraîna en réalité la création de nouveaux géants des télécommunications et la disparition d'un grand nombre d'acteurs mineurs de ce secteur. Nombre d'observateurs accusèrent le Telecommunications Act d'avoir ainsi ouvert la voie à la domination complète des médias de masse. En l'occurrence, la nouvelle législation permit à quelques grands acteurs de s'emparer du marché des fournisseurs d'accès, à l'instar de UUNet (devenu Verizon), Sprint corporation, Level 3 Communication (racheté le 31 octobre 2016 par Centurylink), Comcast ou AT&T. Au lendemain de l'annonce de la signature du Telecommunications Act par Bill Clinton, John Perry Barlow, cofondateur de l'Electronic Frontier Foundation[5] rédigeait une « Déclaration d'indépendance du cyberespace »[6], dans laquelle il affirmait qu'aucun gouvernement, aucune corporation ou institution ne devait imposer son autorité ou revendiquer un quelconque droit de propriété sur Internet. La déclaration proclamait notamment, à l'adresse des gouvernements ou des dirigeants de grands consortiums économiques : « Vous n'êtes pas les bienvenus ici. Vous n'avez aucune souveraineté là où nous nous réunissons. Nous formons notre propre contrat social. » La rhétorique « cyberrévolutionnaire », à l'image de celle de John Perry Barlow, peut sembler aujourd'hui bien fantaisiste. Elle irrigue pourtant encore les courants qui, à travers de multiples groupuscules, acteurs individuels, sites ou forums de discussion, défendent ardemment l'idée non plus d'un darknet mais d'un « Librenet », pour reprendre le nom donné au réseau social créé en 2010 : un Internet 3.0 anonyme et libre sur lequel l'usager reste toujours « en contrôle ».

Vingt ans après la publication de la « Déclaration d'indépendance du cyberespace », les temps ont cependant changé. Internet également. Selon les chiffres de l'Observatoire de la donnée[7], le volume mondial des bases de données en ligne atteint 4,4 zettabytes[8]. L'International Data Center[9] prévoit que ce volume

5. Fondée en 1990 aux États-Unis par Mitch Kapor, John Gilmore et John Perry Barlow, l'Electronic Frontier Foundation se donne pour principal objectif de défendre la liberté d'expression sur Internet.

6. Voir le texte en annexe 1.

7. Observatoire de la donnée, juillet 2014, étude IDC pour EMC-Digital Universe.

8. 1 zettabyte = 1 000 exabytes, soit 1021 bytes, l'unité de base mesurant les volumes d'information numérique. À titre de comparaison, 1 zettabyte correspond à 152 millions d'années de visionnage de cassettes VHS standards.

9. En 1976, un groupe de scientifiques fonde à Genève le GSE (*Group of Scientific Experts*), à l'issue de la conférence de désarmement de Genève, afin d'étudier l'évolution technologique. Entre 1984 et 1995, une série d'expérimentations dans le domaine de

mondial sera multiplié par 10 d'ici à 2020 pour atteindre 44 zettabytes[10]. Le rythme de développement exponentiel d'Internet rend aujourd'hui tout calcul partiellement caduc : certains auteurs évoquent un trillion de pages créées, soit mille milliards, d'autres un trilliard, etc. [PIS 08, p. 188] Cette croissance exponentielle intéresse les entreprises publiques et privées, soucieuses de tirer profit des opportunités économiques offertes par le « web profond » et le « Big Data ». Elle ouvre aussi de nouvelles perspectives à tous ceux qui entendent tirer profit d'une croissance du réseau mondial qui remet de plus en plus en question la capacité des structures étatiques à établir une surveillance efficace des multiples réseaux constituant aujourd'hui Internet. Cette aspiration à échapper au contrôle des institutions répond à des motivations économiques ou idéologiques et s'accorde aux promesses, parfois illusoires, d'un système globalisé rendant caduque toute forme de frontières, barrières et régulations.

Le développement récent des darknets, qui ne sont plus désormais seulement des réseaux d'échanges, mais de véritables couches de réseaux alternatifs superposées au réseau mondial, porte en lui toutes les interrogations suscitées par la croissance exponentielle des flux immatériels, la modification des usages du numérique et la remise en cause du statut régulateur des États. Ces derniers, ainsi que les agences de sécurité et de renseignement qui en dépendent, prennent aujourd'hui conscience du danger attaché à l'idée de zones de non-droit virtuelles échappant peu ou prou à leur contrôle. Tous multiplient donc les efforts pour développer des politiques crédibles et efficaces dans le domaine de la cybersécurité. La recrudescence du terrorisme, mais aussi d'autres activités illégales telles que trafics de drogue, d'armes ou d'êtres humains, qui utilisent les nouvelles technologies pour se développer, suscite la mise en place de politiques de sécurisation et de surveillance du cyberespace. Elles sont en retour sévèrement critiquées et remises en question par certaines franges de la société civile qui mettent au contraire en avant l'utilité de ces espaces où l'anonymat est relativement préservé pour les journalistes ou les dissidents menacés par les régimes autoritaires, permettant ainsi la libre circulation de l'information et la liberté d'expression. Mais les États utilisent aussi les possibilités offertes par les darknets pour conduire eux-mêmes une nouvelle forme de conflit interétatique ou asymétrique qui prend désormais place dans l'espace virtuel, mais a des

---

l'amélioration de la collecte de données est menée conjointement par des scientifiques américains, russes et suédois. En 1996, après la création de la *Comprehensive Nuclear-Test-Ban Organisation* (CBTO), le Centre international de la donnée (*International Data Center*) est transféré d'Arlington, en Virginie, à Vienne, en Autriche, pour devenir officiellement l'IDC. Depuis, cette organisation internationale génère des études et analyses de données indépendantes dans de multiples domaines.

10. Soit l'équivalent, selon le linguiste Mark Liberman, de l'intégralité des vocables et langages parlés sur la planète.

conséquences très concrètes, sous forme de cyberattaques, comme celle de grande ampleur qui avait visé l'Estonie en 2007, inaugurant l'entrée dans une nouvelle dimension de la guerre moderne. Si, pour le journaliste Duncan Campbell [CAM 07], les États ont perdu la bataille de la cryptographie visant à empêcher, à partir des années 1990, la diffusion de techniques de cryptage avancées dans la société civile, il semble cependant que les réseaux cryptés à l'image de Tor offrent aujourd'hui des capacités de résistance aux cyberattaques et représentent également un intérêt pour les États ou les entreprises souhaitant pouvoir mieux protéger leurs bases de données en ligne.

L'auteur de ce livre n'a pas l'ambition de proposer ici une approche technique détaillée des différents protocoles et applications liés au darknet [REN 16]. Il ne s'agit pas non plus d'un manuel informatique. L'objectif est ici de livrer des clés de compréhension d'un phénomène en pleine expansion en définissant bien sûr les notions de *darknet*, *dark web* et *deep web,* en prêtant attention à la production intellectuelle et idéologique qui a accompagné et accompagne encore l'essor des réseaux alternatifs et en examinant les enjeux économiques, sécuritaires et géopolitiques qui sont liés au darknet ou au deep web. On tentera de montrer ici notamment que la confrontation entre ces différents enjeux et entre les intérêts divergents des usagers, des institutions et des acteurs économiques renvoie toujours à la question des modes de gouvernance d'Internet. Les darknets sont au seuil d'une ère de développement beaucoup plus importante et rendent aujourd'hui ces questionnements cruciaux car, comme l'affirmaient Peter Biddle, Paul England, Marcus Peinado et Bryan Willman en 2003, « le génie du darknet ne pourra pas être remis dans sa lampe ».