Le Darknet

Stephen Hallot

ESIT – Université Sorbonne Nouvelle – Paris 3

Le Darknet

Stephen HALLOT

Sous la direction de Madame Isabelle COLLOMBAT

Mémoire de Master 2 professionnel

Mention : Traduction et interprétation
Spécialité : Traduction éditoriale, économique et technique

anglais-français (C-A)

Session de septembre 2018

Sommaire

Avertissement au lecteur :

Les termes faisant l'objet d'une fiche terminologique sont signalés en gras souligné lors de leur première occurrence. Les termes repris dans le glossaire apparaissent quant à eux en gras lors de leur première occurrence.

Première partie : exposé

Introduction : démythifier le Darknet

Dans l'univers de l'informatique, le **Darknet**, au même titre que la figure du hacker, est fortement connoté. Sulfureux, illégal, immoral, le Darknet serait la face sombre d'Internet, le lieu où s'effectuent les activités et les transactions les plus condamnables. C'est en tout cas ainsi qu'il est souvent présenté par les organes de presse traditionnels. Voici ce qu'on pouvait lire dans le chapeau d'un article de *Marianne* consacré au sujet :

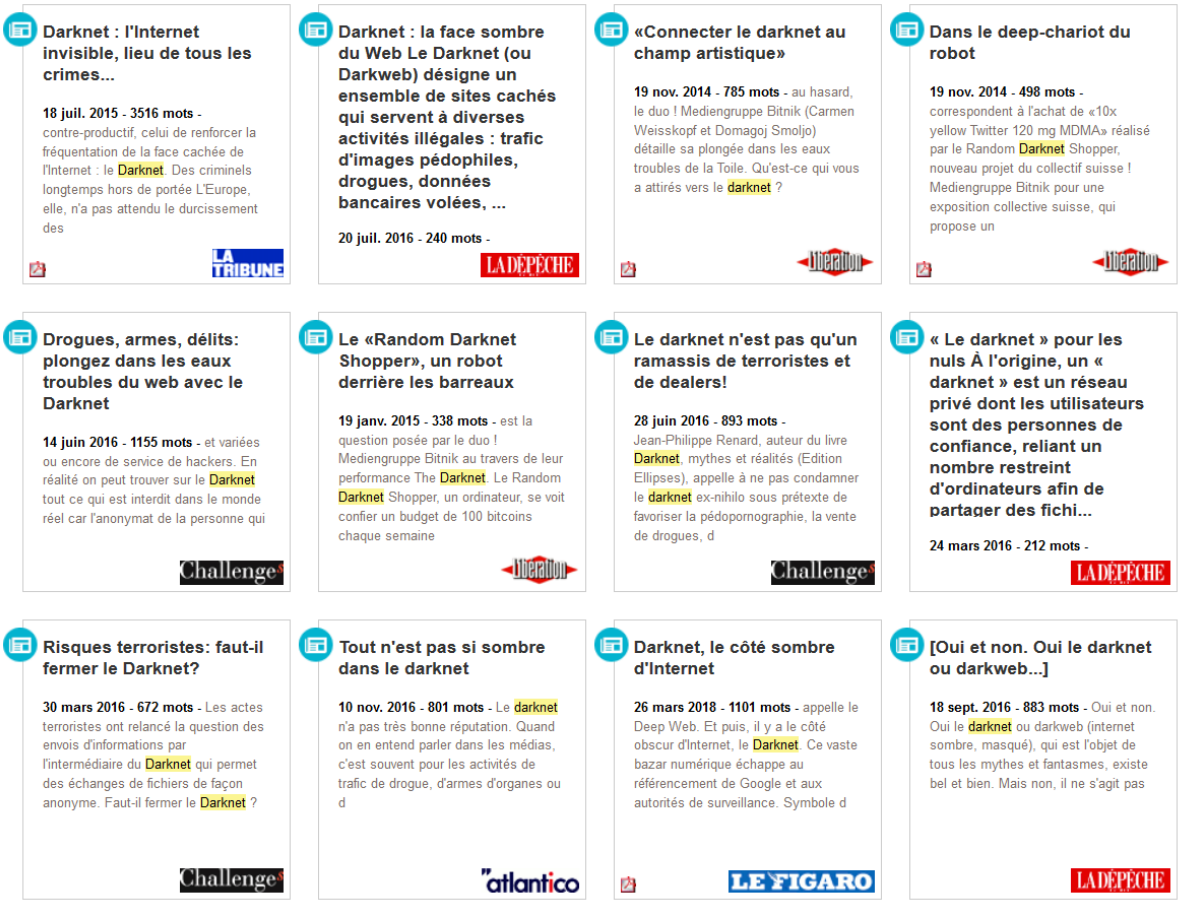
« Descente dans le « dark Web ». Les initiés y achètent drogues, armes, faux papier, films nécrophiles ou pédophiles, livres de cuisine anthropophagique[1]... »

Le Darknet porterait-il bien son nom ? Serait-il un espace permettant de laisser libre cours aux aspects les plus sombres de l'âme humaine ? Avant de répondre à cette question, il convient de conduire une analyse objective de ce phénomène, par-delà les aspects sensationnalistes chers à la presse.

Afin de comprendre la richesse du Darknet, il nous faudra l'aborder sous différentes perspectives. La notion de *Darknet* est une notion d'informatique, et, à ce titre, elle renvoie à des procédés techniques qu'il nous conviendra d'éclaircir et de distinguer des procédés classiques employés sur Internet. En parcourant la littérature grand public consacrée au sujet, on ne peut que remarquer la confusion qui règne entre ***deep web***, ***dark web*** et *Darknet*. Pourtant, ces termes renvoient chacun à des réalités bien distinctes qu'il convient de définir rigoureusement. Cette approche technique et terminologique constituera la première partie de cet exposé.

Au-delà de la simple notion, le Darknet est une réalité tangible constituée d'outils, de logiciels, de programmes permettant d'y accéder et de l'utiliser. Ces outils indispensables au

[1] Marianne, « Plongée dans l'Internet criminel », publié le 10/05/2013, https://www.marianne.net/societe/plongee-dans-l-internet-criminel (consulté le 02/04/2018).



Le Darknet dans les médias, une présentation anxiogène frôlant la désinformation (premiers résultats d'une recherche avec le mot-clé « Darknet » sur Europresse).

fonctionnement du Darknet, nombreux, constituent *les darknets*. Loin de prétendre à l'exhaustivité, nous en présenterons les deux plus connus. Ce sera l'objet de notre deuxième partie.

Mais le Darknet ne saurait être réduit à ses aspects techniques : derrière tout terminal se trouve un individu relié à d'autres individus par sa connexion Internet. Le Darknet est donc par essence un *phénomène social* qu'il nous faudra analyser à travers les usages qui en sont faits et les motivations des internautes qui s'en servent. Ces analyses occuperont notre troisième partie.

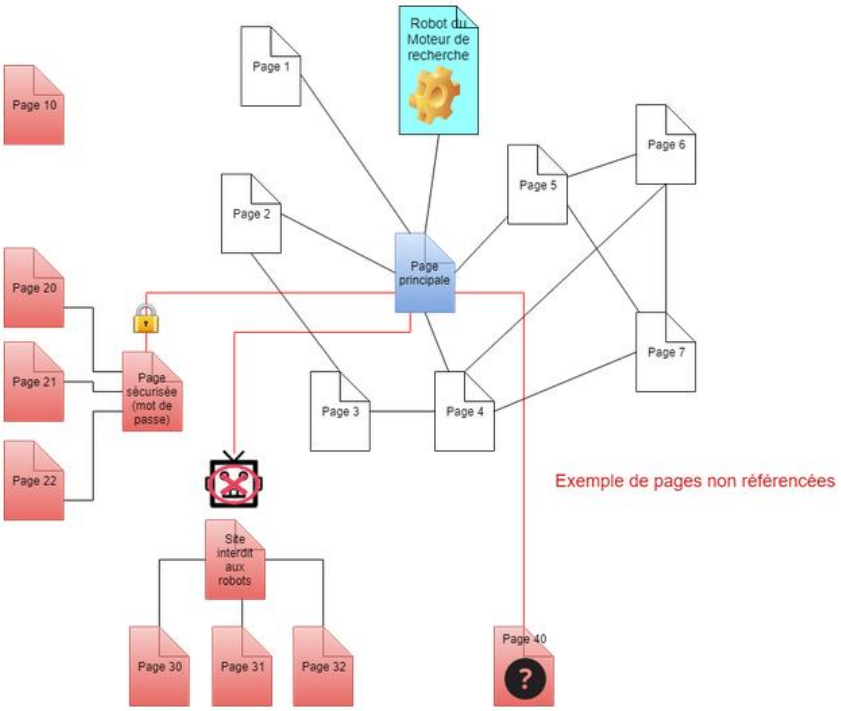
1) Qu'est-ce que le Darknet ?

a) Deep web, dark web et Darknet

Il est impossible de comprendre la nature du Darknet sans le distinguer du deep web et du dark web, avec lesquels il est trop souvent confondu. Si ces réalités se recouvrent partiellement, elles restent fondamentalement distinctes.

Le deep web désigne simplement les pages qui ne sont pas référencées par les **moteurs de recherche** traditionnels (*Google, Yahoo!, Bing* etc.). Il peut s'agir de données protégées par des mots de passe (clients e-mail, comptes bancaires…), d'informations configurées pour ne pouvoir être consultées que par certaines personnes (on pensera ici aux paramètres de confidentialité des réseaux sociaux), d'**intranets** ou encore de **bases de données**. Les informations contenues sur le deep web ne sont pas *dissimulées*, elles ne sont simplement pas *indexées* par les moteurs de recherche : il n'est d'ailleurs pas difficile d'y accéder et quiconque se rend sur le site de l'INSEE ou sur sa boîte mail surfe sur le deep web. La majorité des internautes utilisant le **web** via le filtre des moteurs de recherche, le deep web leur reste inaccessible, sauf s'ils utilisent d'autres moyens[2] pour accéder à l'information.

[2] Il s'agit ici simplement d'accéder à l'information sans passer par un moteur de recherche. Ainsi, se connecter à son client e-mail (*Thunderbird* par exemple) ou entrer une **URL** directement dans la barre d'adresse du **navigateur** sont des moyens alternatifs d'accès à l'information.



Pages référencées et non référencées (appartenant au deep web) à partir d'une demande sur un moteur de recherche.

© www.culture-informatique.net

Le deep web s'oppose ainsi au **web de surface**[3], la partie du web indexée par les moteurs de recherche traditionnels. On peut donc raisonnablement douter du sérieux et de l'honnêteté intellectuelle de nombreux articles, parfois publiés sur des plateformes *a priori* dignes de confiance[4], décrivant le deep web comme un repaire de criminels en tout genre. Le deep web n'est ni illégal, ni immoral, ni difficile d'accès, ni chiffré : il est simplement une couche du web ne répondant pas aux critères de **référencement**[5]. Les raisons en sont diverses : aucun **hyperlien** ne renvoyant vers la page, accès protégé par un mot de passe, **contenus dynamiques**[6], pages incompréhensibles pour les robots ou encore demande explicite des administrateurs du site de ne pas référencer celui-ci (l'équivalent web de la décision de faire mettre son numéro de téléphone sur liste rouge).

Si la taille du web indexable est considérable[7], elle ne représente cependant qu'une petite portion du World Wide Web, puisque celui-ci comprend également l'ensemble des pages et sites non référencés constituant le deep web. L'étude de référence comparant l'envergure du surface web et celle du deep web a été publiée par Michael K. Bergman[8], et, bien qu'elle date un peu, elle est encore admise comme faisant autorité par les spécialistes du domaine. D'après cet article, le deep web serait *500 fois plus gros* que le web indexable[9]. Ainsi, l'image de l'iceberg souvent utilisée pour représenter le rapport entre le surface web et le deep web, bien

[3] Cf. Michael K. Bergman, « The Deep Web : Surfacing Hidden Value », 24/09/2001, https://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf (consulté le 16/04/2018).
[4] Le site web de l'*European Communication School* par exemple, dont le titre d'un article sur le sujet laisse déjà rêveur : https://ecs-digital.com/culture/deep-web-la-face-cachee-dinternet-ou-comment-recevoir-un-kilo-de-cocaine-par-la-poste/ (consulté le 16/04/2018).
[5] https://toiledefond.net/referencement-internet/ (consulté le 16/04/2016).
[6] Les contenus dynamiques sont des contenus web générés à la demande, c'est-à-dire qu'ils prennent en compte des **métadonnées** (heure, date, localisation de l'internaute…) avant d'afficher la page. Cela signifie que les données affichées peuvent varier selon divers facteurs. La recherche d'un trajet en train sur le site de la SNCF est un exemple de contenu dynamique. Il s'oppose au contenu statique.
[7] Une estimation précise est par définition difficile à obtenir. Les spécialistes s'accordent sur plusieurs milliards de pages web indexables. Voir par exemple http://www.worldwidewebsize.com/ ou encore http://alessiosignorini.com/articles/indexable-web-size/paper.pdf (pages consultées le 16/04/2018). Le nombre de pages web augmente de façon exponentielle.
[8] Michael K. Bergman, *op. cit.*, https://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf (consulté le 16/04/2018).
[9] *Ibid.*, p. 5.

L’image de l’iceberg est souvent utilisée pour représenter le rapport entre surface web et deep web. Bien qu’elle soit intéressante, elle sous-estime la taille réelle du deep web.

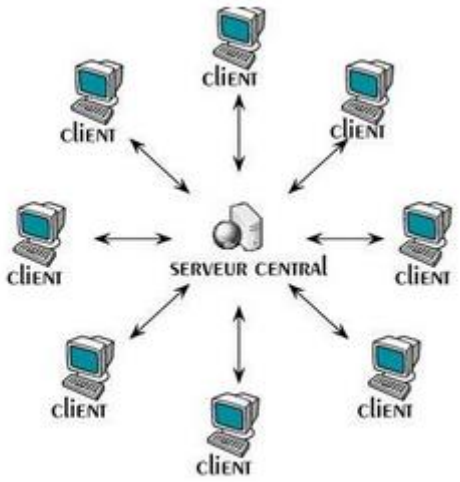
qu'elle soit évocatrice, est erronée : il faudrait que la partie immergée soit 500 fois plus importante que le partie émergé.

Le Darknet[10] appartient en partie au deep web, dans la mesure où il n'est pas référencé par les moteurs de recherche traditionnels. Cependant, il s'en distingue par les **protocoles** qu'il intègre nativement. Il convient de préciser que le Darknet ne constitue aucunement une infrastructure séparée d'Internet, car il utilise les protocoles essentiels au fonctionnement de ce dernier : les protocoles **TCP/IP**[11]. Le Darknet n'est pas un réseau unique, comme pourrait le laisser penser l'utilisation récurrente de l'article défini. Il s'agit bien plutôt d'un ensemble de réseaux qui, en vertu de certaines caractéristiques communes et malgré les différences qu'ils présentent, peuvent tous être désignés comme des darknets[12]. Quelles sont donc ces caractéristiques ? Un darknet nécessite :

- l'existence de l'infrastructure Internet (TCP/IP), qu'il utilise ;
- un protocole spécifique permettant l'instauration d'un **réseau superposé** ;
- une **architecture décentralisée** de type **pair-à-pair** ;
- l'intégration de processus d'anonymisation.

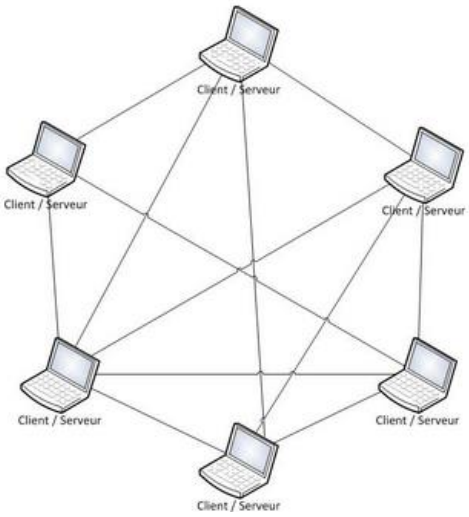
Tout darknet utilise l'infrastructure Internet, mais s'en distingue par la création d'un réseau superposé grâce à un protocole qui lui est spécifique : le réseau superposé s'appuie sur l'infrastructure sous-jacente tout en intégrant des fonctions qui lui sont propres[13]. Un réseau de type darknet répond à un langage spécifique et forme une réalité hermétique : aucune communication ne peut avoir lieu entre un darknet et un autre. En revanche, les ordinateurs

[10] Nous utilisons *Darknet* avec une majuscule pour désigner l'ensemble des darknets, de la même manière qu'on utilise *Internet* pour désigner l'ensemble des réseaux reliés entre eux.
[11] *Internet Protocol* (IP) et *Transmission Control Protocol* (TCP) sont les deux protocoles de base sur lesquels repose Internet. Le protocole de réseau IP permet le transfert de **paquets** (données découpées) entre des ordinateurs connectés. Pour ce faire, chaque équipement se voit attribuer une adresse IP unique (suite de quatre nombres entiers séparés par des points, par exemple 193.43.55.67). Les paquets transitant par différents chemins, il faut pouvoir s'assurer que l'information a bien été intégralement reconstituée à l'arrivée. C'est la fonction du protocole de transport TCP : il gère la correction et l'ordre des paquets. C'est l'adresse IP qui permet d'identifier l'internaute. Elle contient de nombreuses informations, comme on peut le voir ici : http://www.mon-ip.com/.
[12] Nous en présenterons quelques-uns dans notre deuxième partie.
[13] Internet est lui-même superposé au réseau téléphonique.



Architecture de type client-serveur.

© Télécom Lille



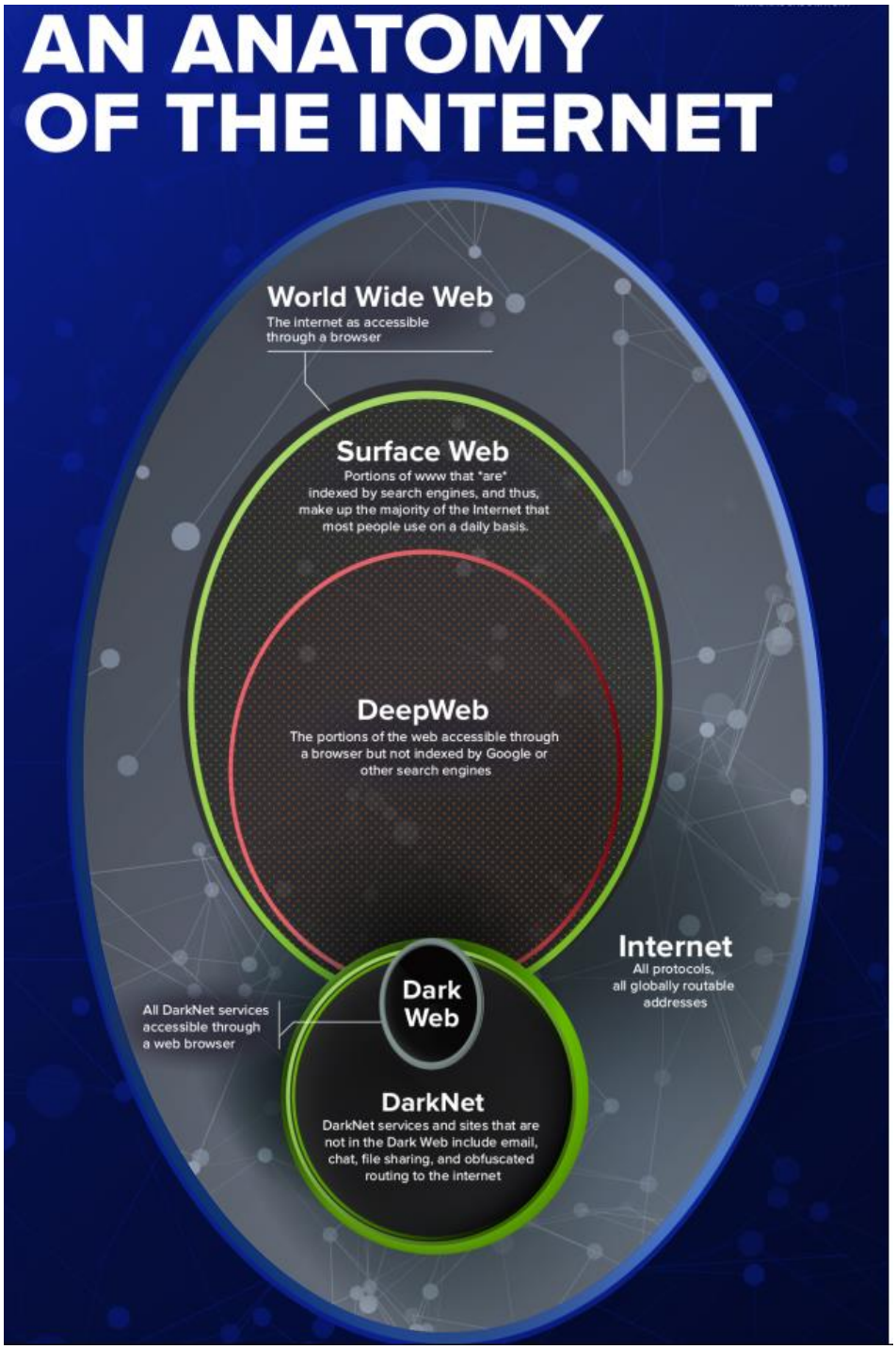
Architecture pair-à-pair décentralisée.

© Télécom Lille

reliés au sein de ce réseau superposé peuvent bien entendu échanger des informations, sans quoi on ne pourrait pas parler de réseau.

Les darknets fonctionnent selon une architecture décentralisée de type pair-à-pair. La majorité des échanges d'informations sur Internet s'effectuent grâce à une **architecture client-serveur**. Un logiciel client, installé sur un ordinateur client (le plus souvent de type ordinateur personnel) va faire une requête auprès d'un logiciel serveur (installé sur un ordinateur beaucoup plus puissant qu'un ordinateur personnel et dont l'ensemble de la mémoire de calcul est dédié à cette activité). Le serveur qui héberge l'information requise répond ensuite au client, ce qui permet à ce dernier d'accéder aux données recherchées. Le langage **HTTP** (*Hypertext Transfer Protocol*) est le langage dans lequel échangent un client et un serveur sur le web. La puissance de calcul d'un serveur lui permet de répondre à de nombreux clients en même temps[14]. L'architecture client-serveur est dite **centralisée**, car l'information est stockée à un endroit bien précis (sur le serveur), et les clients désirant accéder à cette information devront tous interroger le même serveur. L'architecture pair-à-pair, quant à elle, permet à n'importe quel client de devenir serveur, c'est-à-dire d'héberger des données ou de renvoyer les clients vers l'hébergeur. Elle peut néanmoins être centralisée, dans la mesure où, pour accéder aux données situées sur un ordinateur, le client qui est à l'origine de la requête devra en premier lieu interroger un serveur qui le redirigera ensuite vers l'ordinateur en question[15]. En revanche, dans le cas du pair-à-pair décentralisé sur lequel reposent les darknets, les clients (qui peuvent toujours devenir des serveurs) ne communiquent qu'avec des clients (des pairs) devenant serveurs pour renvoyer l'information ou transmettre la requête à l'ordinateur censé héberger l'information. L'information n'est plus centralisée sur un serveur unique, mais est disséminée (voire dupliquée) sur de nombreux ordinateurs, ce qui rend ainsi l'ensemble du système plus robuste[16].

[14] Cette puissance est cependant limitée. C'est ce qu'exploitent les **attaques de type déni de service** (DoS), qui inondent les serveurs de requêtes, provoquant un arrêt du serveur et rendant les services qu'il héberge inaccessibles.
[15] Le célèbre protocole d'échange de fichiers **BitTorrent** utilise ce type d'architecture.
[16] Il est déjà possible d'entrevoir l'intérêt d'une telle architecture pour l'accès à l'information. Nous en verrons une application concrète en étudiant Freenet.



Deep web, dark web et Darknet, des réalités distinctes.

Enfin, les darknets intègrent une fonction d'anonymisation de l'utilisateur. Cette propriété leur est consubstantielle, et c'est d'elle qu'ils tirent leur dénomination. Leur fonction essentielle est la **confidentialité** des échanges et la préservation de l'**anonymat**. Ces termes ne sont pas interchangeables et il est crucial de les distinguer afin de saisir la nature des darknets. L'anonymat est la dissimulation de l'identité. Nous avons vu que l'adresse IP permettait l'identification de l'internaute : les darknets rendent cette identification sinon impossible, du moins très difficile[17]. La confidentialité consiste quant à elle à empêcher une tierce personne d'accéder à l'information échangée. Dans le cas d'un échange d'e-mails, je pourrai prétendre à la confidentialité si je suis certain que le *contenu* des e-mails ne pourra être lu que par mon correspondant. Mais l'échange ne sera anonyme que si *l'origine* des e-mails est dissimulée. Il est donc possible d'être anonyme sans échanger de données confidentielles ou de chiffrer le contenu de ses communications sans dissimuler son identité[18]. Les darknets sont des outils de protection de l'anonymat et de la confidentialité en ligne. Avant d'en expliquer le fonctionnement, il nous reste un concept à éclaircir : celui de dark web.

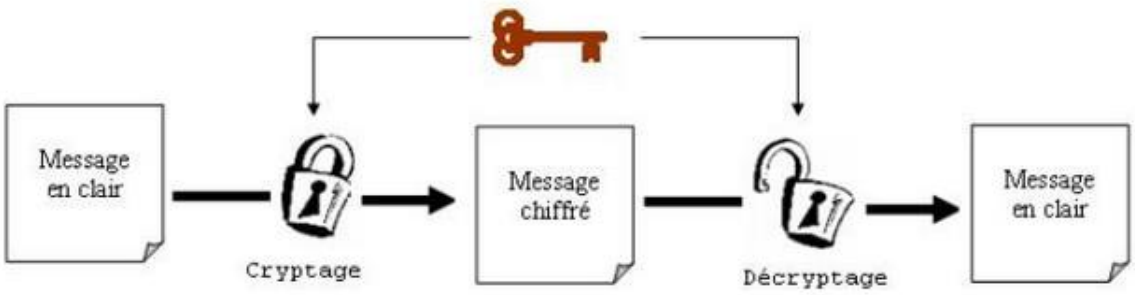
Tout comme le World Wide Web ne saurait être identifié à Internet (il n'en est qu'une couche applicative), le Darknet ne saurait se résumer au dark web. En effet, de nombreuses applications constituent des darknets sans appartenir au web : le logiciel **Retroshare** ou le service d'e-mail Mailpile sont des darknets, au sens où ils intègrent des fonctions de chiffrement des transmissions et d'anonymisation de l'utilisateur, mais ils n'appartiennent pas au dark web, qui désigne tout simplement l'ensemble des sites d'un darknet donné[19] auxquels il est possible d'accéder grâce à un navigateur.

---

[17] Tout est une question de moyens. La **NSA** (National Security Agency), l'agence de renseignements américaine, peut se targuer de nombreuses réussites dans son effort pour affaiblir les logiciels de chiffrement et d'anonymisation. Sa technique de prédilection est l'installation de **portes dérobées** dans les logiciels, ce qui lui permet de contourner les moyens de défense mis en place par l'internaute. Voir par exemple https://arstechnica.com/information-technology/2013/09/nsa-attains-the-holy-grail-of-spying-decodes-vast-swaths-of-internet-traffic/ et https://arstechnica.com/information-technology/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ (consultés le 16/04/2018).

[18] L'application Telegram, principale concurrente de Whatsapp, intègre une clé de chiffrement permettant d'échanger de manière confidentielle sans dissimuler pour autant l'identité des interlocuteurs. https://www.lci.fr/high-tech/comment-fonctionne-telegram-la-messagerie-cryptee-preferee-des-jihadistes-terroristes-2066909.html (consulté le 16/04/2018).

[19] Par exemple, l'ensemble des adresses en .onion constitue le dark web de **Tor**.



Cryptographie symétrique : la même clé permet de chiffrer et de déchiffrer le message.

Source : Steemit

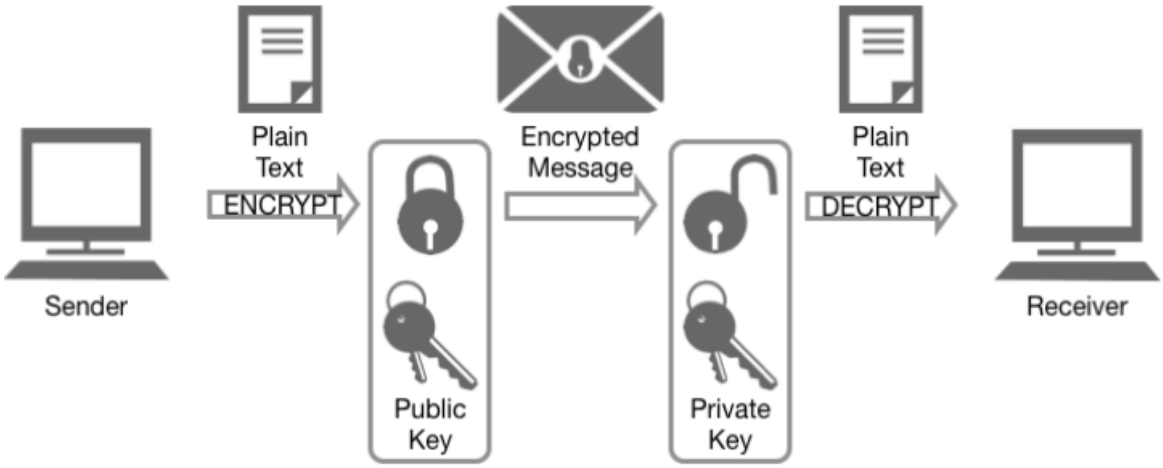
b) Darknet et cryptographie : les mixnets

Nous l'avons souligné : la caractéristique essentielle d'un darknet est l'anonymisation et la confidentialité des échanges. Pour parvenir à cette fin, les darknets utilisent le chiffrement des données, rendant celles-ci inutilisables par une tierce personne. Comment fonctionne ce chiffrement ? Pour le saisir, il nous faut aborder quelques éléments de **cryptographie**.

La cryptographie est une technique consistant à rendre un message inintelligible afin d'en protéger le contenu. Les méthodes cryptographiques sont aussi nombreuses qu'anciennes[20] et nous ne nous intéresserons ici qu'à deux d'entre elles, largement usitées en informatique et en particulier par les darknets : la **cryptographie symétrique** et la **cryptographie asymétrique**[21].

La cryptographie symétrique se développe dans les années 1970 afin d'assurer aux banques et aux entreprises des moyens de communication sécurisés. Elle a depuis été perfectionnée, et sa version la plus aboutie, **AES** (*Advanced Encryption Standard*), est encore utilisée aujourd'hui. La cryptographie symétrique consiste à chiffrer un message via une clé, cette même clé permettant également le déchiffrement du message. La clé doit donc être connue non seulement par l'expéditeur, mais également par le destinataire. Cet échange de clé rend l'opération risquée, car si une tierce personne parvenait à intercepter cette clé lors de l'échange, le chiffrement ne serait plus d'aucune utilité. En outre, il est nécessaire de créer une clé suffisamment complexe pour résister à la puissance de calcul des ordinateurs actuels[22].

[20] Le chiffre de César fait partie des plus anciennes techniques de cryptographie connues. Cette technique dite de substitution consiste à remplacer chaque lettre du message par une autre lettre en progressant dans l'alphabet selon une clé déterminée à l'avance. On reprend à la lettre a une fois l'alphabet épuisé. Pour une clé équivalente à quatre, A deviendra E, B deviendra F etc. Selon cette clé, « cryptographie » deviendrait « gvctxskvetlmi ».
[21] Également appelées respectivement chiffrement à clé secrète et chiffrement à clé publique.
[22] Le **DES** (*Data Encryption Standard*, ancêtre du AES) développé par Horst Feistel dans les années 1970 utilisait à l'origine une clé de 128 bits. Mais la NSA, trouvant ce format trop sécurisé, imposa un format de 56 bits. La différence en matière de sécurité est considérable : « Si vous pouvez tester un milliard de clés par seconde, il vous faudra environ 70 millions de secondes, soit un peu plus de deux ans, pour tester toutes les clés de 56 bits. Dans la même configuration, avec une clé de 128 bits, il vous faudra environ 10^{22} fois plus longtemps, soit quelques milliards de fois l'âge de l'univers. » Jean-Philippe Rennard, *Darknet, mythes et réalités*, Paris, Ellipses, 2016, p. 32.



Cryptographie asymétrique : la clé publique sert à chiffrer le message, la clé privée permet de le déchiffrer.

© IBM

```
-----BEGIN PGP MESSAGE-----

hQEMA9JnCzrKYE8mAQgAs52ag3kU91FYm9c7TexAhBKgHk5/DQ1RjPZALj+ayXB5
X+tNhBKdwTWEwAPfyTa2H1C/iVZOEkmBV6Z7zsQUEXtfz/YMhiLIBgajV/o6pDmF
KPSU6rJthZJTStFVkION6/0bXor2zJvOdObUye8bRNCC/EXhfPkfdz5TqmigKoIG
Zfbe7xcq5w/kq2DGuzsJx/QRdVnH2B6EkFBn9elGQl/ZXgUaiKPCSYCQqZhgjog6
4vwM79l0YVPcZ/w3pJK6P/6bF2cdjXHoyD5zcDGp4Kzl2B5tgJqUSFbl6gbMBzB1
lqFkCoTEf5rPYBTeNx+m2wDmPHX4B4ITDAHcAHr3mtJCAdqy/hmo9akyP7hMiw4R
LSy9BJgye2F/Drs3kvKwgeLLIO/+S7o7ZJiTjHC4Ec/+W4skpTRVaDMHW74WfkFp
hL1i
=w4xl
-----END PGP MESSAGE-----
```

Ci-dessus le mot « darknet » après chiffrement sur GPA, un logiciel utilisant la cryptographie asymétrique.

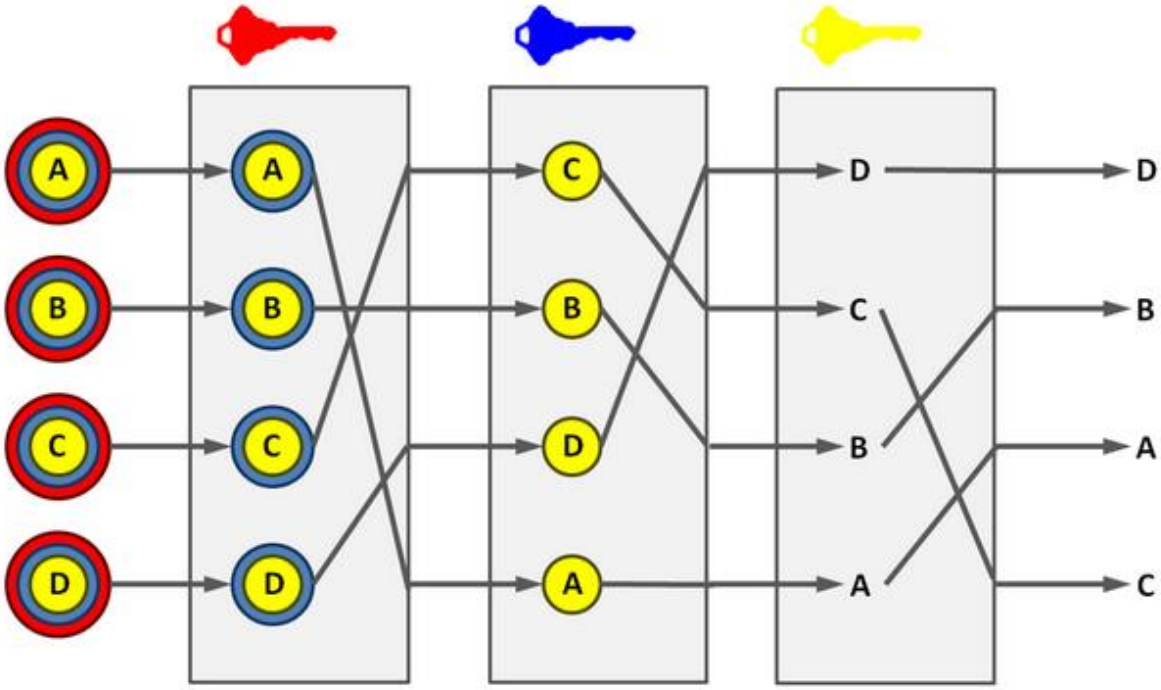
Cette technique cryptographique présente cependant l'avantage de la légèreté et permet donc des échanges plus rapides, c'est la raison principale pour laquelle elle est aujourd'hui encore largement répandue sur Internet.

La cryptographie asymétrique s'est développée en réaction aux faiblesses de l'algorithme DES dans sa version 56 bits[23]. En 1976, Whitfield Diffie et Martin Hellman proposent de découper la clé en deux parties, dont l'une serait publique et l'autre privée. Admettons que Bob et Alice veuillent communiquer. Alice crée une clé scindée en deux parties. Elle diffuse la clé publique afin que Bob (mais pas seulement[24]) puisse l'utiliser et conserve la clé privée dans un endroit sécurisé[25]. Bob utilisera la clé publique d'Alice pour chiffrer le message qu'il désire lui envoyer et Alice utilisera sa clé privée pour déchiffrer le message de Bob. En plus de permettre des échanges confidentiels sans avoir à échanger une clé secrète, cette technique de chiffrement présente un avantage supplémentaire : si la clé privée peut déchiffrer un message chiffré avec la clé publique, l'inverse est également vrai. Cette propriété permet l'authentification de l'émetteur par le destinataire en ajoutant une couche de chiffrement supplémentaire. Si Bob possède lui-même une clé, il lui suffira de chiffrer son message avec sa propre clé privée, puis avec la clé publique d'Alice (double chiffrement). À la réception, Alice devra dans un premier temps utiliser sa clé privée (déchiffrement de la première couche) puis utiliser la clé publique de Bob, ce qui lui permettra de s'assurer que Bob est bien à l'origine du message (Bob étant le seul à pouvoir utiliser sa clé privée).

Les darknets reposent principalement sur la cryptographie asymétrique : ils intègrent des algorithmes permettant de générer automatiquement des clés de session[26] aléatoires qui assurent la confidentialité de la communication. Cependant, confidentialité ne signifie pas anonymat, et l'objectif des darknets est précisément de combiner ces deux aspects de la protection de la vie privée.

---

[23] Pour une présentation détaillée de l'histoire et de l'évolution de la cryptographie moderne, voir notamment Laurent Gayard, *Géopolitique du Darknet*, ISTE Éditions, Paris, 2018, p. 69 et ss.
[24] Toute personne désirant communiquer de manière confidentielle avec Alice pourra utiliser cette clé publique.
[25] L'idéal étant de protéger l'accès à cette clé par un mot de passe.
[26] Une clé de session est une clé qui n'est utilisée que durant la connexion actuelle. Une nouvelle clé est générée à chaque nouvelle communication.



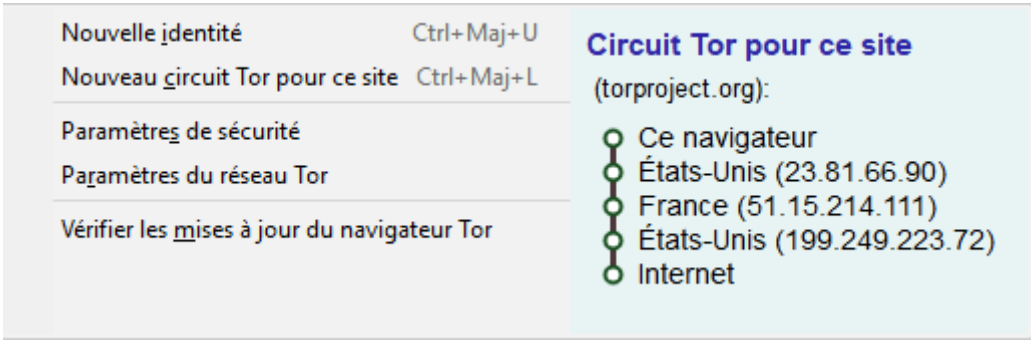
Représentation d'un mix network (ou mixnet) comprenant trois relais. Les couches de chiffrement sont représentées par différentes couleurs que les clés de couleur correspondante permettent de déchiffrer. Les flèches représentent le chemin aléatoire emprunté par le message.

Source : Wikipedia

Pour ce faire, les darknets intègrent une autre fonctionnalité : les relais, rendus possibles par une structure de type **mix network**. En 1981, David Chaum publie un article fondateur[27], dans lequel il dévoile un système permettant de garantir la confidentialité et l'anonymat. La confidentialité des échanges est assurée par un chiffrement à clé publique. L'introduction d'un mix network (ou mixnet) permet quant à elle d'anonymiser les communications. Le fonctionnement d'un mix network est assez simple : au lieu d'une communication directe entre deux ordinateurs (client-serveur), les informations vont transiter par des relais, des ordinateurs intermédiaires. Afin de garantir l'anonymat, chaque relais connaît seulement l'identité[28] de son prédécesseur et de son successeur. Ainsi, si je transite par trois relais A, B et C, seul le relais A aura accès à mon adresse IP, le relais B n'ayant accès qu'aux adresses de A et de C, et le relais C ne connaîtra que les adresses de B et du destinataire final. Le destinataire final, à qui nous voulions dissimuler notre identité en premier lieu, ne connaîtra que l'identité du dernier relais, le relais C. Afin d'assurer la transmission et la confidentialité de la communication, l'information est protégée par plusieurs couches de chiffrement. Le nombre de couches est fonction du nombre de relais[29] : en effet, afin de garantir la confidentialité de l'échange, les relais ne doivent pas pouvoir prendre connaissance du contenu du message, qui est réservé au destinataire. Admettons que Bob utilise un mix network composé de trois relais pour communiquer avec Alice. L'information sera donc chiffrée de la manière suivante : l'ordinateur de Bob utilise la clé publique d'Alice pour créer une première couche de chiffrement. Le message chiffré est ensuite chiffré une deuxième fois avec la clé publique du relais C, puis avec la clé publique du relais B et, enfin, avec la clé publique du relais A. À la réception du message, le relais A déchiffre la première couche avec sa clé privée, puis transmet le message à B qui déchiffre la deuxième couche. Lorsque le dernier relais, C, transmet le message à Alice, celui-ci n'est plus protégé que par une couche de chiffrement, qu'Alice pourra décrypter grâce à sa clé privée.

[27] « Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms », disponible sur https://www.freehaven.net/anonbib/cache/chaum-mix.pdf (consulté le 18/04/2018).
[28] C'est-à-dire l'adresse IP.
[29] Le nombre de relais peut être configuré. L'augmenter permet de renforcer l'anonymat, le diminuer permet d'augmenter la vitesse de communication. L'internaute effectue donc un arbitrage selon ses priorités.

Page d'accueil du navigateur Tor.



Un circuit Tor (les trois adresses IP intermédiaires sont les relais).

Les mixnets, qui permettent d'assurer à la fois la confidentialité et l'anonymat des échanges, constituent la structure de base sur laquelle reposent les darknets. Si ces derniers ont chacun leur particularité, comme nous allons le voir, ils intègrent tous, d'une manière ou d'une autre, des relais et des algorithmes de chiffrement à clé publique.

2) Les outils du Darknet

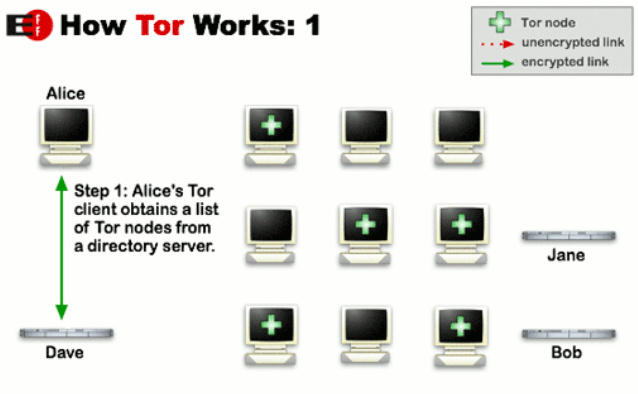
Comme nous l'avons souligné, le Darknet n'existe pas plus que l'Homme, il n'est qu'une dénomination commode permettant de regrouper différents darknets existants. L'accès à un darknet est rendu possible par des outils (logiciels) : ces logiciels sont des points d'entrée. Ne pouvant prétendre à l'exhaustivité, notre propos se limitera aux classiques : Tor et **Freenet**.

a) Tor

Tor (acronyme de *The Onion Router*) est le darknet le plus célèbre et celui qui a fait la réputation sulfureuse de cet espace numérique. Si le principe de Tor, le routage en oignon, est développé dès 1996[30] par des chercheurs de la *Naval Research Laboratory* (NRL) dans le but de chiffrer et d'anonymiser les communications militaires[31], sa première version ne voit le jour que six ans plus tard, en 2002. En 2004, la NRL décide d'arrêter le financement de Tor et publie son code source ; il est alors récupéré par l'***Electronic Frontier Foundation***[32] (EFF) et devient *The Tor Project*[33].

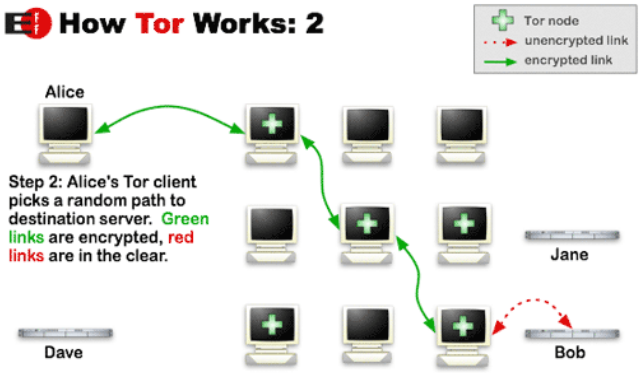
Le routage en oignon repose sur le principe de mixnet développé par David Chaum. Au lieu d'établir une connexion directe entre le client et le service recherché, Tor dissimule le trafic via un ensemble de relais (ou **nœuds**). L'ensemble des relais de Tor est renseigné dans un annuaire librement consultable[34], le fournisseur d'accès à Internet peut donc aisément repérer

[30] Cf. David M. Goldschlag *et al.*, « Hiding Routing Information », *Workshop on Information Hiding*, Cambridge, 1996, disponible sur https://pdfs.semanticscholar.org/9610/11a97535f89d386f81926335bdd8196ff300.pdf (consulté le 18/04/2018).
[31] Dans l'imaginaire collectif, Tor ne peut être que l'œuvre de geeks anarchistes. Pourtant, rien n'est plus faux : Tor est avant tout un projet militaire développé par la marine américaine.
[32] L'EFF est une ONG américaine de défense des droits et libertés numériques : https://www.eff.org/.
[33] https://www.torproject.org/.
[34] https://metrics.torproject.org/rs.html#toprelays (consulté le 18/04/2018).



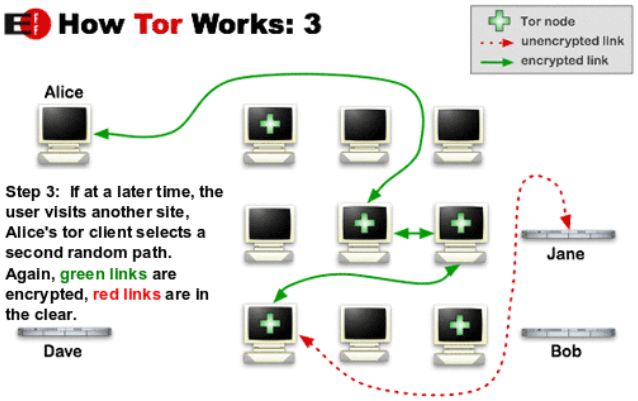
Afin d'établir un circuit Tor, le client utilise la liste des nœuds disponibles.

© The Tor Project



Le client détermine ensuite aléatoirement un chemin.

© The Tor Project



Le circuit Tor est modifié toutes les dix minutes.

© The Tor Project

les clients qui utilisent ce réseau[35] : on peut ainsi savoir qu'un internaute utilise Tor, bien qu'on ne puisse savoir ce qu'il y fait. L'établissement d'un circuit Tor se fait en plusieurs étapes : le client utilise l'annuaire des relais pour sélectionner un relais d'entrée dans le réseau, à partir duquel le réseau sera ensuite élargi à un deuxième relais, puis à un troisième. Un circuit Tor est ainsi composé d'un relais d'entrée, d'un relais intermédiaire et d'un relais de sortie. Le relais de sortie se connecte enfin au serveur de destination. Ce circuit est déterminé par l'ordinateur client de manière aléatoire et change toutes les dix minutes environ[36].

Tor étant un mixnet, les paquets sont transmis avec plusieurs couches de chiffrement. Après avoir déterminé un circuit, le client utilise la clé publique des différents relais pour chiffrer les données. Le paquet est ensuite progressivement déchiffré, couche après couche, au cours de son passage par les différents relais : c'est la raison pour laquelle on parle de routage en oignon. Chaque relais ne connaissant que son prédécesseur et son successeur immédiat, l'anonymat de l'utilisateur est garanti[37]. Le serveur de destination ne connaît quant à lui que l'adresse du relais de sortie.

Le navigateur Tor permet d'accéder à n'importe quel site sur le web : il permet de faire des achats sur *Amazon*, d'aller consulter ses courriels ou encore de regarder des vidéos sur *YouTube*. Dans ce cas, les données transitant du dernier relais au serveur de destination ne sont pas chiffrées : en effet, en se connectant à des sites du **Clearnet**[38], on sort de l'environnement Tor, et les paquets d'informations ne sont alors plus protégés par celui-ci. Tor ne peut imposer le chiffrement à des serveurs se trouvant en dehors de son réseau. Ainsi, se connecter à un service utilisant un simple protocole HTTP et y entrer son mot de passe revient à s'exposer à

[35] Notons ici que si l'utilisation de Tor n'est aucunement répréhensible, elle peut en revanche éveiller des soupçons.
[36] « *For efficiency, the Tor software uses the same circuit for connections that happen within the same ten minutes or so. Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones*. » https://www.torproject.org/about/overview.html (consulté le 19/04/2018).
[37] L'adresse IP de l'internaute n'est connue que par le relais d'entrée.
[38] C'est-à-dire au réseau non chiffré, donc non confidentiel. Cf. Laurent Gayard, *op. cit.*, p. 126-127 et Jean-Philippe Rennard, *op. cit.*, p. 163.

une potentielle récupération des données par une personne mal intentionnée, que l'on utilise le navigateur Tor, Firefox ou Internet Explorer[39].

Tor permet également de proposer des services (des sites web par exemple) en dissimulant l'adresse IP du serveur : les **services oignon**[40]. L'adresse de ces sites, souvent impossible à mémoriser, se compose de 16 lettres et chiffres suivis du nom de domaine *.onion*[41]. L'anonymisation du serveur fonctionne exactement comme celle du client : le serveur détermine aléatoirement différents chemins d'accès constitués de relais. Le client et le serveur n'étant chacun visible que par leur troisième relais, leur anonymat respectif est garanti. Lors de la connexion à un service oignon, le chiffrement est effectif de bout en bout : le client et le serveur hébergé sur le réseau Tor communiquent via un protocole de chiffrement asymétrique.

b) Freenet

Développé en 1999 par Ian Clarke, alors élève en informatique à l'Université d'Édimbourg, Freenet est le plus ancien darknet encore en usage aujourd'hui. Avec Freenet, Ian Clarke cherchait à réaliser un triple objectif : garantir l'anonymat à ceux qui produisent l'information et à ceux qui la consultent, donner la possibilité à ceux qui stockent l'information de nier en avoir connaissance et résister aux tentatives de tiers souhaitant limiter voire supprimer l'accès à l'information.

Freenet est un réseau pair-à-pair décentralisé dans lequel l'ensemble des nœuds[42] participe au stockage et à la diffusion des données. Bien que Freenet soit originellement destiné au partage de fichier, il intègre aujourd'hui d'autres fonctionnalités, notamment **Freemail**, qui permet d'avoir une boîte mail anonyme. L'architecture de Freenet est singulière : contrairement à Tor, qui gère ses propres relais[43], Freenet est constitué par les nœuds qui s'y connectent.

---

[39] Cependant, de nombreux sites (en particulier ceux des banques et des clients e-mail) intègrent maintenant le protocole **HTTPS** (*HyperText Transfer Protocol Secure*), qui chiffre les données.
[40] https://tb-manual.torproject.org/fr/onion-services.html (consulté le 19/04/2018).
[41] Par exemple, http://pjaopjqvjk6be4wz.onion.
[42] Chaque ordinateur connecté.
[43] Il est possible de configurer son ordinateur pour qu'il serve de relais Tor, mais la **bande passante** allouée est souvent trop faible pour réellement soutenir le réseau. C'est pourquoi Tor utilise des relais dédiés.

Page d'accueil de Freenet.

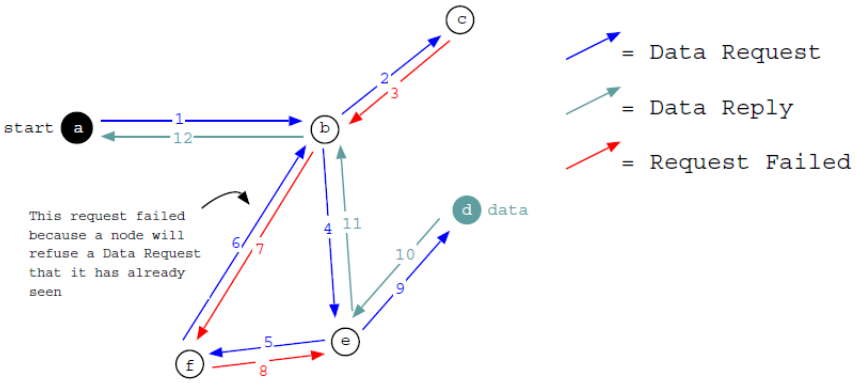
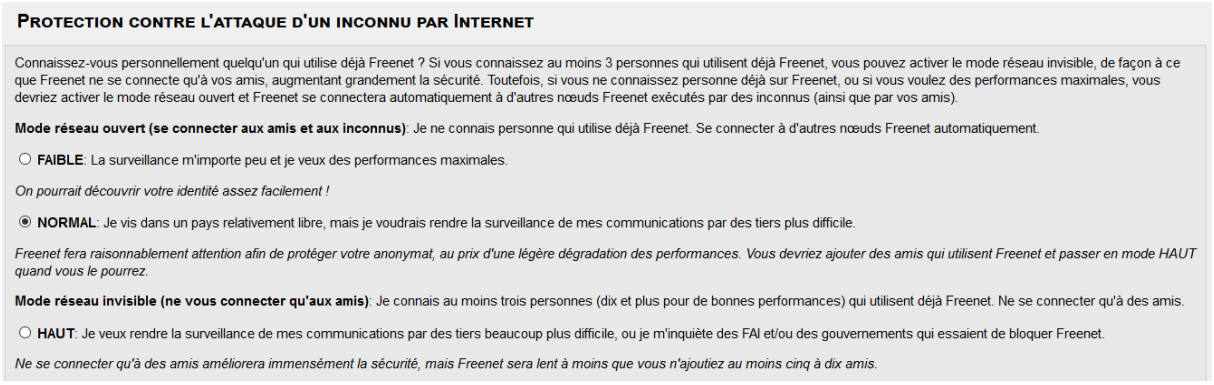


Illustration d'une requête de fichier sur Freenet. L'erreur numéro sept est due à la boucle effectuée par la requête.

Lorsqu'un ordinateur se connecte à Freenet, une partie de sa bande passante et de l'espace de stockage du **disque dur** lui seront désormais alloués[44]. L'ordinateur, devenu un nœud, servira à stocker et à diffuser certains fichiers, participant ainsi à l'architecture du réseau. Chaque nœud du réseau maintient une **table de routage**[45] qui contient une liste de clés et les identifiants des nœuds qui les stockent. Le **magasin**, situé sur le disque dur, contient des fichiers et les clés permettant de déchiffrer les données[46]. À chaque fichier correspond une clé permettant son identification. Lorsqu'un client souhaite récupérer du contenu, l'ordinateur commence par chercher la clé correspondante[47] et interroge sa table de routage afin de savoir si le fichier est stocké sur son propre nœud. Si ce n'est pas le cas, il transfère la requête au nœud environnant qui contient la clé la plus proche. La requête se poursuit de la sorte jusqu'à ce que le nœud contenant le fichier soit trouvé ou jusqu'à ce que le **nombre de sauts maximum**[48] soit atteint (un message d'échec est alors renvoyé au premier nœud). Lorsque le fichier est trouvé, il est envoyé au premier nœud en suivant le chemin de la requête en sens inverse. Chaque nœud participant au chemin de retour met le fichier en cache, c'est-à-dire qu'il en fait une copie sur son espace dédié. Ce procédé permet de soutenir l'architecture décentralisée de Freenet, puisque tout fichier chargé se retrouve stocké sur plusieurs nœuds, mais également de garantir le déni plausible des utilisateurs. En effet, les fichiers stockés sur un nœud sont non seulement chiffrés – ce qui empêche l'hébergeur de savoir quels fichiers sont stockés sur sa machine –, mais chaque nœud ayant participé à l'acheminement d'un fichier peut se présenter comme l'hébergeur, semant ainsi le doute quant à l'emplacement original du documen[49]. L'architecture de Freenet rend impossible toute éventuelle accusation de détenir des fichiers illégaux. Lorsque la limite de l'espace de stockage dédié à Freenet est atteinte, les fichiers les moins utilisés sont supprimés en premier, ce qui permet d'optimiser le réseau selon la demande.

[44] Ces paramètres sont évidemment configurables selon le type de connexion Internet de l'utilisateur et l'espace total disponible sur son disque dur.
[45] Cette table de routage, installée lors de la première utilisation de Freenet, permet d'acheminer des paquets vers leur destination.
[46] La confidentialité des échanges est assurée par un chiffrement asymétrique.
[47] Ce qui peut être fait grâce aux nombreux annuaires, comme *Nerdageddon*.
[48] Un saut désigne le passage d'une requête d'un nœud à un autre. Le nombre de sauts maximum est déterminé lors de la formulation de la requête.
[49] Il en va bien évidemment de même pour les pages web.



Les différentes configurations de Freenet, un arbitrage entre anonymat et performance.

L'anonymat est assuré de la même manière que sur Tor : chaque nœud ne connaît que son prédécesseur et son successeur. En outre, rien ne permet de différencier le nœud qui initie la requête et le nœud qui héberge le fichier. En transmettant des informations, un nœud ne peut donc jamais savoir s'il communique avec un nœud final ou de transfert.

Il convient de noter que Freenet peut être configuré de manière à assurer une protection quasiment absolue de la vie privée. Le mode réseau invisible[50] permet d'utiliser le réseau en sélectionnant uniquement les nœuds auxquels l'utilisateur fait confiance[51]. Ce mode reste cependant peu accessible au néophyte, puisqu'il faut renseigner soi-même les adresses des nœuds de confiance. En outre, ce mode augmente nécessairement la durée de chargement des pages, déjà importante sur Freenet[52].

3) Usages du Darknet

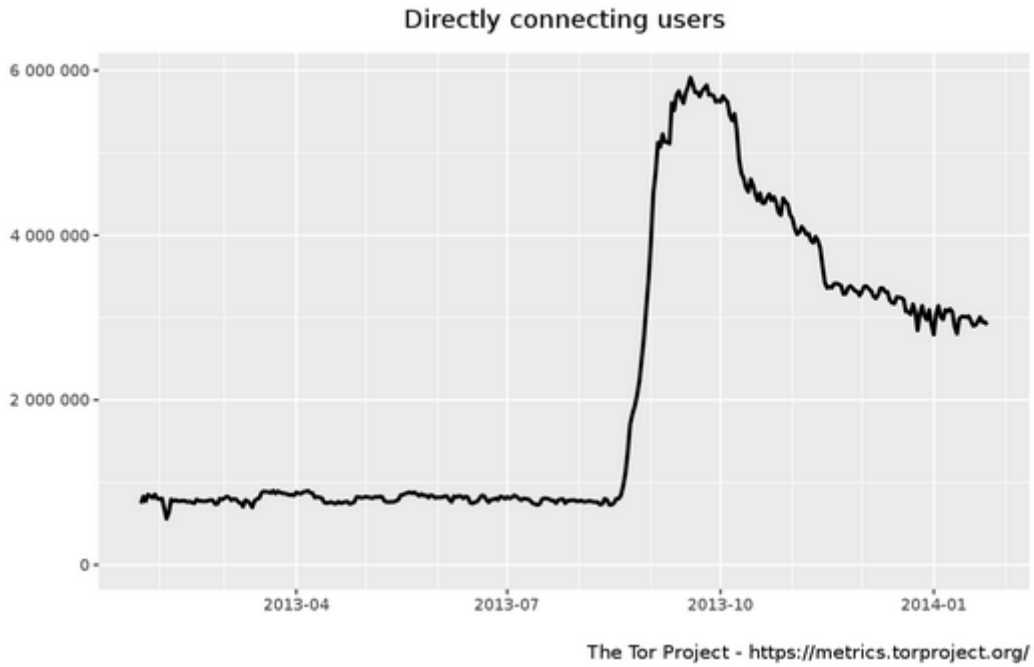
Les médias, friands de sensationnalisme, présentent souvent le Darknet[53] sous un jour défavorable : entre pédopornographie, trafic de stupéfiants et services de tueurs à gages, il ne serait qu'un repaire de malfrats. Qu'en est-il réellement ?

Il est bien évidemment difficile de recenser avec précision les usages du Darknet et de les quantifier puisque les différents darknets cherchent par définition à dissimuler leurs utilisateurs. Cependant, il est possible d'analyser le trafic d'un réseau donné sans pour autant compromettre l'anonymat des internautes, car l'analyse de bande passante ne permet pas à elle seule une identification.

Tor étant de loin le premier darknet en termes d'utilisation et de contenu, c'est sur ce réseau que nous avons choisi d'appuyer notre analyse[54]. Afin de conduire celle-ci avec probité, il convient de distinguer les usages du dark web et les usages du Darknet.

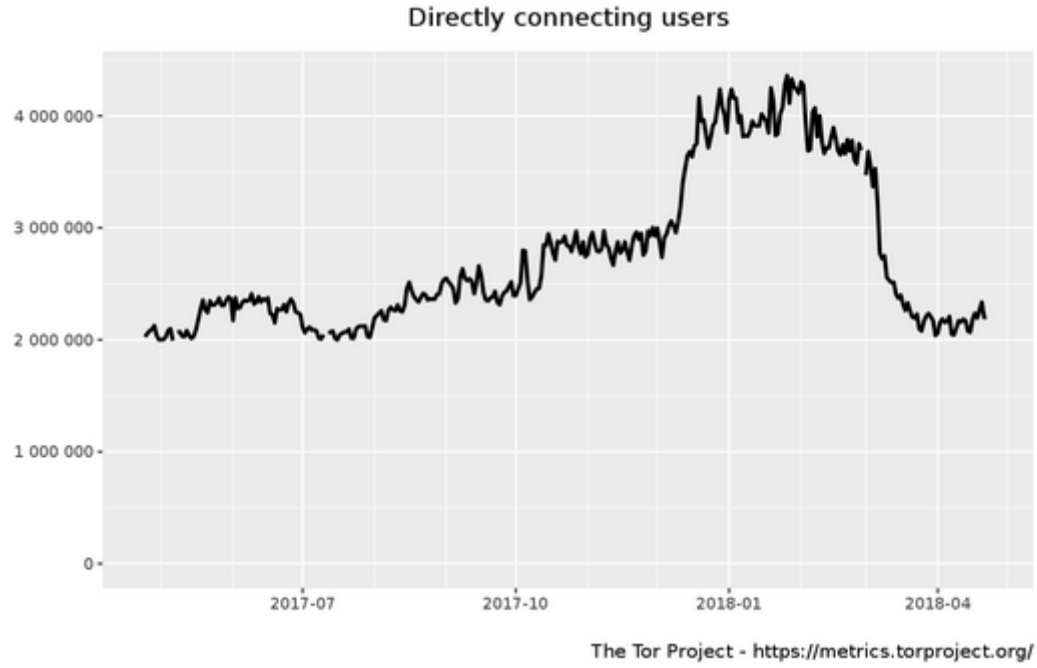
---

[50] Nommé *darknet mode* en anglais.
[51] Cette configuration est souvent appelée ***Friend-to-Friend*** (F2F), en référence à l'architecture pair-à-pair (*peer-to-peer*). Voir par exemple Jean-Philippe Rennard, *op. cit.*, p. 64.
[52] Il est parfois nécessaire d'attendre quelques minutes pour accéder à une page.
[53] Par *Darknet*, les journalistes désignent souvent le dark web, c'est-à-dire des sites et non du protocole.
[54] Qui ne saurait donc prétendre à l'exhaustivité.



Nombre d'utilisateurs quotidiens de Tor entre janvier 2013 et janvier 2014.
Le pic de valeur fait suite aux révélations Snowden, initiées au mois de juin.

© The Tor Project



Nombre d'utilisateurs quotidiens de Tor entre avril 2017 et avril 2018.

© The Tor Project

a) Usages du dark web

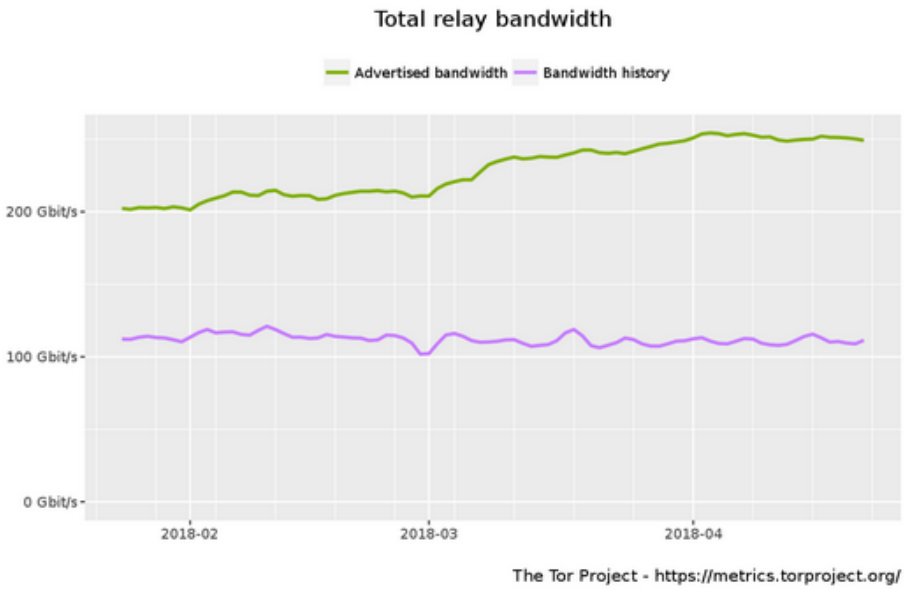
La fermeture de la plateforme Silk Road par le FBI en 2013[55] et les procédures judiciaires à l'encontre de son créateur et administrateur Ross Ulbricht[56], largement relayées par la presse, ont contribué à projeter le dark web sur le devant de la scène et à multiplier les discours alarmistes à son sujet[57]. À quoi s'adonnent donc les utilisateurs du web de Tor ?

Tor est de loin le darknet le plus utilisé : d'après *Tor Project*, entre deux et quatre millions d'internautes s'y connectent quotidiennement[58]. On est bien loin des 15 000 utilisateurs quotidiens estimés sur Freenet[59]. Les révélations d'Edward Snowden ont créé un engouement pour Tor : début 2013, le réseau comptait à peine un million d'utilisateurs ; à la fin de l'année, ce nombre avait été multiplié par quatre, après un bref pic à six millions d'utilisateurs.

Ces données concernent l'ensemble du darknet et ne se limitent pas à la couche applicative qu'est le dark web. En raison du chiffrement utilisé sur Tor, il est impossible de distinguer les personnes utilisant le navigateur Tor pour se rendre sur le dark web parmi les quelque deux millions d'utilisateurs quotidiens. Afin de distinguer ces usages, il faut utiliser une autre donnée statistique : l'analyse de la bande passante. En effet, le chiffrement des données n'empêche nullement d'en analyser la quantité transitant sur le réseau.

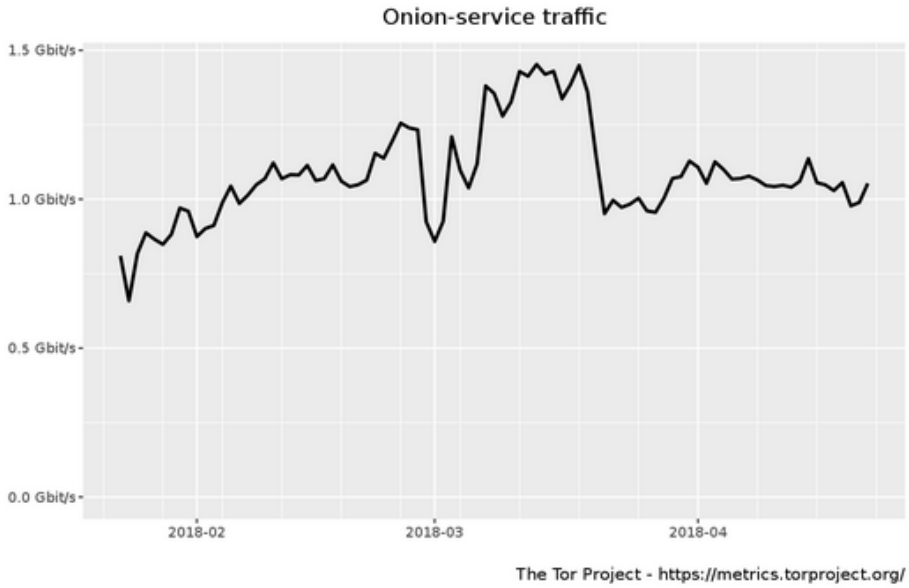
L'ensemble des relais du réseau Tor peut assurer la transmission d'un peu plus de 200 Go d'information par seconde. Environ la moitié, soit un peu plus de 100 Go par seconde, est effectivement utilisée. Les *onion services*, qui constituent le dark web de Tor, consomment

[55] http://www.lemonde.fr/technologies/article/2013/10/03/silk-road-ferme-et-alors_3488971_651865.html (consulté le 22/04/2018).
[56] Le 31 mai 2017, la cour d'appel de New York a confirmé la condamnation à la prison à perpétuité à l'encontre de « Dread Pirate Roberts » : http://www.lemonde.fr/pixels/article/2017/06/01/le-fondateur-de-silk-road-le-supermarche-de-la-drogue-definitivement-condamne-a-la-prison-a-vie_5137343_4408996.html (consulté le 22/04/2018).
[57] En 2016, Bernard Debré, alors député Les Républicains, prononce un discours particulièrement anxiogène à l'Assemblée nationale, en parlant du Darknet [sic] comme du « plus grand supermarché de l'horreur du monde ». L'homme politique a été alerté de l'existence de ce réseau par les journalistes de *Valeurs actuelles* : https://www.youtube.com/watch?v=RaUGdrik74Q (consulté le 22/04/2018).
[58] Les statistiques qui suivent sont tirées de https://metrics.torproject.org/ (consulté le 22/04/2018).
[59] Cf. Jean-Philippe Rennard, *op. cit.*, p. 68.



Bande passante du réseau Tor entre février 2018 et avril 2018. La courbe verte représente le trafic total que le réseau peut supporter ; la courbe violette représente le trafic effectif (par seconde).

© The Tor Project



Trafic effectif (par seconde) enregistré sur les *onion services*, les sites web de Tor, entre février 2018 et avril 2018.

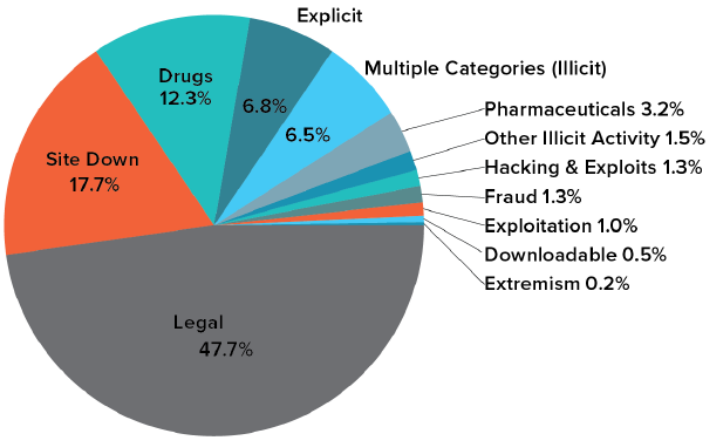
© The Tor Project

entre 0,5 et 1,5 Go de bande passante par seconde, *soit environ 1 % de l'ensemble du trafic Tor*. Ces chiffres montrent que la réalité est bien différente de ce qu'on peut habituellement lire sur le Darknet et en particulier sur Tor : 99 % du trafic s'effectue hors des *onion services*[60].

Allons un peu plus loin : que trouve-t-on sur les services oignon, ce dark web qui ne représente que 1 % du trafic sur Tor ? Le contenu y est-il illégal ? Si l'on en croit une étude publiée en 2016[61], le dark web n'est pas si sombre.

Grâce à un robot programmé pour sélectionner de manière aléatoire 400 sites hébergés sur le réseau Tor et analyser leur contenu, Clare Gollnick et Emily Wilson ont obtenu les résultats suivants : 47,7 % des sites visités hébergeaient du contenu légal[62], 17,7 % étaient inaccessibles[63], 12,3 % étaient consacrés au commerce de stupéfiants, 6,8 % dédiés à la pornographie, 6,5 % proposaient différents contenus illicites[64], 3,2 % étaient des plateformes de vente de médicaments et 2,6 % hébergeaient du contenu relatif au piratage ou aux faux documents. Quatre dernières catégories, activité illégale indéterminée (1,5 %), pédopornographie et torture[65] (1 %), contenu téléchargeable (0,5 %) et extrémisme (0,2 %) se partageaient la (maigre) part restante. Ces statistiques ne sont bien évidemment pas exhaustives (comment pourraient-elles l'être ?), mais s'appuient sur un échantillon suffisamment large pour

[60] Et s'effectue donc selon toute vraisemblance sur des sites appartenant au Clearnet.
[61] Clare Gollnick & Emily Wilson, « Separating Fact from Fiction: The Truth about the Dark Web », Terbium Labs, 2016. Disponible sur https://terbiumlabs.com/darkwebstudy.html (consulté le 22/04/2018).
[62] Une catégorie large qui comprend par exemple des blogs personnels, des forums sur l'anonymat et la technologie ou encore des sites de partis politiques scandinaves. Cf. *Ibid*, p. 8.
[63] Sur le dark web, le contenu évolue très vite. Comme le remarque Rayna Stamboliyska, « il est crucial de comprendre que le contenu est très dynamique […]. Ainsi, des sites peuvent disparaître en une après-midi et ne plus revenir ; des sites 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. » Cf. Rayna Stamboliyska, *La face cachée d'Internet*, Larousse, Paris, 2017, p. 270-271.
[64] Il s'agit, d'après les auteures, de plateformes commerciales sur lesquelles on peut trouver différents types de produits illicites : drogues, logiciels malveillants, numéros de cartes bleues, faux passeports, armes… Cf. Clare Gollnick & Emily Wilson, *op. cit.* p. 17.
[65] Le groupe Anonymous a déclaré la guerre à ce type de contenu il y a quelques années et a depuis enregistré un certain nombre de succès : des sites ont été fermés et certains de leurs utilisateurs dénoncés. Parmi ces actions, on peut citer *Operation Darknet*, lancée en 2011 (http://www.bbc.com/news/technology-15428203) et #OpPedoChat, initiée l'année suivante (http://www.wired.co.uk/article/anonymous-targets-paedophiles) (consultés le 22/04/2018).



Contenu du dark web de Tor (*onion services*) d'après l'étude de Clare Gollnick et d'Emily Wilson (« Separating Fact from Fiction : The Truth about the Dark Web », p. 5).

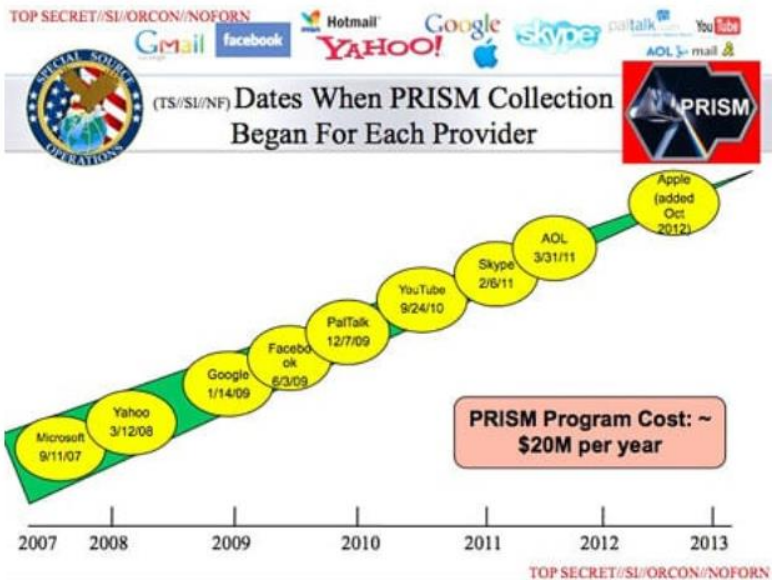
prétendre être représentatives de l'usage des *onion services* ainsi que du contenu qu'ils proposent.

b) Usages du Darknet

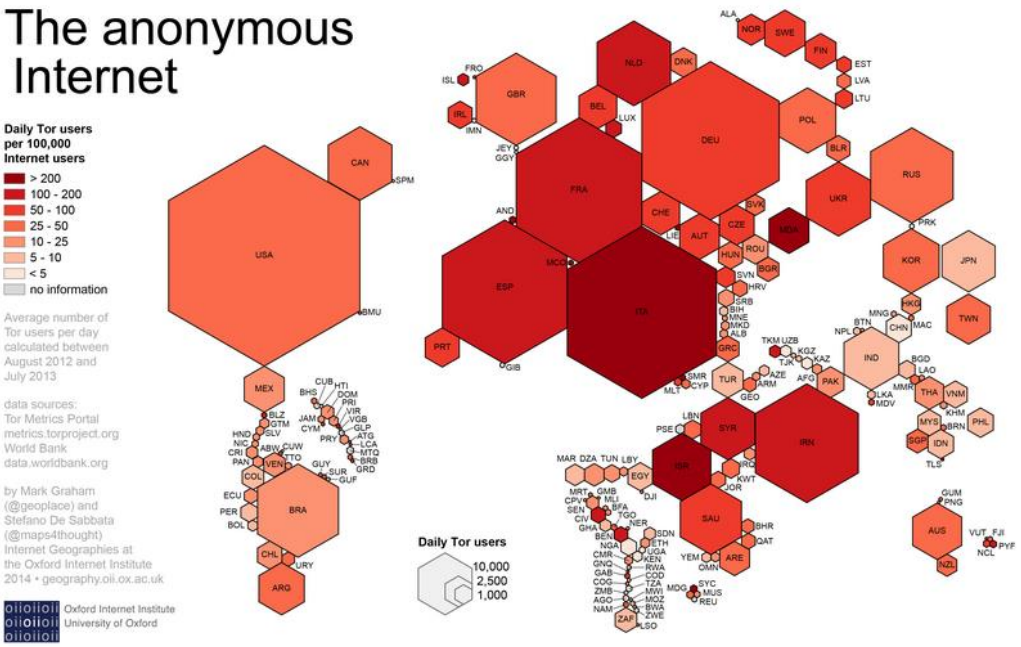
Si seulement 1 % du trafic sur Tor concerne le dark web, c'est que les 99 % restants sont utilisés par les internautes dans le seul but de protéger leur vie privée numérique grâce à la confidentialité des échanges et à l'anonymat que garantit le Darknet en tant qu'architecture réseau. Les raisons de cet usage diffèrent selon la situation politique du pays dans lequel se situe l'internaute : dans les pays démocratiques, un outil comme Tor permet de se soustraire à la surveillance de masse et à l'exploitation économique de nos données, tandis que dans les pays autoritaires, il permet de libérer l'accès à l'information et de donner une plateforme d'expression aux dissidents politiques.

D'aucuns trouveront néanmoins étrange, voire suspect, qu'un individu vivant dans un pays jugé démocratique veuille dissimuler son identité et le contenu de ses échanges en ligne. La volonté de se cacher ne trahit-elle pas nécessairement des activités répréhensibles ? Raisonner de la sorte revient à dire que les rideaux, les volets et les portes d'une maison ne sont d'aucune utilité excepté pour les criminels. Cet argument ignore de fait la revendication légitime de tout individu à protéger sa sphère privée[66]. En outre, c'est oublier que les États *démocratiques* se sont intéressés dès la création d'Internet aux moyens de surveiller les communications sur le réseau. Dès 1971, le programme Echelon est mis en place par les États-Unis, auxquels viennent rapidement s'ajouter le Canada, la Grande-Bretagne, l'Australie et la Nouvelle-Zélande. Dans un contexte de Guerre froide, le programme devait en premier lieu permettre d'espionner les communications de l'URSS et de ses alliés. Mais rapidement, le programme dévie de sa fonction première en interceptant les communications de particuliers ou d'entreprises. Il faudra cependant attendre la fin des années 1990 pour que ces dérives soient dévoilées au public[67].

[66] « 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). » Rayna Stamboliyska, *op. cit.*, p. 8.
[67] https://www.monde-diplomatique.fr/mav/46/RIVIERE/1908 (consulté le 24/04/2018).



Extrait d'un document PowerPoint de la NSA renseignant, de manière chronologique, les entreprises ayant accepté de laisser l'agence américaine accéder aux données de leurs clients dans le cadre du programme PRISM.

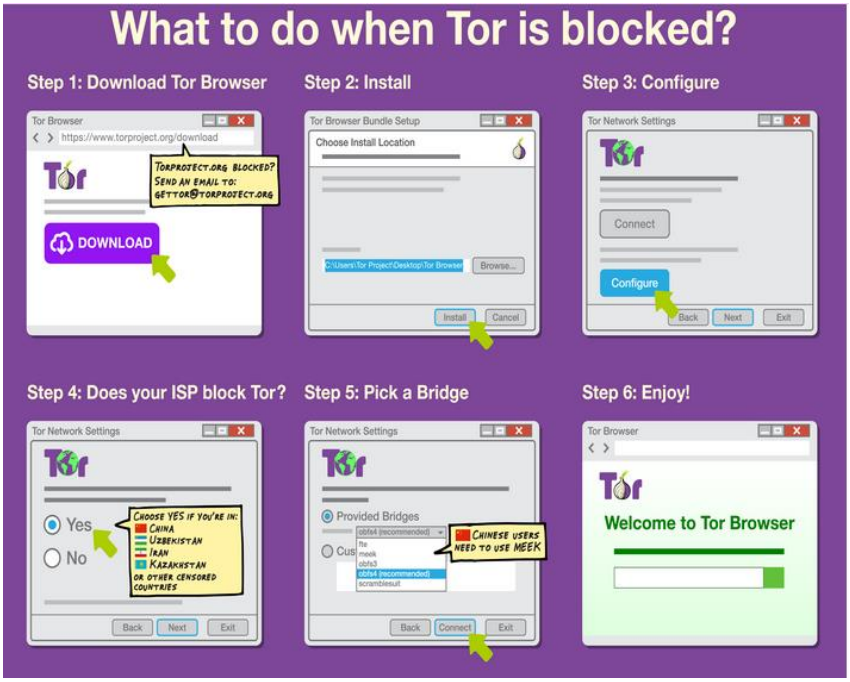


Carte du monde selon les utilisateurs quotidiens de Tor entre août 2012 et juillet 2013. Le nombre d'utilisateurs est représenté par la taille des hexagones. La proportion d'utilisateurs par rapport au nombre d'habitants est représentée par les nuances de rouge.

Dès 1985, David Chaum, l'inventeur des mixnets, avait mis la communauté informatique en garde contre ce qu'il voyait pointer à l'horizon : une société de dossiers[68]. En 2013, les révélations d'Edward Snowden[69] ont confirmé les angoisses de Chaum. Nous savons que le programme **PRISM** a permis à la NSA d'accéder aux données des plus grands opérateurs du net, dont Microsoft, Google, Apple, Yahoo et YouTube[70]. **XKeyScore**, le programme phare de la NSA, dispose quant à lui d'une puissance suffisante pour intercepter quasiment tout ce que fait un individu sur Internet[71] : conversations Facebook, e-mails, historique des pages web visitées. S'intéresser à Tor ou au système d'exploitation **Tails** suffit à être considéré comme suspect par l'agence[72]. Enfin, le programme **Bullrun**, d'un acabit quelque peu différent, a pour objectif de contourner les systèmes de chiffrement les plus répandus par la force ou par l'instauration de portes dérobées[73]. Il n'est donc pas surprenant que les citoyens des pays occidentaux aient recours au Darknet et en particulier à Tor : les communications chiffrées permettent de sauvegarder notre vie privée à l'heure du voyeurisme à outrance.

Dans les régimes autoritaires, l'utilisation du Darknet recouvre des enjeux encore plus cruciaux : échapper à la censure. De nombreuses dictatures exercent un contrôle quasiment absolu sur Internet[74]. Celui-ci se traduit souvent par l'impossibilité d'accéder à certains contenus jugés dangereux ou subversifs et par la surveillance généralisée des internautes. En Chine, le grand Firewall permet, entre autres, le filtrage des paquets et des URL par l'analyse

[68] David Chaum, « Security without Identification : Transaction Systems to make Big Brother Obsolete », *Communications of the ACM*, vol. 28, n° 8, 1985, p. 1030.
[69] http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (consulté le 24/04/2018).
[70] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (consulté le 24/04/2018).
[71] http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html?xtmc=cybersurveillance&xtcr=14. Pour une présentation générale du programme, voir notamment http://www.lemonde.fr/technologies/article/2013/07/31/l-outil-qui-permet-a-la-nsa-d-examiner-quasiment-tout-ce-que-fait-un-individu-sur-internet_3455916_651865.html (pages consultées le 24/04/2018).
[72] https://www.nextinpact.com/news/88527-nsa-surveillance-reseau-tor-plus-serree-que-prevue.htm (consulté le 24/04/2018).
[73] https://www.numerama.com/magazine/26916-comment-la-nsa-peut-contrecarrer-le-chiffrement-des-communications.html (consulté le 24/04/2018).
[74] Les plus répressifs d'entre eux sont recensés dans la « liste des 13 ennemis d'Internet » de Reporters sans frontières : https://rsf.org/fr/actualites/la-liste-des-13-ennemis-dinternet (consulté le 24/04/2018).



Configuration de Tor en mode *pluggable transports*.

E-mail envoyé par Telecomix à environ 6 000 internautes syriens
au mois d'août 2011

Source : owni.fr

des mots-clés qu'ils contiennent, ainsi que le blocage de certaines adresses IP. Un outil comme Tor, qui permet de chiffrer le contenu des paquets et de dissimuler l'adresse IP des sites web aussi bien que des utilisateurs, peut contourner cette censure. Mais, bien évidemment, Tor est bloqué en Chine. Cependant, ses développeurs ont installé un mode, appelé ***pluggable transports***, rendant impossible la détection de l'usage des relais Tor[75]. Aux yeux des autorités de contrôle, le trafic semble utiliser le réseau Internet classique, ce qui permet ainsi d'échapper à la censure.

L'utilisation de Tor a également permis à certains dissidents syriens de communiquer en contournant le contrôle des autorités. Dans la nuit du 11 au 12 août 2011, alors que la révolte avait éclaté depuis quelques mois, le groupe **Telecomix**[76] envoie un e-mail à environ 6 000 internautes syriens avec, en pièce-jointe, des instructions afin de contourner la censure du gouvernement : #OpSyria était lancé[77]. Parmi les outils recommandés dans la pièce-jointe figurait Tor. L'utilisation du Darknet a non seulement permis à la population syrienne de s'informer, mais également d'informer le reste du monde de la situation sur place[78].

Il convient enfin de mentionner l'importance que revêt le Darknet et les outils de chiffrement dans leur ensemble pour les journalistes du monde entier. À une époque où le journalisme d'investigation est menacé dans de nombreux pays, le Darknet représente la possibilité de protéger ses sources, ses données, son identité et, parfois, sa vie. On notera à cet égard que Tor figure aussi bien dans le « kit de sécurité numérique » de Reporters sans frontières [79] que dans la brochure *Information Security for Journalists* [80] du *Centre for Investigative Journalism*. Dans les pays où la démocratie est foulée aux pieds, le Darknet est un outil permettant de redonner un certain pouvoir aux populations qui peuvent ainsi se soustraire au contrôle de l'État.

---

[75] https://www.torproject.org/docs/pluggable-transports.html.en (consulté le 24/04/2018).
[76] https://telecomix.org/ (consulté le 24/04/2018).
[77] http://owni.fr/2011/09/14/opsyria-syrie-telecomix/index.html (consulté le 24/04/2018).
[78] Pour plus de détails sur les mesures mises en place par Telecomix dans le cadre de #OpSyria, voir notamment Jean-Philippe Rennard, *op. cit.*, p. 147.
[79] https://rsf.org/fr/kit-de-securite-numerique (consulté le 24/04/2018).
[80] https://files.gendo.ch/Books/InfoSec_for_Journalists_V1.1.pdf (consulté le 24/04/2018).

Conclusion

Comme nous l'avons souligné, la notion de Darknet renvoie en premier lieu à une réalité technique : une architecture dépendante d'Internet, constituant un réseau spécifique, décentralisé, et intégrant des protocoles de chiffrement et d'anonymisation des échanges. Mais le Darknet en soi n'existe pas : ce n'est qu'un terme générique regroupant l'ensemble des darknets existants. Ces darknets peuvent être ouverts à la navigation classique sur le web, comme Tor, ou être des réseaux autonomes et cloisonnés, tel Freenet. Ils reposent tous sur le système des mixnets, développé par David Chaum, qui permet d'assurer la confidentialité et l'anonymat grâce à un système de relais et à des outils de chiffrement.

Mais le Darknet est également un phénomène social et politique. Les techniques sur lesquelles il repose ne sont que le résultat d'une revendication libertaire : le droit à la vie privée sur Internet ainsi que le libre accès à l'information et la liberté d'expression.

Il est certain que le Darknet, en assurant l'anonymat de l'internaute, permet à certains internautes de se livrer à des activités illégales, voire immorales. Nous avons cependant montré que ces usages étaient largement minoritaires, et qu'il est donc foncièrement erroné de présenter le Darknet comme un lieu de perdition où seules les pires crapules se donneraient rendez-vous. Le Darknet est avant tout un outil, et comme tout outil, il peut servir différentes fins : les technologies seront ce que nous en ferons.

À une époque où les données de tout un chacun sont échangées et exploitées par des gouvernements et des entreprises, il semblerait que le Darknet redonne un certain pouvoir aux individus en leur permettant de protéger leur intimité[81].

[81] « Loin de se réduire à de simples havres de paix pour hackeurs et criminels, les darknets véhiculent également une idéologie et représentent un modèle d'organisation décentralisée qui, sans forcément avoir les moyens de la remettre complètement en question, s'opposent néanmoins à la philosophie qui guide actuellement la régulation d'Internet au sein des institutions internationales. » Laurent Gayard, *op. cit.*, p. 64.

Deuxième partie : texte-support et traduction

Avertissement au lecteur :

Les termes faisant l'objet d'une fiche terminologique sont repérés en gras souligné lors de leur première occurrence, ceux repris dans le glossaire sont simplement signalés en gras dans le texte-support et sa traduction.

Les extraits analysés dans la partie « Stratégie de traduction » y sont quant à eux soulignés.

Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong, « Freenet : A Distributed Anonymous Information Storage and Retrieval System », in *Lecture Notes in Computer Science*, vol. 2009, pp. 46-66, 2001.

Texte source : 3 372 mots/17 255 signes

Freenet: A Distributed Anonymous Information Storage and Retrieval System

3 – Architecture

Freenet is implemented as an **adaptive** peer-to-peer network of nodes that query one another to store and retrieve data files, which are named by location-independent keys. Each node maintains its own local datastore which it makes available to the network for reading and writing, as well as a **dynamic routing table** containing addresses of other nodes and the keys that they are thought to hold. It is intended that most users of the system will run nodes, both to provide security guarantees against inadvertently using a hostile foreign node and to increase the storage capacity available to the network as a whole.

The system can be regarded as a cooperative distributed filesystem incorporating location independence and transparent **lazy replication**. Just as systems such as distributed.net enable ordinary users to share unused **CPU cycles** on their machines, Freenet enables users to share unused disk space. However, where distributed.net uses those CPU cycles for its own purposes, Freenet is directly useful to users themselves, acting as an extension to their own **hard drives**.

The basic model is that requests for keys are passed along from node to node through a chain of **proxy** requests in which each node makes a local decision about where to send the request next, in the style of IP (Internet Protocol) routing.

Texte cible : 3 405 mots/18 281 signes

Freenet : un système distribué et anonyme de stockage et de récupération des données

3 – Architecture

Freenet est un réseau pair-à-pair **auto-adaptatif** composé de nœuds formulant des requêtes afin de stocker ou de récupérer des fichiers identifiables grâce à une clé indépendante de leur localisation. Chaque nœud gère localement son propre magasin, accessible au réseau en lecture et en écriture, tout en maintenant une table de **routage dynamique** répertoriant l'adresse d'autres nœuds et les clés censées s'y trouver. La plupart des utilisateurs administrera un nœud non seulement afin de prévenir l'utilisation involontaire d'un nœud distant hostile, mais aussi pour augmenter la capacité de stockage totale du réseau.

Freenet peut être décrit comme un système de fichiers distribué et coopératif permettant d'identifier les fichiers indépendamment de leur localisation ainsi qu'une **réplication asynchrone** et transparente. Tout comme distributed.net permet d'exploiter les **cycles d'instruction** disponibles du processeur, Freenet permet à ses utilisateurs de partager leur espace disque libre. Cependant, tandis que le premier utilise ces cycles afin d'exécuter ses propres tâches, le second est directement utile à ses utilisateurs en devenant une extension de leur **disque dur**.

Freenet fonctionne par requêtes de clés transmises de nœud en nœud via une chaîne de requêtes relayée par des **serveurs mandataires**. Au cours du processus, chaque nœud décide localement de la direction à donner à la requête, à la manière du routage IP (*Internet Protocol*).

Depending on the key requested, routes will vary. The routing algorithms for storing and retrieving data described in the following sections are designed to adaptively adjust routes over time to provide efficient performance while using only local, rather than global, knowledge. This is necessary since nodes only have knowledge of their immediate upstream and downstream neighbors in the proxy chain, to maintain privacy.

Each request is given a **hops-to-live** limit, analogous to IP's **time-to-live**, which is decremented at each node to prevent infinite chains. Each request is also assigned a pseudo-unique random identifier, so that nodes can prevent loops by rejecting requests they have seen before. When this happens, the immediately preceding node simply chooses a different node to forward to. This process continues until the request is either satisfied or exceeds its hops-to-live limit. Then the success or failure result is passed back up the chain to the sending node. No node is privileged over any other node, so no hierarchy or **central point of failure** exists. Joining the network is simply a matter of first discovering the address of one or more existing nodes through **out-of-band** means, then starting to send messages.

3.1 Keys and searching

Files in Freenet are identified by binary file keys obtained by applying a **hash function**. Currently we use the 160-bit SHA-1 function as our **hash**. Three different types of file keys are used, which vary in purpose and in the specifics of how they are constructed.

The simplest type of file key is the keyword-signed key (KSK), which is derived from a short descriptive text string chosen by the user when storing a file in the network.

Les chemins empruntés dépendront de la clé demandée. Les algorithmes de routage décrits ci-après permettant le stockage et la récupération de données sont conçus pour optimiser les chemins empruntés avec le temps afin d'augmenter la performance du réseau tout en ne faisant appel qu'à une connaissance locale, et non globale. Ce dernier aspect est inévitable, car les nœuds, afin de garantir l'anonymat, ne connaissent que leurs voisins immédiats dans la chaîne de serveurs mandataires.

À la manière des paquets IP et de leur **durée de vie**, chaque requête se voit attribuer un nombre de sauts maximum qui diminue lors de son passage par un nouveau nœud, ce qui permet d'éviter les chaînes infinies. À chaque requête correspond en outre un identifiant unique, généré aléatoirement, permettant aux nœuds de rejeter celles qu'ils ont déjà transférées et ainsi d'éviter les boucles. Dans ce cas, le nœud précédent choisit un chemin différent pour transmettre la requête. Ce processus se poursuit jusqu'à ce que la requête aboutisse ou atteigne le nombre de sauts maximum, après quoi le fichier demandé ou un message d'erreur est renvoyé par le chemin inverse jusqu'au premier nœud. Aucun nœud n'est privilégié par rapport à un autre, il n'y a donc ni hiérarchisation, ni **point de défaillance unique**. Pour se connecter au réseau, il faut simplement trouver l'adresse d'un ou de plusieurs nœuds existants via une **signalisation hors-bande** avant d'initier l'envoi de messages.

3.1 Les différents types de clés et la recherche d'un fichier

Sur Freenet, les fichiers sont identifiables par des clés de fichier binaires obtenues via une **fonction de hachage** : il s'agit actuellement du SHA-1, qui produit des **empreintes** de 160 bits. Freenet utilise trois types de clés de fichier, dont la fonction et les modalités de génération varient.

Les clés de fichier les plus élémentaires sont les clés KSK (*keyword-signed keys*)**,** générées à partir d'une chaîne de caractères courte et descriptive, choisie par l'utilisateur lors du stockage du fichier sur le réseau.

For example, a user inserting a treatise on warfare might assign it the description, text/philosophy/sun-tzu/art-of-war. This string is used as input to deterministically generate a public/private key pair. The public half is then hashed to yield the file key.

The private half of the asymmetric key pair is used to sign the file, providing a minimal **integrity check** that a retrieved file matches its file key. Note however that an attacker can use a **dictionary attack** against this signature by compiling a list of descriptive strings. The file is also encrypted using the descriptive string itself as a key, for reasons to be explained in section 3.4.

To allow others to retrieve the file, the user need only publish the descriptive string. This makes keyword-signed keys easy to remember and communicate to others. However, they form a flat global **namespace**, which is problematic. Nothing prevents two users from independently choosing the same descriptive string for different files, for example, or from engaging in “key-squatting" – inserting junk files under popular descriptions.

These problems are addressed by the signed-subspace key (SSK), which enables personal namespaces. A user creates a namespace by randomly generating a public/private key pair which will serve to identify her namespace. To insert a file, she chooses a short descriptive text string as before. The public namespace key and the descriptive string are hashed independently, **XOR**'ed together, and then hashed again to yield the file key.

As with the keyword-signed key, the private half of the asymmetric key pair is used to sign the file. This signature, generated from a random key pair, is more secure than the signatures used for keyword-signed keys. The file is also encrypted by the descriptive string as before.

To allow others to retrieve the file, the user publishes the descriptive string together with her subspace's public key. Storing data requires the private key, however, so only the owner of a subspace can add files to it.

Un utilisateur déposant un traité sur l'art de la guerre pourrait par exemple lui donner la description suivante : texte/philosophie/sun-tzu/l'art-de-la-guerre. C'est à partir de cette chaîne que seront déterminées la clé publique et la clé privée. La clé publique est ensuite hachée pour donner la clé de fichier.

Le fichier est signé avec la clé privée, ce qui permet d'effectuer un **contrôle d'intégrité** élémentaire du fichier récupéré. Une personne malveillante pourra néanmoins utiliser une **attaque par dictionnaire** sur cette signature en rassemblant une liste de chaînes descriptives. Le fichier est également chiffré avec la chaîne descriptive, qui sert alors de clé. Nous en donnerons les raisons au chapitre 3.4.

Afin de permettre à d'autres utilisateurs de récupérer le fichier, il suffit de publier la chaîne descriptive : les clés KSK ont ainsi l'avantage d'être facilement mémorisables et communicables. Elles constituent cependant un **espace de noms** global et plat, ce qui est problématique. En effet, rien n'empêche deux utilisateurs de choisir la même chaîne descriptive pour des fichiers différents par exemple, ou d'associer des descriptions célèbres à des fichiers indésirables.

Il est possible d'éviter ces inconvénients en utilisant une clé SSK (*signed-subspace key*). Celle-ci permet de créer des espaces de noms personnels identifiables via une clé publique et une clé privée générées aléatoirement. Pour déposer un fichier, l'utilisateur choisit une chaîne descriptive, comme s'il utilisait une clé KSK. La clé publique de l'espace de noms et la chaîne descriptive sont ensuite hachées indépendamment l'une de l'autre, encodés ensemble via une **opération XOR** et enfin hachées une seconde fois afin de produire la clé de fichier.

Comme avec la clé KSK, la clé privée permet de signer le fichier. Une signature SSK, générée à partir d'une paire de clés aléatoire, est plus sécurisée qu'une signature KSK. Le fichier est également chiffré avec la chaîne descriptive.

Afin que d'autres internautes puissent récupérer le fichier, l'utilisateur publie sa chaîne descriptive ainsi que la clé publique de son sous-espace. Cependant, ce sous-espace ne peut être modifié que par son propriétaire, la clé privée étant nécessaire au stockage de fichiers.

The owner now has the ability to manage her own namespace. For example, she could simulate a hierarchical structure by creating directory-like files containing hypertext pointers to other files. A directory under the key text/philosophy could contain a list of keys such as text/philosophy/sun-tzu/art-of-war, text/philosophy/confucius/analects, and text/philosophy/nozick/anarchy-state-utopia, using appropriate syntax interpretable by a client. Directories can also recursively point to other directories.

The third type of key is the content-hash key (CHK), which is useful for implementing updating and splitting. A content-hash key is simply derived by directly hashing the contents of the corresponding file. This gives every file a pseudo-unique file key. Files are also encrypted by a randomly-generated encryption key. To allow others to retrieve the file, the user publishes the content-hash key itself together with the decryption key. Note that the decryption key is never stored with the file but is only published with the file key, for reasons to be explained in section 3.4.

Content-hash keys are most useful in conjunction with signed-subspace keys using an indirection mechanism. To store an updatable file, a user first inserts it under its content-hash key. She then inserts an indirect file under a signed-subspace key whose contents are the content-hash key. This enables others to retrieve the file in two steps, given the signed-subspace key.

To update a file, the owner first inserts a new version under its content-hash key, which should be different from the old version's content hash. She then inserts a new indirect file under the original signed-subspace key pointing to the updated version. When the insert reaches a node which possesses the old version, a key collision will occur. The node will check the signature on the new version, verify that it is both valid and more recent, and replace the old version. Thus the signed-subspace key will lead to the most recent version of the file, while old versions can continue to be accessed directly by content-hash key if desired. (If not requested, however, these old versions will eventually be removed from the network – see section 3.4.) This mechanism can be used to manage directories as well as regular files.

À ce stade, le propriétaire peut gérer son espace de noms. Il lui est par exemple possible de simuler une structure hiérarchique en créant des fichiers semblables à des répertoires, contenant des liens hypertextes vers d'autres fichiers. Un répertoire correspondant à la clé texte/philosophie pourrait contenir plusieurs clés, comme texte/philosophie/sun-tzu/l'art-de-la-guerre, texte/philosophie/confucius/entretiens ou texte/philosophie/nozick/anarchie-État-utopie, en utilisant une syntaxe compréhensible par le client. Les répertoires peuvent également, de manière récursive, renvoyer vers d'autres répertoires.

Enfin, les clés CHK (*content-hash keys*) sont utiles pour le fractionnement ou les mises à jour. Elles sont directement obtenues à partir d'un hachage du contenu du fichier, conférant ainsi une clé unique à chaque fichier. Ces derniers sont également chiffrés par une clé de chiffrement générée aléatoirement. Pour que d'autres internautes récupèrent le fichier, l'utilisateur publie la clé CHK et la clé de déchiffrement, qui n'est jamais stockée avec le fichier (voir section 3.4).

C'est en lien avec les clés SSK et l'adressage indirect que les clés CHK sont les plus utiles. Pour stocker un fichier actualisable, il faut tout d'abord l'insérer avec sa clé CHK puis insérer un fichier indirect sous une clé SSK contenant un pointeur vers la clé CHK. Les utilisateurs pourront ainsi récupérer le fichier en deux temps grâce à la clé SSK.

Pour mettre un fichier à jour, il faut en charger une nouvelle version assortie d'une nouvelle clé CHK avant d'insérer un nouveau fichier indirect sous la clé SSK originale pointant vers la version mise à jour. Lorsque le fichier mis à jour atteindra un nœud hébergeant l'ancienne version, une collision aura lieu. Le nœud vérifiera alors la signature de la nouvelle version, son authenticité et son âge avant de remplacer l'ancienne version. La clé SSK ouvrira ainsi un chemin vers la dernière version du fichier, tandis que les anciennes versions resteront accessibles directement via la clé CHK (cependant, si elles ne sont pas demandées, ces versions finiront par être effacées du réseau, voir section 3.4). Ce mécanisme permet de gérer des dossiers aussi bien que des fichiers classiques.

Content-hash keys can also be used for splitting files into multiple parts. For large files, splitting can be desirable because of storage and bandwidth limitations. Splitting even medium-sized files into standard-sized parts (e.g. 2^n kilobytes) also has advantages in combating traffic analysis. This is easily accomplished by inserting each part separately under a content-hash key, and creating an indirect file (or multiple levels of indirect files) to point to the individual parts.

All of this still leaves the problem of finding keys in the first place. The most straightforward way to add a search capability to Freenet is to run a **hypertext spider** such as those used to search the web. While an attractive solution in many ways, this conflicts with the design goal of avoiding centralization. A possible alternative is to create a special class of lightweight indirect files. When a real file is inserted, the author could also insert a number of indirect files each containing a pointer to the real file, named according to search keywords chosen by her. These indirect files would differ from normal files in that multiple files with the same key (i.e. search keyword) would be permitted to exist, and requests for such keys would keep going until a specified number of results were accumulated instead of stopping at the first file found. Managing the likely large volume of such indirect files is an open problem.

An alternative mechanism is to encourage individuals to create their own compilations of favorite keys and publicize the keys of these compilations. This is an approach also in common use on the world-wide web.

3.2 Retrieving data

To retrieve a file, a user must first obtain or calculate its binary file key. She then sends a request message to her own node specifying that key and a hops-to-live value. When a node receives a request, it first checks its own store for the data and returns it if found, together with a note saying it was the source of the data. If not found, it looks up the nearest key in its routing table to the key requested and forwards the request to the corresponding node. If that request is ultimately successful and returns with the data, the node will pass the data back to the upstream requestor, cache the file in its own datastore, and create a new entry in its routing table associating the actual data source with the requested key.

Les clés CHK servent également à fragmenter les fichiers, ce qui peut s'avérer intéressant pour les fichiers volumineux, la bande-passante et l'espace de stockage étant limités. La fragmentation de fichiers de taille moyenne en éléments de taille standard (c.-à-d. 2^n ko) permet en outre d'empêcher l'analyse du trafic. Il suffit pour ce faire d'insérer chaque partie du fichier sous une clé CHK différente et de créer un ou plusieurs fichiers indirects pointant vers ces parties.

Ceci n'explique néanmoins pas comment trouver les clés de fichier. La façon la plus directe d'ajouter une fonction de recherche à Freenet consisterait à utiliser un **robot d'indexation** semblable à ceux utilisés sur le web. Cette solution attrayante irait cependant à l'encontre de notre objectif de décentralisation. Il est possible de la contourner en créant des fichiers indirects et légers d'un genre spécifique. Lors de l'insertion d'un fichier, son auteur pourrait y ajouter des fichiers indirects pointant vers celui-ci, nommés en fonction de mots-clés déterminés. Contrairement aux fichiers classiques, ces fichiers indirects pourraient avoir la même clé, c.-à-d. le même mot-clé de recherche, et les requêtes relatives ne s'arrêteraient pas au premier fichier trouvé mais continueraient jusqu'à l'obtention d'un nombre de résultats déterminé. La question de la gestion d'un tel volume de fichiers indirects reste ouverte.

Une alternative serait d'encourager les internautes à compiler leurs clés préférées et à publier les clés de ces compilations, une technique communément utilisée sur le web.

3.2 Récupération de données

Pour récupérer un fichier, il est nécessaire d'obtenir ou de calculer sa clé, puis d'envoyer une requête comprenant cette clé et le nombre de sauts maximum à son propre nœud. Lorsqu'un nœud reçoit une requête, il vérifie tout d'abord que le fichier ne se trouve pas dans son magasin et, le cas échéant, renvoie le fichier et se présente comme l'hébergeur. Dans le cas contraire, le nœud interroge sa table de routage pour trouver la clé la plus proche et transmettre la requête au nœud correspondant. Si la requête aboutit et que le fichier est transmis, ce nœud le fera remonter jusqu'à l'initiateur, mettra le fichier en cache dans son magasin et actualisera sa table de routage en associant la clé au nœud hébergeur.

A subsequent request for the same key will be immediately satisfied from the local cache; a request for a "similar" key (determined by lexicographic distance) will be forwarded to the previously successful data source. Because maintaining a table of data sources is a potential security concern, any node along the way can unilaterally decide to change the reply message to claim itself or another arbitrarily-chosen node as the data source.

If a node cannot forward a request to its preferred downstream node because the target is down or a loop would be created, the node having the second-nearest key will be tried, then the third-nearest, and so on. If a node runs out of candidates to try, it reports failure back to its upstream neighbor, which will then try its second choice, etc. In this way, a request operates as a steepest-ascent **hill-climbing search** with backtracking. If the hops-to-live limit is exceeded, a failure result is propagated back to the original requestor without any further nodes being tried. Nodes may unilaterally curtail excessive hops-to-live values to reduce network load. They may also forget about pending requests after a period of time to keep message memory free.

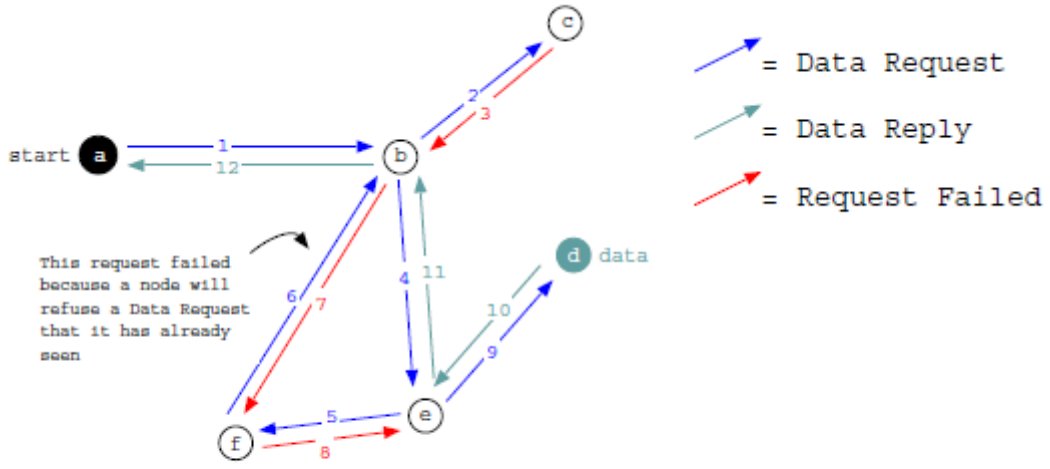


Fig. 1. A typical request sequence.

Lors d'une requête ultérieure pour la même clé, le cache local transmettra directement le fichier, tandis qu'une requête d'une clé proche au niveau lexicographique sera transmise au dernier nœud hébergeur. Pour pallier le problème sécuritaire que constitue le maintien d'une table des nœuds hébergeurs, tout nœud intermédiaire peut décider de modifier le message de réponse et se présenter lui-même ou n'importe quel autre nœud choisi arbitrairement comme la source du fichier.

Si la requête ne peut être transmise au nœud suivant car celui-ci est arrêté ou qu'une boucle se formerait, c'est le deuxième nœud ayant la clé la plus proche qui sera interrogé, puis le troisième et ainsi de suite. Si aucun des nœuds de substitution ne permet de satisfaire la requête, un message d'erreur est renvoyé vers le nœud précédent, qui à son tour interroge le deuxième nœud ayant la clé la plus proche etc. Les requêtes suivent ainsi une procédure de **recherche par escalade**, consistant à suivre la plus forte pente, tout en mémorisant le chemin parcouru. Lorsque le nombre de sauts maximum est atteint, un message d'échec est renvoyé le long de la chaîne au premier nœud et la requête s'arrête. Tout nœud peut arbitrairement choisir de diminuer un nombre de sauts maximum jugé trop grand afin d'alléger le réseau. Il peut également effacer les requêtes en attente au bout d'un certain temps pour libérer de l'espace de stockage.

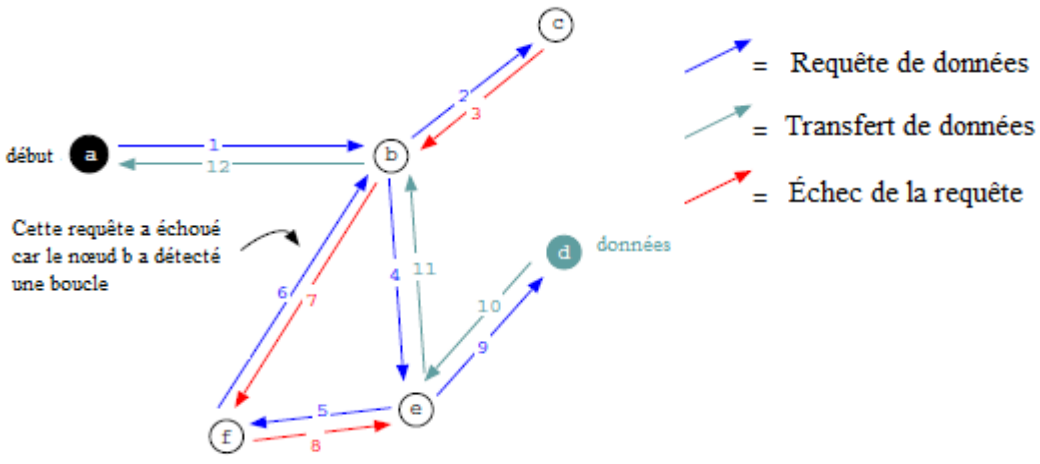


Fig. 1. Une chaîne de requêtes typique

Figure 1 depicts a typical sequence of request messages. The user initiates a request at node a. Node a forwards the request to node b, which forwards it to node c. Node c is unable to contact any other nodes and returns a backtracking "request failed" message to b. Node b then tries its second choice, e, which forwards the request to f. Node f forwards the request to b, which detects the loop and returns a backtracking failure message. Node f is unable to contact any other nodes and backtracks one step further back to e. Node e forwards the request to its second choice, d, which has the data. The data is returned from d via e and b back to a, which sends it back to the user. The data is also cached on e, b, and a.

This mechanism has a number of effects. Most importantly, we hypothesize that the quality of the routing should improve over time, for two reasons. First, nodes should come to specialize in locating sets of similar keys. If a node is listed in routing tables under a particular key, it will tend to receive mostly requests for keys similar to that key. It is therefore likely to gain more "experience" in answering those queries and become better informed in its routing tables about which other nodes carry those keys. Second, nodes should become similarly specialized in storing **clusters** of files having similar keys. Because forwarding a request successfully will result in the node itself gaining a copy of the requested file, and most requests will be for similar keys, the node will mostly acquire files with similar keys. Taken together, these two effects should improve the efficiency of future requests in a self-reinforcing cycle, as nodes build up routing tables and datastores focusing on particular sets of keys, which will be precisely those keys that they are asked about.

In addition, the request mechanism will cause popular data to be transparently replicated by the system and **mirrored** closer to requestors. For example, if a file that is originally located in London is requested in Berkeley, it will become cached locally and provide faster response to subsequent Berkeley requests. It also becomes copied onto each computer along the way, providing **redundancy** if the London node fails or is shut down. (Note that "along the way" is determined by key closeness and does not necessarily have geographic relevance.)

La figure 1 représente une chaîne de requêtes typique. Le nœud a lance une requête qu'il transmet au nœud b, qui la transmet à son tour au nœud c. Ce dernier ne pouvant transférer la requête, il la renvoie au nœud b avec le message « échec de la requête ». Le nœud b choisit alors sa deuxième option, e, qui à son tour transmet la requête à f. Le nœud f transmet ensuite la requête à b, lequel détecte une boucle et renvoie un message d'erreur. Le nœud f ne pouvant interroger d'autres nœuds, il fait remonter la requête à e. Ce dernier opte alors pour sa deuxième option, d, qui héberge le fichier. Le fichier remonte ensuite la chaîne de requête, en partant de d pour passer par e, b et enfin a, qui renvoie l'information à l'utilisateur. Le fichier est mis en cache par e, b et a.

Un tel mécanisme a différentes conséquences. La plus importante est l'optimisation du routage avec le temps, pour deux raisons. Premièrement, les nœuds finiront par se spécialiser dans la localisation de clés semblables : un nœud associé à une clé particulière dans les tables de routage recevra surtout des requêtes de clés proches et y répondra ainsi vraisemblablement de manière de plus en plus efficace, ajoutant les nœuds qui y sont associés à sa table de routage. Deuxièmement, les nœuds auront également tendance à se spécialiser au niveau des fichiers, stockant des **clusters** de fichiers ayant des clés proches. En effet, puisque le fichier est copié par les nœuds de la chaîne lorsqu'une requête aboutit et que la plupart des requêtes concerneront des clés proches, chaque nœud copiera surtout des fichiers ayant des clés semblables. Ces deux aspects devraient permettre aux requêtes futures de gagner en efficacité grâce à un auto-renforcement du système, les tables de routage et les magasins se spécialisant dans les types de clés pour lesquelles ils risquent d'être interrogés.

De plus, les données les plus demandées seront répliquées de manière transparente par le système et **mises en miroir** plus près du nœud à l'origine de la requête. Ainsi, un fichier situé originairement à Londres et demandé à Berkeley sera non seulement mis en cache localement, permettant de satisfaire plus rapidement les requêtes suivantes, mais également copié sur chaque ordinateur de la chaîne, garantissant la **redondance** du fichier si jamais le nœud situé à Londres est arrêté ou échoue (il convient de noter que « les ordinateurs de la chaîne » sont déterminés par proximité de clé et non par situation géographique).

Finally, as nodes process requests, they create new routing table entries for previously-unknown nodes that supply files, increasing connectivity. This helps new nodes to discover more of the network (although it does not help the rest of the network to discover them). Note that direct links to data sources are created, bypassing the intermediate nodes used. Thus, nodes that successfully supply data will gain routing table entries and be contacted more often than nodes that do not. Since keys are derived from hashes, lexicographic closeness of keys does not imply any closeness of the original descriptive strings and presumably, no closeness of subject matter of the corresponding files. This lack of semantic closeness is not important, however, as the routing algorithm is based on knowing where keys are located, not where subjects are located. That is, supposing a string such as text/philosophy/sun-tzu/art-of-war yields a file key AH5JK2, requests for this file can be routed more effectively by creating clusters containing AH5JK1, AH5JK2, and AH5JK3, not by creating clusters for works of philosophy. Indeed, the use of hashes is desirable precisely because philosophical works will be scattered across the network, lessening the chances that failure of a single node will make all philosophy unavailable. The same is true for personal subspaces – files belonging to the same subspace will be scattered across different nodes.

3.3 Storing data

Inserts follow a parallel strategy to requests. To insert a file, a user first calculates a binary file key for it, using one of the procedures described in section 3.1. She then sends an insert message to her own node specifying the proposed key and a hops-to-live value (this will determine the number of nodes to store it on). When a node receives an insert proposal, it first checks its own store to see if the key is already taken. If the key is found, the node returns the pre-existing file as if a request had been made for it. The user will thus know that a collision was encountered and can try again using a different key. If the key is not found, the node looks up the nearest key in its routing table to the key proposed and forwards the insert to the corresponding node.

Enfin, en traitant des requêtes, les nœuds ajoutent de nouveaux pairs à leur table de routage, augmentant par-là la connectivité tout en permettant aux nouveaux nœuds d'augmenter leur connaissance du réseau (sans permettre cependant au reste du réseau de les découvrir). Des liens directs sont établis avec certaines sources, contournant les nœuds intermédiaires. Les nœuds qui satisfont les requêtes seront par conséquent ajoutés à des tables de routages et seront interrogés plus souvent que les nœuds ne les satisfaisant pas. Les clés étant dérivées d'empreintes numériques, la proximité lexicographique n'implique aucune proximité des chaînes descriptives et *a priori* aucune proximité de contenu des fichiers. Cette absence de proximité sémantique importe peu, car l'algorithme de routage s'appuie sur la localisation des clés et non sur celle des contenus. Admettons qu'une chaîne comme texte/philosophie/sun-tzu/l'art-de-la-guerre donne la clé de fichier AH5JK2 ; créer des clusters contenant AH5JK1, AH5JK2 et AH5JK3 permettra d'acheminer les requêtes relatives au fichier plus efficacement qu'en créant des clusters d'œuvres de philosophie. C'est en effet précisément parce que les œuvres philosophiques seront éparpillées sur le réseau que l'échec d'un seul nœud ne rendra pas l'ensemble de la philosophie inaccessible. Il en va de même des sous-espaces personnels : les fichiers appartenant au même sous-espace seront répartis sur différents nœuds.

3.3 Stockage des données

Le procédé de dépôt des fichiers est semblable à celui des requêtes. Pour déposer un fichier, il faut d'abord calculer sa clé suivant l'un des procédés décrits en 3.1. Un message est ensuite envoyé au nœud de l'utilisateur, indiquant la clé calculée et le nombre de sauts maximum (ceci déterminera le nombre de nœuds qui stockeront le fichier). En recevant le message, le premier nœud vérifiera si la clé n'existe pas déjà dans son magasin et, si oui, renverra le fichier comme si une requête avait été faite, indiquant ainsi qu'une collision a eu lieu et qu'une nouvelle clé doit être calculée. Dans le cas contraire, il interrogera sa table de routage et transmettra le message au nœud hébergeant la clé la plus proche.

If that insert causes a collision and returns with the data, the node will pass the data back to the upstream inserter and again behave as if a request had been made (i.e. cache the file locally and create a routing table entry for the data source).

If the hops-to-live limit is reached without a key collision being detected, an "all clear" result will be propagated back to the original inserter. The user then sends the data to insert, which will be propagated along the path established by the initial query and stored in each node along the way. Each node will also create an entry in its routing table associating the inserter (as the data source) with the new key. To avoid the obvious security problem, any node along the way can unilaterally decide to change the insert message to claim itself or another arbitrarily-chosen node as the data source.

If a node cannot forward an insert to its preferred downstream node because the target is down or a loop would be created, the insert backtracks to the second-nearest key, then the third-nearest, and so on in the same way as for requests. If the backtracking returns all the way back to the original inserter, it indicates that fewer nodes than asked for could be contacted. As with requests, nodes may curtail excessive hops-to-live values and/or forget about pending inserts after a period of time.

This mechanism has three effects. First, newly inserted files are selectively placed on nodes already possessing files with similar keys. This reinforces the clustering of keys set up by the request mechanism. Second, new nodes can use inserts as a supplementary means of announcing their existence to the rest of the network. Third, attempts by attackers to supplant existing files by inserting junk files under existing keys are likely to simply spread the real files further, since the originals are propagated on collision. (Note, however, that this is mostly only relevant to keyword-signed keys, as the other types of keys are more strongly verifiable.)

Si une collision a lieu car la clé existe déjà, le fichier sera transmis au nœud à l'origine du message comme s'il avait formulé une requête (*i.e.* le fichier sera mis en cache le long de la chaîne et la table de routage sera actualisée).

Si aucune collision n'a eu lieu lorsque le nombre de sauts maximum est atteint, un message de confirmation sera renvoyé à l'utilisateur voulant déposer le fichier. Ce fichier est ensuite envoyé, propagé et stocké sur les nœuds constituant le chemin emprunté initialement par le message. La table de routage de ces nœuds sera actualisée, associant la nouvelle clé à l'hébergeur, c'est-à-dire au nœud ayant déposé le fichier. Pour des raisons de sécurité évidentes, n'importe quel nœud de la chaîne peut unilatéralement décider de changer le message d'insertion et se présenter lui-même ou tout autre nœud choisi arbitrairement comme la source du fichier.

Si le nouveau fichier ne peut être propagé sur le nœud suivant car celui-ci est arrêté ou qu'une boucle se formerait, il sera propagé sur le deuxième nœud ayant la clé la plus proche, puis sur le troisième et ainsi de suite, à la manière des requêtes de fichiers. Un nouveau fichier renvoyé vers sa source signifie que le nombre de nœuds contacté est inférieur à ce qui était prévu. Comme pour les requêtes, tout nœud peut choisir de réduire un nombre de sauts maximum excessif et/ou d'effacer les dépôts en attente au bout d'un certain temps.

Un tel mécanisme a trois conséquences. Premièrement, les nouveaux fichiers sont délibérément stockés sur des nœuds ayant des clés proches, renforçant ainsi l'agencement en cluster mis en place lors des requêtes. Deuxièmement, déposer des fichiers est un moyen supplémentaire pour les nouveaux nœuds de signaler leur existence au reste du réseau. Enfin, toute tentative de remplacer des fichiers existants par des fichiers indésirables avec une clé déjà utilisée aura vraisemblablement pour effet de diffuser les vrais fichiers, ceux-ci étant propagés lorsqu'il y a collision (cette dernière conséquence concerne surtout les clés KSK, les autres types de clés présentant des mécanismes de vérification plus puissants).

3.4 Managing data

All information storage systems must deal with the problem of finite storage capacity. Individual Freenet node operators can configure the amount of storage to dedicate to their datastores. Node storage is managed as an LRU (Least Recently Used) cache in which data items are kept sorted in decreasing order by time of most recent request (or time of insert, if an item has never been requested). When a new file arrives (from either a new insert or a successful request) which would cause the datastore to exceed the designated size, the least recently used files are evicted in order until there is room. The resulting impact on availability is mitigated by the fact that the routing table entries created when the evicted files first arrived will remain for a time, potentially allowing the node to later get new copies from the original data sources. (Routing table entries are also eventually deleted in a similar fashion as the table fills up, although they will be retained longer since they are smaller.)

Strictly speaking, the datastore is not a cache, since the set of datastores is all the storage that there is. That is, there is no "permanent" copy which is being replicated in a cache. Once all the nodes have decided, collectively speaking, to drop a particular file, it will no longer be available to the network. In this respect, Freenet differs from systems such as Eternity and Free Haven which seek to provide guarantees of file lifetimes.

The expiration mechanism has an advantageous aspect, however, in that it allows outdated documents to fade away naturally after being superseded by newer documents. If an outdated document is still used and considered valuable for historical reasons, it will stay alive precisely as long as it continues to be requested.

3.4 Gestion des données

Tout système de stockage des données doit répondre au problème des limites de l'espace disponible. Chaque opérateur individuel d'un nœud sur Freenet peut configurer la quantité d'espace allouée à son magasin. Le stockage est géré selon le principe de l'utilisation la moins récente : les fichiers sont classés selon la fréquence des requêtes dont il font l'objet (ou selon la date de dépôt s'ils n'ont fait l'objet d'aucune requête). Lorsque l'espace alloué au magasin ne suffit plus à supporter la copie d'un nouveau fichier (résultante d'une requête fructueuse ou d'un dépôt récent), les fichiers ayant fait l'objet des requêtes les plus anciennes sont supprimés de manière à libérer suffisamment d'espace. Le fait que les entrées créées dans les tables de routage lors de l'arrivée du fichier ne disparaissent pas immédiatement, permettant ainsi au nœud d'en récupérer ultérieurement une nouvelle copie à partir des hébergeurs, limite l'impact négatif d'un tel procédé sur la disponibilité des fichiers. Les entrées dans les tables de routage sont supprimées de la même manière que les fichiers, mais elles sont néanmoins conservées plus longtemps car elles prennent moins de place.

Le magasin n'est pas à proprement parler un cache, l'ensemble des magasins constituant la totalité de l'espace de stockage : cela signifie qu'aucune copie « permanente » n'est enregistrée dans un cache. Lorsque l'ensemble des nœuds aura choisi de supprimer un fichier donné, ce dernier disparaitra du réseau. En ce sens, Freenet se distingue de systèmes comme Eternity ou Free Haven, dont l'objectif consiste à garantir la disponibilité des fichiers.

Un tel mécanisme présente cependant l'avantage de permettre le remplacement naturel de documents obsolètes par des documents plus récents. Un document obsolète qui est encore utilisé et précieux d'un point de vue historique restera disponible tant qu'il continuera à être demandé.

For political or legal reasons, it may be desirable for node operators not to explicitly know the contents of their datastores. This is why all stored files are encrypted. The encryption procedures used are not intended to secure the file – that would be impossible since a requestor (potentially anyone) must be capable of decrypting the file once retrieved. Rather, the objective is that the node operator can plausibly deny any knowledge of the contents of her datastore, since all she knows a priori is the file key, not the encryption key. The encryption keys for keyword-signed and signed-subspace data can only be obtained by reversing a hash, and the encryption keys for content-hash data are completely unrelated. With effort, of course, a dictionary attack will reveal which keys are present – as it must in order for requests to work at all – but the burden such an effort would require is intended to provide a measure of cover for node operators.

Pour des raisons juridiques ou politiques, les opérateurs de nœuds peuvent préférer ignorer le contenu stocké dans leur magasin : c'est pourquoi les fichiers sont tous chiffrés. Ce chiffrement n'est pas censé protéger le fichier, une entreprise impossible puisque le nœud à l'origine de la requête (potentiellement n'importe qui) doit pouvoir le déchiffrer. Il s'agit bien plutôt de permettre à l'utilisateur un déni plausible du contenu de son magasin, seule la clé de fichier, et non la clé de chiffrement, étant supposée connue. En effet, les clés de chiffrement de données chiffrées par une clé KSK ou par une clé SSK ne peuvent être obtenues qu'en inversant l'empreinte numérique, tandis que celles des données chiffrées par un clé CHK n'ont aucun rapport. En associant des efforts et une attaque par dictionnaire, il serait évidemment possible de révéler les clés stockées, et qui doivent l'être pour que les requêtes puissent fonctionner, mais la seule envergure d'une telle entreprise constitue une protection pour les opérateurs de nœud.

Troisième partie : stratégie de traduction

1) Choix du texte-support

La littérature consacrée au Darknet est peu abondante, un fait assez aisément compréhensible si l'on garde à l'esprit qu'il s'agit d'un sujet complexe, peu connu du grand public et relativement récent (les premiers darknets ont été développés à la fin des années 1990). J'ai donc eu quelques difficultés à trouver un document suffisamment technique pour servir de texte-support. Après avoir lu des ouvrages de vulgarisation et m'être familiarisé avec le sujet, j'ai rapidement réalisé que la solution consisterait à traduire un document expliquant le fonctionnement d'un darknet particulier et j'ai d'abord pensé à Tor, le darknet le plus étudié. Cependant, le document qui aurait le mieux répondu aux critères fixés pour le choix du texte-support était un article sur l'utilisation de Tor[82] et non sur son fonctionnement technique. Je me suis donc finalement tourné vers Freenet, ce qui m'a permis de trouver un texte adéquat : *Freenet : A Distributed Anonymous Information Storage and Retrieval System*. Au-delà de l'intérêt technique de l'article, un tel choix me donnait l'opportunité de mettre en lumière un darknet dont la popularité a toujours pâti de l'engouement pour Tor.

a) Nature du texte-support

Mon texte-support est tiré d'un article publié en 1999 par Ian Clarke dans lequel le fonctionnement de Freenet est expliqué. Né en Irlande en 1977, Ian Clarke déménage en 1995 à Edimbourg afin d'y étudier l'informatique. C'est pour son projet de fin d'études qu'il développe Freenet en 1999, un système qu'il dévoile de manière détaillée deux ans plus tard dans son article *Freenet : A Distributed Anonymous Information Storage and Retrieval System*.

L'article d'Ian Clarke décrit les spécificités techniques du réseau Freenet de manière détaillée. Il s'agit d'un document de spécialiste destiné à des spécialistes (informaticiens,

[82] Damon McCoy et *al.*, « Shining Light in Dark Places: Understanding the Tor Network », *Lecture Notes in Computer Science*, vol. 5134, 2008, pp. 63-76.

ingénieurs, mathématiciens…), rédigé dans une langue épurée et concise. Les phrases sont relativement courtes et leur construction syntaxique peu complexe. C'est avant tout à la clarté que vise ce texte, puisqu'il s'agit de présenter un nouveau système à la communauté scientifique.

b) Découpage

Le document intégral étant assez conséquent (20 pages, 9 184 mots), j'ai dû en extraire une partie afin de constituer mon texte-support. Après une brève introduction, l'article replace l'apparition de Freenet dans son contexte en faisant un point sur les différents programmes protégeant l'anonymat. L'architecture du système est ensuite décrite en détail dans la principale partie de l'article. Le texte se conclut sur des considérations relatives à la sécurité et à la performance du réseau. Pour que mon texte-support ait une certaine cohérence et forme un tout, j'ai décidé d'extraire la quasi-totalité de la troisième partie, consacrée à l'architecture de Freenet. J'en ai supprimé le dernier chapitre, qui décrit l'ajout de nœuds sur le réseau, afin de réduire le nombre de mots de 3 684 à 3 372.

Le contenu de l'extrait choisi porte sur les différents types de clés utilisées sur Freenet et décrit la manière dont elles se rapportent à leur fichier, le processus de requête et de dépôt de fichiers ainsi que la gestion de l'espace de stockage disponible sur le réseau. Il s'agit donc de la partie essentielle de l'article, qui permet de saisir la singularité de Freenet.

c) En amont de la traduction

Avant de me lancer dans la traduction, j'ai lu plusieurs fois l'article afin de ma familiariser avec son rythme, sa structure et les enchaînements d'idées. Ces lectures préliminaires m'ont également permis de réfléchir à mon postulat traductif ainsi qu'à des procédés concrets de traduction. J'ai ainsi pu définir provisoirement les grands axes de ma stratégie de traduction avant même de commencer à traduire mon texte-support.

Après avoir effectué ces lectures, j'ai identifié des articles et des extraits d'ouvrages traitant de Freenet afin de réellement me familiariser avec le sujet et de découvrir des

perspectives ou des précisions complémentaires sur le sujet. C'est seulement lorsque j'ai commencé à saisir le fonctionnement général de Freenet que je me suis attelé à la traduction.

2) Procédés de traduction

a) Postulat traductif

Afin d'aborder méthodiquement la traduction du texte-support, j'ai effectué un travail préalable sur le texte source afin de déterminer sa fonction, une étape à mon sens nécessaire afin de réellement saisir l'intention de l'auteur et de retranscrire adéquatement non seulement le sens du texte, mais également sa finalité. Pour ce faire, je me suis appuyé sur la théorie du skopos et en particulier sur la typologie des textes élaborée par Katharina Reiss.

L'article d'Ian Clarke est un texte de type informatif, qui vise à augmenter le bagage cognitif de son lecteur. En effet, l'auteur y présente le fonctionnement de Freenet, un darknet d'un type bien particulier : son objectif est donc avant tout de familiariser les spécialistes du domaine avec un nouveau logiciel. Faire comprendre, voilà la finalité de ce texte.

Après avoir déterminé la fonction du texte, j'ai pu définir mon postulat traductif : afin d'être conforme à l'esprit du texte source, ma traduction devait avant tout se plier à une *exigence de clarté*, qui ne saurait cependant s'identifier à une exigence de simplicité : le texte d'Ian Clarke est un texte technique qu'on ne saurait simplifier sans perdre de l'information. Pour tenir ce postulat traductif, il a parfois été nécessaire d'ajouter des éléments à mon texte cible (explicitation) ou d'en supprimer par rapport au texte source (ellipses). De façon presque paradoxale, j'ai ajouté ou retranché des éléments dans une optique de fidélité au texte et à sa fonction informative.

J'ai en outre essayé de limiter au maximum le taux de foisonnement, qui est souvent positif de l'anglais vers le français, et ce pour deux raisons. La première est directement liée à mon exigence de clarté. Comme le note Jean Delisle, « la recherche de la concision n'est pas une fin en soi. Elle se justifie par un souci d'exposer les idées du texte de départ de la façon la plus

claire et la plus cohérente possible[83]. » La seconde est directement liée à la forme de l'exercice, qui consiste à présenter le texte source en regard du texte cible : limiter le foisonnement permet de présenter des textes de longueur à peu près égale et de faciliter au lecteur la comparaison des textes. Je me suis efforcé d'éviter au maximum les circonvolutions et autres périphrases afin de produire un texte dense et concis, à l'image de l'original.

Enfin, j'ai limité au maximum les répétitions, très fréquentes dans le texte source, *si celles-ci ne me semblaient pas nécessaires à la bonne compréhension du texte*, c'est-à-dire tant que cela ne nuisait pas à mon objectif de clarté. Cette limitation m'a semblé essentielle au respect du génie de la langue française, qui supporte moins les répétitions que la langue anglaise[84].

b) Les procédés de traduction directs[85]

i) La traduction littérale

Lorsque le texte source le permettait, c'est-à-dire lorsqu'une structure phrastique particulière en anglais pouvait être reprise telle qu'elle en français, sans que cela ne porte préjudice à la compréhension ou au génie de la langue, j'ai simplement transposé la structure anglaise en français.

Exemple :

« *Just as systems such as distributed.net enable ordinary users to share unused CPU cycles on their machines, Freenet enables users to share unused disk space.* » (p. 44)
« Tout comme distributed.net permet d'exploiter les cycles d'instruction disponibles du processeur, Freenet permet à ses utilisateurs de partager leur espace disque libre. » (p. 45)

[83] Jean Delisle, *La traduction raisonnée*, Presses de l'Université d'Ottawa, 2013 (1993), p. 524.
[84] « L'anglais tolère mieux que le français la répétition lexicale, même dans les textes de style soutenu. » Michel Ballard, *La traduction : de l'anglais au français*, Nathan, Paris, 1992, p. 232. Sur ce point, voir également Jean Delisle, *op. cit.*, p. 546.
[85] Cette taxonomie est empruntée à Vinay et Darbelnet, *Stylistique comparée du français et de l'anglais*, Éditions Didier, Paris, 1958.

Dans la langue source, la phrase commence par la subordonnée pour finir par la proposition principale, une structure que l'on retrouve couramment en français. Il ne m'a donc pas semblé nécessaire de modifier la structure originale, que j'ai reprise comme telle. On notera cependant deux omissions dans la traduction : « *systems such as* » et « *ordinary users* ». J'ai décidé de supprimer le premier élément pour des raisons de concision et eu égard au public cible : les lecteurs de ce texte sont des spécialistes du domaine et connaissent selon toute vraisemblance distributed.net[86], il est donc superflu de préciser sa nature ici. Je n'ai pas non plus repris « *ordinary users* », le substantif étant répété un peu plus loin.

ii) L'emprunt

L'informatique étant un domaine en constante évolution, les néologismes y sont nombreux. Développer un nouveau programme, c'est souvent introduire des fonctionnalités qui n'existaient pas auparavant et qu'il va bien falloir nommer. Freenet ne déroge pas à la règle : les trois types de clés qui y sont utilisés (*keyword-signed-keys*, *signed-subspace-keys* et *content-hashed-keys*) ont été développées par Ian Clarke et n'ont ni traduction officielle, ni traduction d'usage. En parcourant la maigre littérature en français faisant état de ces clés, je me suis rapidement aperçu que ces termes n'étaient jamais traduits, mais devenaient des sigles (KSK, SSK et CHK) qui peuvent avoir la catégorie lexicale de substantif (« la CHK[87] ») ou d'adjectif (« la clé SSK[88] »). J'ai dans un premier temps choisi la première solution pour des raisons de logique : chaque sigle contient le mot « *key* » et parler de « clé KSK » est donc à la fois superflu et redondant. Cependant, après m'être mis à la place du public cible, qui découvre ici un nouveau système informatique, je suis revenu sur ma position. En effet, parler de « la KSK » ou de « la CHK » sans plus de précisions à un public certes expert, mais qui n'a pas encore vraiment intégré cette réalité, signifiait à mon sens courir le risque de semer la confusion chez

[86] Créé en 1997, distributed.net est un logiciel de calcul distribué dont l'objectif est d'apporter des solutions à des problèmes mathématiques en utilisant des cycles d'instruction inutilisés des processeurs (https://www.distributed.net/, consulté le 06/06/2018).
[87] Cf. par exemple Jean-Philippe Rennard, *op. cit.*, p. 66 et Benoît Romito, *Stockage décentralisé adaptatif : autonomie et mobilité des données dans les réseaux pair-à-pair*, Université de Caen, 2012, p. 17.
[88] Cf. Telesphore Tiendrebeogo, *Système dynamique et réparti de nommage à indirections multiples pour les communications dans l'Internet*, Université de Bordeaux I ; Université de Ouagadougou, 2013, p. 39.

le lecteur. J'ai donc finalement opté pour la deuxième solution et ai employé les sigles comme adjectifs.

Exemple :

« *The third type of key is the content-hash key (CHK), which is useful for implementing updating and splitting*. » (p. 50)
« Enfin, les clés CHK (*content-hashed keys*) sont utiles pour le fractionnement ou les mises à jour. » (p. 51)

iii) Le calque

Dans le langage informatique, qui se développe et se constitue en anglais pour ensuite être repris ou adapté dans les autres langues, le calque est, au même titre que l'emprunt, une réalité que l'on ne saurait ignorer. Au cours de mes recherches terminologiques, j'ai pu prendre conscience de l'importance de ce procédé, ce qui m'a amené à l'utiliser dans ma traduction après m'être assuré à chaque fois que j'épousais ainsi l'usage et que je n'introduisais pas une simple traduction de mon cru. Ainsi, en effectuant des recherches pour traduire le terme *hash function*, j'ai rapidement réalisé que l'équivalent français est tout simplement « fonction de hachage ». De la même façon, *dictionary attack* correspond en français à « attaque par dictionnaire ».

Exemple 1 :

« *Files in Freenet are identified by binary file keys obtained by applying a hash function.* » (p. 46)
« Sur Freenet, les fichiers sont identifiables par des clés de fichier binaires obtenues via une fonction de hachage. » (p. 47)

Exemple 2 :

« *Note however that an attacker can use a dictionary attack against this signature by compiling a list of descriptive strings.* » (p. 48)
« Une personne malveillante pourra néanmoins utiliser une attaque par dictionnaire sur cette signature en rassemblant une liste de chaînes descriptives. » (p. 49)

c) Les procédés de traduction obliques

Si les procédés de traduction directs peuvent s'avérer utiles et efficaces (au niveau terminologique aussi bien que stylistique), il est bien entendu impossible de s'y limiter pour traduire un texte de plusieurs pages. La raison principale en est l'insuffisante proximité morphosyntaxique entre le français et l'anglais : ces langues fonctionnent différemment. Ainsi, « il se peut que par suite de divergences d'ordre structural ou métalinguistique certains effets linguistiques ne se laissent pas transposer en LA [langue d'arrivée] sans un bouleversement plus ou moins grand de l'agencement ou même du lexique[89]. »

J'ai par conséquent dû adapter certains passages afin de respecter le génie de la langue d'arrivée, sans quoi mon texte aurait pu heurter le lecteur français et perdre en authenticité. Pour ce faire, j'ai eu recours à différents procédés.

i) La transposition

J'ai plusieurs fois utilisé la transposition lorsque la structure phrastique dans le texte source ne pouvait être reprise telle quelle en français. Très commode pour le traducteur en ce qu'elle lui permet de se détacher du texte à traduire, la transposition consiste à « remplacer une partie du discours par une autre, sans changer le sens du message[90] ».

[89] Vinay et Darbelnet, *op. cit.*, p. 46.
[90] *Ibid.*., p. 50.

Sans vouloir à tout prix défendre la thèse selon laquelle le français est la langue du nom et que l'anglais est celle du verbe[91], j'ai souvent eu recours à la recatégorisation d'un verbe en substantif, soit parce qu'elle me semblait nécessaire, soit parce qu'elle me semblait plus naturelle.

Exemple :

« *This lack of semantic closeness is not important, however, as the routing algorithm is based on knowing where keys are located, not where subjects are located.* » (p. 58)
« Cette absence de proximité sémantique importe peu, car l'algorithme de routage s'appuie sur la localisation des clés et non sur celle des contenus. » (p. 59)

Dans ce passage, il était tout simplement impossible de se passer de la recatégorisation. La langue française ne permet pas d'apposer un verbe à la suite d'une structure comme « être basé sur » ou « s'appuyer sur » : la préposition accolée au verbe impose l'emploi d'un substantif. J'avais donc dans un premier temps procédé à une double recatégorisation en traduisant « *based on knowing where keys are located* » par « s'appuie sur la connaissance de la localisation des clés ». Cependant, lors de la relecture, j'ai trouvé cette formulation à la fois trop lourde et trop explicite. J'ai finalement opté pour « s'appuie sur la localisation des clés », estimant que « connaissance » devenait implicite puisque pour s'appuyer sur la localisation de quelque chose, il faut nécessairement connaître cette localisation.

J'ai également utilisé la recatégorisation pour traduire l'ensemble des sous-titres de l'article, exprimés par un participe présent dans le texte source. J'ai ainsi traduit « *retrieving data* », « *storing data* » et « *managing data* » par « récupération des données », « stockage des données » et « gestion des données », la forme substantivée me paraissant à la fois plus idiomatique et plus adaptée à un titre de section.

[91] Sur ce point, nous renvoyons à l'ouvrage de Jean Delisle, *op. cit.*, et en particulier à son chapitre « Tournures nominales, tournures verbales », p. 511-517. Voir également Vinay et Darbelnet, *op. cit.*, p. 102-104.

ii) La restructuration

L'article d'Ian Clarke étant un document technique à visée explicative, il est important que ses lecteurs puissent saisir aisément les relations de causalité entre les différentes parties du discours. En lisant le texte, j'ai été frappé par l'agencement de certaines phrases qui, à mon sens, ne soulignait pas suffisamment le lien entre certains énoncés. Quand cela m'a paru permettre une meilleure compréhension du contenu de l'article, j'ai donc effectué des restructurations.

Exemple :

« *First, nodes should come to specialize in locating sets of similar keys. If a node is listed in routing tables under a particular key, it will tend to receive mostly requests for keys similar to that key. It is therefore likely to gain more "experience" in answering those queries and become better informed in its routing tables about which other nodes carry those keys.* » (p. 56)
« Premièrement, les nœuds finiront par se spécialiser dans la localisation de clés semblables : un nœud associé à une clé particulière dans les tables de routage recevra surtout des requêtes de clés proches et y répondra ainsi vraisemblablement de manière de plus en plus efficace, ajoutant les nœuds qui y sont associés à sa table de routage. » (p. 57)

Le texte original explique ici la propriété d'auto-optimisation du routage sur Freenet : avec le temps, les nœuds vont se spécialiser dans certains types de clés car certaines tables de routage les auront identifiés comme interlocuteurs privilégiés, transmettant effectivement les fichiers associés à ces clés. Pourtant, cette explication est structurée en trois phrases distinctes : la première pose la thèse, la seconde énonce un fait et la troisième en tire la conséquence (indiquée par « *therefore* »), confirmant la thèse. Dans ma traduction, j'ai fusionné ces trois phrases en modifiant la ponctuation afin de faire ressortir ce lien de conséquence. J'ai d'abord introduit deux points à la place du premier point final, indiquant par là au lecteur qu'il aborde l'explicitation de l'énoncé précédent, puis j'ai remplacé le second point final par « et », remplaçant ce qui était une rupture par un signe de continuité. Enfin, j'ai traduit ce qui était une conjonction de coordination (« *and* ») dans la dernière phrase par un participe présent (« ajoutant »). Cette modulation permet de souligner qu'il s'agit d'une justification de ce qui précède, alors qu'ils apparaissent dans le texte source

comme des éléments distincts. C'est en effet parce qu'un nœud associe des clés à d'autres nœuds dans sa table de routage qu'il peut répondre plus efficacement aux requêtes ultérieures.

iv) Du passif à l'actif

Il est difficile de ne pas remarquer l'utilisation du passif tant celle-ci est abondante : 65 des 157 phrases que comporte le texte source comportent (au moins) une formulation passive. Ce phénomène est particulièrement flagrant dans les premiers paragraphes. Les raisons ne sont pas simplement liées à la langue anglaise, qui, comme l'allemand, a plus facilement recours à la voix passive que le français. On retrouve ce type de formulation dans de nombreux documents techniques et scientifiques, car il permet de donner un caractère impersonnel et objectif aux phénomènes décrits, sans faire intervenir un agent humain à qui l'on attribuerait la cause de ces phénomènes.

J'ai souvent repris ces tournures passives, qui permettent de produire le même sentiment d'objectivité chez le lecteur français et donc de répondre aux codes d'un document technique universitaire destiné à des spécialistes. Cependant, il a parfois été nécessaire de passer à la voix active lorsque la structure passive ne pouvait être conservée sans compromettre le génie de la langue française.

Exemple 1 :

« *These problems are addressed by the signed-subspace key (SSK)* […]. » (p. 48)
« Il est possible d'éviter ces inconvénients en utilisant une clé SSK (*signed-subspace key*). » (p. 49)

Nous avons ici une formulation largement répandue dans le milieu universitaire et scientifique qu'il est impossible de reprendre littéralement en français : « adresser » et « problème » ne constituent pas une collocation. Il serait certes possible de conserver la voix passive en changeant de verbe : « Ces problèmes sont résolus en utilisant une clé SSK » est grammaticalement correct, mais confère un caractère statique à la traduction, qui semble alors décrire un état tandis que la phrase dans le texte source décrit un processus. J'ai donc finalement opté pour une tournure active, sans pour autant insérer un agent, afin de conserver le caractère impersonnel de l'original. Cette formulation présente également l'avantage de souligner que

l'utilisation de la clé SSK est une possibilité que l'utilisateur choisira d'actualiser ou non. En outre, j'ai explicité ce qui était implicite dans le texte source en ajoutant un participe présent.

Exemple 2 :

« *A subsequent request for the same key will be immediately satisfied from the local cache* […]. » (p. 54)
« Lors d'une requête ultérieure pour la même clé, le cache local transmettra directement le fichier […]. » (p. 55)

Dans ce passage, malgré la voix passive, l'agent est clairement identifié : il s'agit du cache local. J'ai donc spontanément choisi de traduire cet extrait par une tournure active ; conserver le passif ne me semblait ni justifié, ni idiomatique (cela aurait alourdi inutilement la phrase). Cette modulation m'a de plus permis de juguler le taux de foisonnement, en supprimant la préposition devant l'agent et l'auxiliaire être, nécessaire à la formation d'un passif au futur.

v) La dépersonnalisation

Comme nous l'avons souligné, les articles techniques ou scientifiques sont souvent rédigés de manière à présenter leur contenu de manière objective. Pour ce faire, leurs auteurs s'efforcent souvent de supprimer tout agent humain, sauf si celui-ci est partie prenante du processus décrit (dans le cas d'une notice de montage par exemple). Bien que l'article d'Ian Clarke, par son recours à la voix passive, ne déroge pas à cette règle, certains passages mettent en scène une utilisatrice[92] lambda de Freenet pour illustrer le propos.

Lorsque cette « mise en scène » me paraissait justifiée, c'est-à-dire lorsqu'elle décrivait une action devant réellement être effectuée par une personne, j'ai choisi de la reprendre dans ma traduction. En revanche, j'ai eu recours à la dépersonnalisation lorsque la référence à l'utilisateur ne servait qu'à illustrer un aspect du fonctionnement de Freenet, supprimant ainsi la subjectivité des processus décrits.

[92] Ian Clarke emploie en effet le pronom personnel « *she* » et non pas « *he* » lorsqu'il se réfère à cette utilisatrice. J'ai cependant choisi d'employer le masculin dans ma traduction, non pas au nom de la défense d'un quelconque patriarcat, mais parce que cette forme me semblait plus adaptée au ton d'un article technique.

Exemple 1 :

« *To insert a file, a user first calculates a binary file key for it, using one of the procedures described in section 3.1.* » (p. 58)
« Pour déposer un fichier, il faut d'abord calculer sa clé suivant l'un des procédés décrits en 3.1. » (p. 59)

Cet extrait décrit le processus de dépôt de fichiers. En lisant le texte source, on pourrait être induit en erreur et penser que la clé de fichier doit effectivement être calculée par l'utilisateur (une entreprise complexe pour un individu, s'il en est !). Ce n'est bien sûr pas le cas : la clé est calculée par le processeur de l'ordinateur depuis lequel on se connecte à Freenet. La référence à l'internaute m'a ici semblé inutile : non seulement elle n'est pas nécessaire pour comprendre le processus décrit, mais elle pourrait dans le pire des cas biaiser la compréhension du lecteur en lui laissant penser que le calcul d'une clé doit être effectué par un individu.

J'ai donc supprimé cette référence à l'utilisateur dans ma traduction et l'ai remplacée par la tournure impersonnelle « il faut ». En plus d'ôter les risques de mécompréhension évoqués ci-dessus, cette formulation permet de souligner une nécessité inhérente au réseau : c'est ainsi que fonctionne Freenet.

Exemple 2 :

« *The user then sends the data to insert, which will be propagated along the path established by the initial query and stored in each node along the way.* » (p. 60)
« Ce fichier est ensuite envoyé, propagé et stocké sur les nœuds constituant le chemin emprunté initialement par le message. » (p. 61)

Situé quelques lignes après l'extrait précédent, ce passage décrit les étapes permettant l'insertion d'un fichier sur le réseau si aucune collision n'a eu lieu au niveau de la clé. Encore une fois, à lire le texte original, on pourrait penser que l'envoi du fichier est effectué par un individu, ce qui n'est pas tout à fait le cas. Certes, pour qu'un fichier soit ajouté au réseau, il faut qu'un utilisateur le décide et l'indique à son ordinateur. Mais une fois cette décision prise, c'est la machine qui prend le relais : elle calcule une clé, interroge les nœuds proches et, si aucune collision n'a eu lieu et qu'un message de confirmation est reçu, envoie effectivement le fichier qui sera ensuite propagé sur certains nœuds du réseau. Ce processus est entièrement automatisé. J'ai par conséquent choisi de traduire ce passage par une tournure passive, qui

permet de décrire un processus sans lui attribuer d'agent et de conférer ainsi à l'énoncé une tonalité plus scientifique.

vi) L'ajout

La traduction consiste à appréhender un message énoncé dans une certaine langue pour ensuite le transmettre dans une autre langue. L'essence de la traduction réside donc dans *la transmission adéquate de l'information originale*. Un bon traducteur transmet cette information sans y ajouter ni y retrancher quoi que ce soit[93]. L'ajout et l'omission sont donc *a priori* à proscrire. Cependant, la traduction est au service du sens avant d'être au service des mots[94], ce qui signifie que le traducteur, s'il estime qu'un élément doit être ajouté ou supprimé pour transmettre plus efficacement le sens du texte source, peut (et doit) procéder à des « modifications lexicales » sur le texte cible.

J'ai exceptionnellement ajouté à ma traduction des éléments lexicaux qui ne se trouvaient pas dans le texte source quand ces ajouts me semblaient justifiés, qu'ils correspondaient au vouloir-dire de l'auteur et qu'ils facilitaient la compréhension du lecteur. Il faut garder à l'esprit que le document d'Ian Clarke est une explication synthétique du fonctionnement de Freenet : faciliter la compréhension du lecteur est donc une entreprise fidèle à la fonction du texte.

Exemple :

« *The resulting impact on availability is mitigated by the fact that the routing table entries created when the evicted files first arrived will remain for a time, potentially allowing the node to later get new copies from the original data sources.* » (p. 62)
« Le fait que les entrées créées dans les tables de routage lors de l'arrivée du fichier ne disparaissent pas immédiatement, permettant ainsi au nœud d'en récupérer ultérieurement une nouvelle copie à partir des hébergeurs, limite l'impact négatif d'un tel procédé sur la disponibilité des fichiers. » (p. 63)

[93] Cette maxime souffre quelques exceptions, notamment quand une particularité culturelle évidente pour le public source doit être explicitée pour le public cible.
[94] Cf. Danica Seleskovitch et Marianne Lederer, *Interpréter pour traduire*, Les Belles Lettres, Paris, 2014, p. 12.

Ce passage s'intéresse à la gestion de l'espace de stockage sur Freenet et à la logique de suppression des fichiers lorsque cet espace est saturé. La phrase précédente explique que les fichiers ayant fait l'objet de la requête la plus ancienne seront supprimés en premier lorsqu'il faudra libérer de l'espace : ces fichiers ne seront donc plus disponibles sur le nœud duquel ils auront été supprimés. La phrase citée dans l'exemple ci-dessus vient nuancer les effets d'un tel mécanisme sur la disponibilité des fichiers, puisqu'elle souligne que les entrées dans les tables de routage seront conservées un certain temps après la suppression desdits fichiers.

J'ai procédé à deux explicitations dans ma traduction : l'une concernant la nature de l'impact mentionné, l'autre venant préciser la disponibilité en question. En effet, dans le texte source « *the resulting impact* » n'est pas qualifié. Or, il est clairement sous-entendu que cet impact est négatif, puisqu'il porte préjudice aux données du réseau (des fichiers sont supprimés). J'ai donc choisi d'expliciter cet aspect dans ma traduction, afin que le lecteur, certes spécialiste, mais néophyte en ce qui concerne Freenet, puisse comprendre sans ambiguïté qu'il s'agit d'un inconvénient. Ma deuxième explicitation porte sur le substantif « disponibilité ». Dans le texte source, Ian Clarke écrit « *availability* » sans préciser son objet. J'ai décidé de préciser à quelle disponibilité il est ici fait référence, pour deux raisons. Premièrement, le nom « disponibilité » demande toujours à être qualifié en français : on parle de la disponibilité *de quelque chose*. Deuxièmement, cette précision permet d'évacuer du texte cible toute ambigüité quant à l'objet de cette disponibilité.

vii) L'ellipse

J'ai exceptionnellement procédé à des ellipses en suivant la même logique que pour les ajouts : quels éléments de l'énoncé sont nécessaires à une bonne compréhension du fonctionnement de Freenet par le lecteur et (dans le cas des ellipses) quels éléments sont superflus ? Afin de réussir à limiter le taux de foisonnement, j'ai supprimé certaines informations quand j'estimais que celles-ci n'étaient qu'une reprise de ce qui avait déjà été dit auparavant et surtout lorsqu'une telle suppression ne constituait pas une entrave à la compréhension du lecteur.

Exemple 1 :

« *The private half of the asymmetric key pair is used to sign the file, providing a minimal integrity check that a retrieved file matches its file key*. » (p. 48)
« Le fichier est signé avec la clé privée, ce qui permet d'effectuer un contrôle d'intégrité élémentaire du fichier récupéré. » (p. 49)

J'ai ici procédé à deux ellipses. Tout d'abord, j'ai choisi de ne pas traduire « *asymmetric key pair* », car cette information est déjà contenue dans la notion de clé privée. En effet, si une clé privée existe, cela signifie nécessairement qu'une clé publique lui correspond (il y est d'ailleurs fait référence dans le paragraphe précédent). Or, s'il y a une association clé publique/clé privée, c'est que la technique cryptographique utilisée est asymétrique (la cryptographie symétrique n'utilisant qu'une seule clé[95]). Le texte source étant destiné à des spécialistes du domaine et les notions de clé publique et de clé privée remontant aux années 1970, j'ai supprimé une information qui me semblait redondante et *a priori* bien connue du lectorat.

C'est en suivant la même logique que je n'ai pas non plus traduit « *matches its file key* » : l'information est contenue dans le fait que le contrôle d'intégrité soit effectué avec la clé privée. Un contrôle d'intégrité consiste à s'assurer « que des données n'ont pas été modifiées ou détruites de façon non autorisée[96] ». Cela peut s'effectuer de plusieurs manières, mais dans le cas qui nous intéresse ici, le contrôle d'intégrité est effectué grâce à la signature numérique du fichier : comme nous l'avons expliqué dans notre exposé[97], la cryptographie asymétrique permet de signer un fichier avec la clé privée. Ainsi, pour s'assurer qu'un fichier correspond bien à la clé demandée, il suffit de déchiffrer le fichier avec la clé publique contenue dans la clé de fichier. Étant donné que les trois paragraphes précédant l'extrait ci-dessus décrivent l'association entre un fichier et sa clé, les lecteurs de l'article comprendront que ce contrôle d'intégrité consiste à associer une clé et son fichier sans qu'il soit nécessaire de l'expliciter.

[95] Sur ce point, voir l'exposé, p. 16-22.
[96] Définition ISO 7498-2.
[97] Cf. p. 18.

Je me suis également permis d'omettre certains éléments quand ceux-ci avaient déjà été mentionnés et qu'ils se laissaient déduire du contexte.

Exemple 2 :

« *To retrieve a file, a user must first obtain or calculate its binary file key.* » (p. 52)
« Pour récupérer un fichier, il est nécessaire d'obtenir ou de calculer sa clé. » (p. 53)

L'omission volontaire porte ici sur « *binary file* », qui vient préciser la nature de « *key* » : Freenet utilise des clés de fichier binaires. Cela signifie que les clés sont composées de bits pouvant prendre la valeur zéro ou un[98]. Il s'agit d'une information importante, puisqu'elle nous indique que la clé n'est pas composée de lettres, comme l'est la description du fichier, mais qu'elle est le résultat d'une fonction de hachage. Cependant, à ce niveau du texte, le lecteur sait déjà que les clés utilisées sur Freenet sont de type binaire : la première phrase de la section 3.1 l'a annoncé. J'ai donc préféré supprimer cette précision superflue par la suite.

viii) Éviter les répétitions

Comme je l'ai mentionné en définissant mon postulat traductif, j'ai essayé de limiter les répétitions, nombreuses dans le texte de départ, lorsque cela ne risquait pas d'introduire une ambiguïté dans ma traduction ou de gêner la compréhension du lecteur.

Exemple 1 :

« *When this happens, the immediately preceding node simply chooses a different node to forward to.* » (p. 46)
« Dans ce cas, le nœud précédent choisit un chemin différent pour transmettre la requête. » (p. 47)

La phrase ci-dessus présente un mécanisme propre à Freenet permettant d'éviter les boucles. Lorsqu'une requête atteint un nœud donné pour la deuxième fois, celui-ci la reconnaît grâce à son

[98] Voir notamment https://www.futura-sciences.com/tech/definitions/informatique-code-binaire-11934/ (consulté le 08/06/2018).

identifiant unique et détecte une boucle : il renvoie alors un message d'erreur au nœud précédent, lequel choisit alors un autre chemin pour transférer la requête.

Il est difficile de ne pas remarquer la répétition de « *node* », tant les deux occurrences sont rapprochées. À première vue, cette répétition semble nécessaire : le nœud recevant un message d'erreur doit transmettre la requête à un autre nœud. Pourtant, en tenant compte du contexte dans lequel cet énoncé est formulé, on peut raisonnablement penser que la seconde occurrence du terme « nœud » est évitable sans nuire au sens original du message. En effet, le mécanisme des requêtes a été défini deux paragraphes plus haut : celles-ci sont *transmises de nœud en nœud via une chaîne de requêtes relayées par des serveurs mandataires*. Autrement dit, le passage d'un nœud à l'autre est contenu dans le concept de requête : le chemin suivi par les requêtes est constitué par certains nœuds du réseau. En m'appuyant sur ce raisonnement, j'ai donc décidé de supprimer une répétition qui était devenue superflue pour la remplacer par « chemin différent », un choix qui ne sera nullement préjudiciable au lecteur attentif.

Exemple 2 :

« *The user initiates a request at node a. Node a forwards the request to node b, which forwards it to node c. Node c is unable to contact any other nodes and returns a backtracking "request failed" message to b.* » (p. 56)
« Le nœud a lance une requête qu'il transmet au nœud b, qui la transmet à son tour au nœud c. Ce dernier ne pouvant transférer la requête, il la renvoie au nœud b avec le message "la requête a échoué". » (p. 57)

Ce passage commente l'illustration du chemin typique emprunté par une requête sur Freenet. J'ai repris la plupart des répétitions afin d'éviter toute ambiguïté : les signifiés doivent être clairement identifiés afin que le lecteur puisse suivre les étapes de la requête. J'ai néanmoins trouvé une répétition inutile à la clarté de l'explication : il s'agit de la deuxième mention de « *node c* ». Cette répétition est flagrante car seul un point final sépare les deux occurrences. J'ai choisi de contourner cette répétition en utilisant la reprise anaphorique « ce dernier », qui ne laisse aucun doute possible quant à son antécédent, puisque celui-ci la précède immédiatement. Cette solution permet en outre de fluidifier un texte dont le rythme général est assez saccadé.

d) Résolution des problèmes de compréhension et de logique dans le texte source

Ne disposant pas de connaissances pointues en informatique et n'appartenant donc pas au public cible, j'ai été gêné par certains passages du texte source. Les problèmes que j'ai rencontrés sont de deux types : problèmes de compréhension et problèmes de logique.

i) Résolution d'un problème de compréhension

Bien que le texte d'Ian Clarke ne soit pas pointu au point d'en devenir inaccessible pour un néophyte, celui-ci reste un article technique qui m'a posé certains problèmes de compréhension.

Exemple :

« *If that request is ultimately successful and returns with the data, the node will pass the data back to the upstream requestor, cache the file in its own datastore, and create a new entry in its routing table associating the actual data source with the requested key.* » (p. 52)
« Si la requête aboutit et que le fichier est transmis, ce nœud le fera remonter jusqu'à l'initiateur, mettra le fichier en cache dans son magasin et actualisera sa table de routage en associant la clé au nœud hébergeur. » (p. 53)

Dans ce passage, c'est le sens de « *pass the data back to the upstream requestor* » qui m'a posé problème, étant donné le contexte dans lequel il s'inscrit : s'agit-il de faire transiter le fichier vers le nœud précédent ou vers le nœud suivant dans la chaîne de requêtes ? Autrement dit, est-ce qu'on décrit ici le trajet du nœud hébergeur vers le nœud à l'origine de la requête ou l'inverse ? Dans un premier temps, j'avais opté pour la première solution, en m'appuyant sur le terme « *requestor* », pensant que celui-ci désignait le requérant originel, le nœud ayant initié la requête. Pourtant, en relisant la phrase attentivement, j'ai été amené à remettre cette interprétation en doute : en effet, on peut y lire « *returns with the data* », qui semble indiquer que le fichier est déjà parvenu jusqu'au requérant. De plus, la requête étant transmise de nœud

en nœud, il serait réducteur d'identifier « *requestor* » avec le requérant : le terme peut en réalité désigner n'importe quel nœud de la chaîne, dans la mesure où chaque nœud reformule la requête pour la transmettre. Cette interprétation est d'ailleurs confirmée par l'adjectif « *upstream* », qui désigne un nœud bien précis parmi un ensemble de candidats possibles. On pourrait alors penser que « *pass the data back* » ne signifie pas « faire remonter le fichier », mais « renvoyer le fichier », au sens où le nœud à l'origine de la requête renverrait le fichier après l'avoir reçu.

Pour résoudre ce conflit d'interprétations, je me suis tourné vers les textes en français portant sur Freenet. Après avoir croisé les sources[99], le doute ne m'était plus permis : lors d'une requête, les fichiers ne sont pas renvoyés vers l'hébergeur après avoir été reçus par l'initiateur de la requête. Ils ne sont transférés que dans une seule direction. « *Upstream requestor* » désigne donc le nœud situé en amont dans la chaîne de requête et donc, en fin de compte, le requérant. « *Returns with the data* » n'englobe pas le trajet du fichier dans son ensemble, mais simplement une réponse positive du nœud hébergeur, qui transmet alors le fichier au nœud précédent.

ii) Résolution d'un problème de logique

Dans son ensemble, le texte source est cohérent et logique : les idées s'enchaînent bien, et, malgré le rythme particulier de l'article, le lecteur peut assez aisément suivre le raisonnement développé par Ian Clarke. Un problème de logique s'y trouve néanmoins, problème qu'une lecture un peu hâtive pourrait manquer de déceler et par suite reproduire dans la traduction.

L'inconséquence en question apparaît deux fois, au tout début du texte (p. 44), puis au milieu (p. 54). En voici la seconde occurrence :

« *If the hops-to-live limit is exceeded, a failure result is propagated back to the original requestor without any further nodes being tried.* »
« Lorsque le nombre de sauts maximum est atteint, un message d'échec est renvoyé le long de la chaîne au premier nœud et la requête s'arrête. »

[99] En particulier Jean-Philippe Rennard, *op. cit.*, p. 67 et Telesphore Tiendrebeogo, *op. cit.*, p. 37.

Sur Freenet, lorsqu'une requête est initiée, un nombre de sauts maximum lui est attribué. Ce nombre de sauts détermine la durée de vie de la requête et est censé empêcher l'encombrement du réseau par des requêtes qui n'aboutiraient pas mais continueraient néanmoins à être transférées. Ce « *hops-to-live* » est donc une limite. Pourtant, en lisant l'extrait ci-dessus, il est permis d'en douter : d'après le texte, le nombre de sauts maximum pourrait en réalité être dépassé avant que le message d'échec ne soit envoyé et que la requête prenne fin. Un tel procédé n'est pas contradictoire au niveau informatique : il suffit de définir le nombre de sauts maximum et d'autoriser son dépassement d'un saut lors de la programmation du logiciel pour en faire une réalité. Mais alors pourquoi parler de « *hops-to-live* » s'il est possible de dépasser cette « limite » ?

Avant de prendre une décision sur la manière de traduire ce passage, j'ai consulté d'autres sources traitant du sujet, afin de savoir si le texte source contenait vraiment une erreur de logique ou s'il s'agissait seulement d'une formulation malheureuse de la part d'Ian Clarke.

La littérature fiable sur le sujet est unanime : une requête ne peut aller au-delà du nombre de sauts maximum[100] et s'arrête donc lorsque celui-ci est *atteint* et non pas *dépassé*. Le passage identifié recèle donc non seulement une erreur de logique (il est par définition impossible de dépasser une limite), mais également une erreur *factuelle* qui risque d'induire le lecteur en erreur. J'ai rectifié cette erreur dans ma traduction, en traduisant « *exceed* » par « atteindre » : si je me suis ainsi éloigné du sens du texte, j'ai cependant produit un énoncé plus fidèle à l'architecture de Freenet.

[100] Sur le site de Freenet, on peut en effet lire :« *HTL (Hops to Live) is a number embedded in each request that is usually decremented when the request is forwarded, starting at a value of 18 at the originator of the request, and serves to limit the number of hops a request can survive on the network.* » https://freenetproject.org/fr/police-departments-tracking-efforts-based-on-false-statistics.html (consulté le 08/06/2018). Jean-Philippe Rennard écrit quant à lui : « Le processus se poursuit jusqu'à ce que l'on ait *atteint* le nombre de sauts maximum. » *Op. cit.*, p. 67 (nous soulignons).

Quatrième partie : analyse terminologique
1) Fiches terminologiques

Vedette anglaise	N°	Vedette française
Darknet	01	Darknet
deep Web	02	deep web
hash	03	empreinte numérique
overlay network	04	réseau superposé
public-key cryptography	05	cryptographie asymétrique

COMMENT LIRE UNE FICHE TERMINOLOGIQUE
Les fiches terminologiques ci-après sont constituées de tout ou partie des champs suivants :

- VE VEdette (terme faisant l'objet de la fiche et ses synonymes)
- EN ENglish
- FR FRançais
- DF DéFinition de la vedette
- DOM DOMaine
- CTX ConTeXte
- COL COLlocations
- ID IDentification de l'auteur
  Bureau Émetteur (organisme pour lequel la fiche a été rédigée) : ESIT
  Collection terminologique à laquelle appartient la fiche : MEM18 pour mémoire soutenu en 2018
  Auteur de la fiche : SHA = Stephen HAllot

- Notes :
  EXP = renseignements encyclopédiques qui ne font pas partie de la définition
  USG = indications relatives à l'USaGe, au niveau de la langue, au registre, à la région, etc.
  GRM = indications GRaMmaticales
  ETY = ETYmologie
  DER = mots DERivés
  HOM = HOMonyme
  ANT = ANTonyme
  SPE = termes SPÉcifiques
  GEN = termes GÉNériques
  REL = renvois associatifs à d'autres termes

- RF RéFérences (sources bibliographiques)

Fiche n° 1 - anglais

VE EN Darknet [1] darknet [2]

DF Overlay network which has been designed specifically for anonymity.

DOM Computer science and cryptography

CTX On another tack, the US Department of Defense Advances Research Projects Agency (DARPA) is working on accessing the Darknet via a search engine.

COL n.:
* markets, * websites
v.:
accessing the *, surfing the *,

ID ESIT MEM18 SHA

Notes

EXP1 The darknet refers to the peer-to-peer network itself, whereas the dark web is the content that is served up on these networks.

EXP2 Two typical darknet types are friend-to-friend networks and privacy networks such as Tor, I2P, Freenet, DN42 etc.

EXP3 Virtual private networks are another aspect of the Darknet that exists within the public internet, which often requires additional software to access. TOR (The Onion Router) is a great example. Hidden within the public web is an entire network of different content which can only be accessed by using the TOR network.

ANT Clearnet

USG [1] refers to the Darknet as a whole; [2] refers to a specific darknet

SPE Dark Web

REL markets, deep Web, Tor, Freenet, Bitcoin, hidden services, onion services

RF TECHLOG360, Darknet vs Dark Web vs Deep Web vs Surface Web [online], available at <https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/> (consulted on 16/06/2018) [1] [DF] [EXP2]; Jamie Bartlett, *The Darknet*, New York, Melville House, 2015, p. 239 [2]; Cath Senker, *Cybercrime and the Darknet*, Arcturus, London, 2016, p. 177 [CTX]; CNET, Dark Web 101: Your Guide To The Badlands of the Internet [online], available at <https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/> (consulted on 16/06/2018) [EXP1]; Steve Pederson, *Understanding the Deep Web in 10 Minutes*, BrightPlantet, 2013, p. 3 [EXP3].

Fiche n° 1 – français

VE FR Darknet [1] darknet [2] internet clandestin [3] internet chiffré [4] Librenet [5]

DF Sous-réseau d'internet utilisant des protocoles spécifiques et intégrant nativement des fonctions d'anonymisation.

DOM Informatique et cryptographie

CTX Le système d'échange de mails chiffrés GPG fait partie de l'écosystème Darknet, tout comme la messagerie instantanée Cryptocat.

COL n. :
plateforme du *, forums du *, marchés du *

ID ESIT MEM18 SHA

Notes

EXP1 Différents types de darknets existent en fonction de leur infrastructure : les réseaux pair-à-pair et les réseaux mixtes (*mixnets*) anonymes.

EXP2 L'un des premiers darknets F2F est Freenet.

EXP3 Le darknet ne se confond ni avec les réseaux pair-à-pair, ni avec le deep web.

ANT Clearnet

USG [1] anglicisme le plus utilisé par les spécialistes, désigne l'ensemble des darknets ; [2] désigne un darknet particulier ; [3] terme recommandé par la Commission d'enrichissement de la langue française (Journal Officiel n°0225 du 26 septembre 2017, texte n° 110), peu attesté dans l'usage. [4] proposition de traduction personnelle qui, contrairement à celle de la Commission d'enrichissement de la langue française, n'est pas connotée négativement, mais s'appuie sur l'essence de ce qui fait le Darknet : le chiffrement [5] Proposition de traduction, encore très peu utilisée, émanant de différents spécialistes et visant à libérer le Darknet de sa connotation négative.

SPE dark web

REL deep web, Tor, Freenet, Bitcoin, services cachés

RF Laurent Gayard, *Géopolitique du Darknet*, London, ISTE Editions, 2018, p. 10 [1] [2] ; FRANCETERME, internet clandestin [en ligne], disponible sur <http://www.culture.fr/franceterme/result?francetermeSearchTerme=internet+clandestin&francetermeSearchDomaine=0&francetermeSearchSubmit=rechercher&action=search> (consulté le 16/06/2018) [3] ; Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 12 [DF] [CTX] ; Rayna Stamboliyska, *La face cachée d'Internet*, Paris, Larousse, 2017, p. 241-242 [EXP1] [EXP2] ; RENNARD JEAN-PHILIPPE, Qu'est-ce que le Darknet ? [en ligne], disponible sur <http://www.rennard.org/Darknet/presentation.html> (consulté le 16/06/2018) [EXP3].

Fiche n° 2 – anglais

VE EN deep Web [1] invisible Web [2] hidden Web [3]

DF Any Internet information or data that is inaccessible by a search engine.

DOM Computer science

CTX When structured data in the Deep Web is surfaced, the structure and hence the semantics of the data is lost.

COL n. :
content from the *, * sources, * sites, * URLs

v. :
accessing the *

ID ESIT MEM18 SHA

Notes

EXP1 The key points are that content in the deep Web is massive –approximately *500 times greater* than that visible to conventional search engines – with much higher quality throughout.

EXP2 The deep Web includes all Web pages, websites, intranets, networks and online communities that are intentionally and/or unintentionally hidden, invisible or unreachable to search engine crawlers.

ANT surface Web, visible Web, indexable Web

GEN World Wide Web

RF Michael K. Bergman, « The Deep Web: Surfacing Hidden Value », Journal of electronic publishing, Vol. 7 (1), 2001 [1] [EXP 1]; European Monitoring Center for Drugs and Drugs Addiction (EMCDDA), EU Drug Market Report, 2016, p. 47 [2]; Encyclopædia Britannica, « The Deep Web, The Internet's Dark Side », 2013, p. 1 [3]; EMCDDA, « Drugs and the Darknet », 2017, p. 77 [DF]; TECHOPEDIA, Deep Web [online], available at <https://www.techopedia.com/definition/15653/deep-web> (consulted on 16/06/2018) [EXP2]; Madhavan Jayant et al., « Harnessing the Deep Web : Present and Future », CIDR Perspectives, 2009, p. 5 [CTX].

Fiche n° 2 – français

VE FR deep web [1] web profond [2] web invisible [3] abysse [4] toile profonde [5]

DF Ensemble du réseau qui n'est pas indexé par les moteurs de recherche.

DOM Informatique

CTX Le Darknet peut pour partie être considéré comme appartenant au deep web, en ce sens qu'il n'est pas indexé par les grands moteurs de recherche, qu'il leur est même globalement inaccessible, mais il n'en est qu'une infime fraction.

COL n. :
ressources du *

v. :
accéder au *,

ID ESIT MEM18 SHA

Notes

EXP1 On estime la taille du deep web à au moins 400 à 500 fois celle du web de surface.

EXP2 Les ressources du Web invisible comprennent, entre autres, les sites Web construits autour d'une base de données (interrogeable uniquement par un moteur de recherche interne), les pages accessibles par un formulaire de recherche, les pages protégées par un mot de passe, les pages interdites aux robots d'indexation, les pages écrites dans des formats propriétaires, les intranets et les extranets.

ANT web de surface, web surfacique, web indexable, web visible

USG [1] anglicisme, terme le plus employé dans la littérature spécialisée [4] [5] termes recommandés par la Commission d'enrichissement de la langue française (Journal Officiel n°0225 du 26 septembre 2017, texte n° 110), qui ne sont cependant pas encore entrés dans l'usage.

GEN Web

RF Rayna Stamboliyska, *La face cachée d'Internet*, Paris, Larousse, 2017, p. 240 [1] ; ICANN, « Le web invisible : terre des services cachés », 2017 [2] ; Service commun de la documentation de l'Université Nice Sophia Antipolis, « Le web invisible », 2011 [3] ; JO n°0225 du 26 septembre 2017 [4] [5] ; Le Monde, « "Dark Web", "deep Web" ou "user interface" ont désormais leur traduction française officielle », 2017 [DF] ; Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 14 [CTX] [EXP1] ; Grand Dictionnaire Terminologique de l'OQLF, « Web invisible », 2017 [EXP2].

Fiche n° 3 – anglais

VE EN hash [1] message digest [2] digest [3] digital fingerprint [4]

DF Fixed size numeric representation of the contents of a message, computed by a hash function.

DOM Computer science and cryptography

CTX This command is used to transfer to the card the result of a hash calculation on some data.

COL n.:
* value, * algorithm, * function, * table, * output, * calculation, * of the message, file *, cryptographic *

v.:
to calculate a *, to produce a *, to reverse a *

ID ESIT MEM18 SHA

Notes

EXP1 Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.

EXP2 In essence, a hash is smaller than the text that produces it. It is generated in a way that a similar hash with same value cannot be produced by another text.

EXP3 Hashing can be used to compare a large amount of data. Hash values can be created for different data, meaning that it is easier comparing hashes than the data itself.

EXP4 The hash function must be one way. It must not be possible to reverse the function to find the message corresponding to a particular message digest, other than by testing all possible messages.

USG [4] polysemic, to be avoided.

GEN Hash function, hash algorithm, hash table

SPE Digital signature

RF Cath Senker, *Cybercrime and the Darknet*, Arcturus, London, 2016, p. 189 [1]; IBM, Messages digests and digital signatures [online], available at <https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10510_.htm> (consulted on 20/06/2018) [2] [3] [DF] [EXP4]; BUSINESS DICTIONARY, digital fingerprint [online], available at < http://www.businessdictionary.com/definition/digital-fingerprint.html> (consulted on 20/06/2018) [4]; Official Journal of the European Communities, Commission Regulation No 1360/2002 of 13 June 2002, p. 116 [online], available at <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:207:0001:0252:EN:PDF> (consulted on 20/06/2018) [CTX]; TECHOPEDIA, Message Digest [online], available at <https://www.techopedia.com/definition/4024/message-digest> (consulted on 20/06/2018) [EXP1]; SSL2BUY, Difference Between Hashing and Encryption [online], available at <https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption> (consulted on 20/06/2018) [EXP2] [EXP3].

Fiche n° 3 – français

VE FR empreinte [1] condensé [2] condensat [3] hash [4]

DF Séquence de bits de longueur fixe créée à partir d'un fichier et issue d'un algorithme.

DOM Informatique et cryptographie

CTX Il est aisé de calculer l'empreinte numérique d'un document, mais il est très difficile de retrouver le document initial à partir de son empreinte.

COL n. :
* d'un fichier, taille d'une *, valeur d'une *,

adj. :
* numérique, * cryptographique

v. :
calculer une *, publier une *, créer une *

ID ESIT MEM18 SHA

Notes

EXP1 Dans les années 1980, plusieurs fonctions de hachage ont ainsi été proposées et normalisées, notamment les fonctions MD5 (Message Digest 5) et SHA-1 (Secure Hash Algorithm 1). La première calcule des empreintes de 128 bits et la seconde des empreintes de 160 bits. Plus récemment ont vu le jour les fonctions de hachage de la famille SHA-2, avec des empreintes allant jusqu'à 512 bits.

EXP2 Une modification à l'intérieur d'un document, même infinitésimale, provoque un changement radical de son empreinte : toute modification devient ainsi immédiatement détectable.

EXP3 Les empreintes sont essentiellement utilisées pour vérifier ou démontrer l'intégrité d'un document, c'est-à-dire s'assurer qu'il n'a subi aucune altération ou modification intentionnelle ou accidentelle.

USG [4] anglicisme, à éviter.

GEN Fonction de hachage, algorithme de hachage, fonction de condensation

SPE Signature numérique

RF Adli Takkal Bataille et Jacques Favier, *Bictoin, la monnaie acéphale*, Paris, CNRS Éditions, 2017, p. 92 [1] ; Jean-François Pillou et Jean-Philippe Bay, *Tout sur la sécurité informatique*, Paris, Dunod, 2016, p. 97 [2] ; Laurent Bloch, *Sécurité informatique : pour les DSI, RSSI et administrateurs*, Paris, Eyrolles, 2011, p. 105 [3] ; Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 95 [4] ; Claude Huc, *Préserver son patrimoine numérique*, Paris, Eyrolles, 2010, p. 314 [DF] [EXP3] ; Patrick Legand, *Sécuriser enfin son PC*, Paris, Eyrolles, 2006, p. 370 [CTX] [EXP2] ; JACQUES STERN, Cryptologie, *Encyclopædia Universalis* [en ligne], accessible sur <http://www.universalis-edu.com/encyclopedie/cryptologie/> (consulté le 20/06/2018) [EXP1].

Fiche n° 4 – anglais

VE EN overlay network [1] SDN overlay [2]

DF Telecommunications network that is built on top of another network and is supported by its infrastructure.

DOM Computer science and Internet

CTX It is theoretically possible to build an overlay that provides an abstraction of a failure-free network over a failure-prone underlay network of the same size and type without significant loss in performance.

COL n.:
* functions, * infrastructure, * architecture,

adj.:
a separate *, a default *, an anonymizing *, a wireless *, a routing *, a peer-to-peer *

v.:
to connect to a *, to create a *, to use a *, to build an *,

ID ESIT MEM18 SHA

Notes

EXP1 All nodes in an overlay network are connected with one another by means of logical or virtual links and each of these links correspond to a path in the underlying network.

EXP2 Most forms of overlay networking use some sort of "encapsulation," or software encoding, that markets the data before it is taken to its destination. When it gets to the destination, this encapsulated message is unwrapped and delivered to the destination it was intended for – typically some sort of network application.

EXP3 Overlay networking can include peer-to-peer networks, IP networks, and virtual local area networks (VLANs). The Internet itself, which uses Layer 3 IP addressing, uses overlay networking, identifying locations by IP addresses.

ANT Underlay network, physical network

SPE TCP/IP, peer-to-peer, HTTP, Darknet, VPN

RF TECHOPEDIA, Overlay Network [online], available at <https://www.techopedia.com/definition/10788/overlay-network> (consulted on 21/06/2018) [1] [EXP1]; RCR WIRELESS NEWS, Three different SDN models [online], available at <https://www.rcrwireless.com/20170811/three-different-sdn-models-tag27-tag99> (consulted on 21/06/2018) [2]; SEARCHSDN, Overlay network [online], available at <https://searchsdn.techtarget.com/definition/overlay-network> (consulted on 21/06/2018) [DF]; Ramesh K. Sitaraman *et al.*, *Overlay Networking: an Akamai Perspective*, John Wiley & Sons, 2014, p. 6 [CTX]; SDXCENTRAL, What is Overlay Networking (SDN Overlay)? [online], available at <https://www.sdxcentral.com/sdn/definitions/what-is-overlay-networking/> (consulted on 21/06/2018) [EXP2] [EXP3].

Fiche n° 4 – français

VE FR réseau superposé [1] réseau overlay [2]

DF Réseau informatique basé sur un autre réseau.

DOM Informatique et Internet

CTX Pour chaque requête disséminée dans le réseau, le protocole DG-CastoR construit de manière implicite un réseau superposé, appelé colonie.

COL n. :
protocole de *, nœuds du *

adj. :
* anonyme, * décentralisé, * distribué, * pair-à-pair

v. :
construire un *, créer un *

ID ESIT MEM18 SHA

Notes

EXP1 Tor, Freenet et I2P sont des réseaux superposés qui ne sont accessibles que sous certaines conditions.

ANT réseau physique

SPE TCP/IP, pair-à-pair, HTTP, Darknet, VPN

RF NUMERAMA, Non, le Darknet n'est pas un « réseau clandestin » [en ligne], accessible sur <https://www.numerama.com/politique/292452-non-le-darknet-nest-pas-un-reseau-clandestin.html> (consulté le 21/06/2018) [1] [DF] ; Rayna Stamboliyska, *La face cachée d'Internet*, Paris, Larousse, 2017, p. 244 [2] ; Talar Atéchian, *Protocole de routage géo-multipoint hybride et mécanisme d'acheminement de données pour les réseaux ad hoc de véhicules*, INSA Lyon, 2010, p. 9 [CTX].

Fiche n° 5 – anglais

VE EN public-key cryptography [1] public-key encryption [2] asymmetric encryption [3] asymmetric cryptography [4] public-key cipher [5] asymmetric cipher [6]

DF Encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication.

DOM Computer science and cryptography

CTX This problem is known as prime factoring, and some implementations of public-key cryptography take advantage of this difficulty for computers to solve what the component prime numbers are.

COL n.:
implementations of *, use of *, * procedure, * protocol

ID ESIT MEM18 SHA

Notes

EXP1 The concept of asymmetric encryption was first introduced by Whitfeld Diffie and Martin Hellman in 1976.

EXP2 The most commonly used implementations of public key cryptography are based on algorithms presented by Rivest-Shamir-Adelman (RSA) Data Security.

EXP3 Public-key Cryptography is implemented by a variety of internet standards, including Transport Layer Security (TLS), Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Secure Socket Layer (SSL) and Hypertext Transfer Protocol (HTTP) websites.

EXP4 Disadvantage: Pure asymmetric procedures take a lot longer to perform than symmetric ones.

ANT Symmetric cryptography, symmetric encryption

SPE RSA Algorithm, DSA

REL PGP, Diffie-Hellman key exchange, SSL, TLS, GPG, Bitcoin

RF IBM, Public key cryptography [online], available at <https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html> (consulted on 18/06/2018) [1] [2] [3] [EXP2]; INFOSEC INSTITUTE, The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure [online], available at <https://resources.infosecinstitute.com/mathematical-algorithms-asymmetric-cryptography-introduction-public-key-infrastructure/#gref> (consulted on 18/06/2018) [4]; Bernhard Esslinger, *The CrypTool Script*, Frankfurt, 2010, p. 7 [5] [EXP1] [EXP4]; Jan De Clercq, Guido Grillenmeier, *Microsoft Windows Security Fundamentals*, Elsevier Digital Press, Burlington, 2007, p. 17 [6]; TECHOPEDIA, Public Key Cryptography [online], available at <https://www.techopedia.com/definition/9021/public-key-cryptography-pkc> (consulted on 18/06/2018) [DF] [EXP3]; SSD EFF, A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? [online], available at <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work> (consulted on 18/06/2016) [CTX].

Fiche n° 5 – français

VE FR cryptographie asymétrique [1] chiffrement asymétrique [2] chiffrement à clé publique [3] chiffrage à clé publique [4] chiffrage asymétrique [5] cryptage asymétrique [6]

DF Technique utilisée dans le but de garantir la confidentialité d'une donnée et qui intègre deux clés de chiffrement, une clé publique et une clé privée.

DOM Informatique et cryptographie

CTX Une signature numérique est un type de technologie de chiffrement utilisant une cryptographie asymétrique pour créer des clés numériques uniques qui, utilisées conjointement, garantissent à la fois la sécurité et l'authenticité des données.

COL n. :
protocole de *, système de *, algorithme de *, technique de *

v. :
s'appuyer sur la *, être basé sur la *

ID ESIT MEM18 SHA

Notes

EXP1 La clé de chiffrement du message est appelée clé publique (et peut-être communiquée sans restriction aucune), et la clé de déchiffrement du message est appelée clé privée.

EXP2 Outre les capacités de chiffrage, le chiffrement à clé publique permet d'authentifier son correspondant.

EXP3 L'algorithme RSA est l'exemple le plus courant de cryptographie asymétrique.

ANT Cryptographie symétrique, chiffrement symétrique, chiffrement à clé privée

USG [4] et [5] attestés dans la littérature spécialisée, mais dont l'usage est contesté, privilégier [1] [2] ou [3] ; [6] à proscrire, seul décryptage peut être employé.

SPE Algorithme RSA, algorithme DSA, PGP, échange de Diffie-Hellman, SSL, TLS, GPG, Bitcoin

RF JOURNAL DU NET, Cryptographie asymétrique : tout sur la méthode de chiffrement [en ligne], disponible sur <https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1209336-cryptographie-asymetrique/> (consulté le 18/06/2018) [1] [EXP1] ; CNIL, Comprendre les grands principes de la cryptologie et du chiffrement [online], disponible sur <http://www.cil.cnrs.fr/CIL/spip.php?article2893> (consulté le 18/06/2018) [2] ; Guy Chassé, *Cryptographie – Algorithmes*, Techniques de l'ingénieur, 2000, p. 5 [3] ; Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016 [4] [5] [DF] [EXP2] ; Philippe Mathon, *VPN : mise en œuvre sous Windows Server 2003*, Paris, Éditions ENI, 2004, p. 9 [6] ; FUTURA SCIENCES, RSA [en ligne], disponible sur <https://www.futura-sciences.com/tech/definitions/tech-rsa-1787/> (consulté le 18/06/2018) [EXP3].

2) Glossaire

AES, algorithme AES, Rijndael, norme de chiffrement avancé, norme AES, standard de chiffrement avancé	AES, Advanced Encryption Standard, Rijndael
Algorithme de chiffrement à clé secrète proposé en 1997 en remplacement du DES et retenu comme standard en 2002. RF : Jean-Philippe Rennard, *Darknet*, Paris Ellipses, 2016, p. 163.	
anonymat	anonymity
Dissimulation de l'identité. RF : Jean-Philippe Rennard, *Darknet*, Paris Ellipses, 2016, p. 12.	
architecture client-serveur, modèle client-serveur, environnement client-serveur	client-server architecture, client-server model
Architecture logicielle dans laquelle les programmes d'application, dits *clients*, font appel, dans le cadre d'un réseau, à des services génériques distants fournis par des ordinateurs appelés *serveurs.* RF : http://www.larousse.fr/dictionnaires/francais/client-serveur/16523 (consulté le 24/06/2018).	
architecture distribuée, architecture répartie, architecture décentralisée	distributed architecture, DNA
Configuration dans laquelle les fonctions d'un système sont réparties entre les différents nœuds d'un réseau. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8369117 (consulté le 24/06/2018).	
attaque par dictionnaire	dictionary attack
Attaque par force brute qui révèle les mots de passe évidents et des combinaisons logiques de mots. RF : https://www.futura-sciences.com/tech/definitions/tech-attaque-dictionnaire-1711/ (consulté le 24/06/2018).	
attaque par déni de service, attaque DoS, attaque par refus de service, attaque par saturation	DoS attack, denial of service attack, saturation attack
Attaque informatique visant à submerger les serveurs d'une société pour les rendre inopérants. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=506804 (consulté le 24/06/2018). NT : Si l'action est lancée depuis plusieurs sources, on parle de déni de service distribué (DDoS).	
auto-adaptatif	adaptive
Se dit d'un système capable de modifier sa configuration ou sa structure interne pour prendre en compte les changements de son environnement et ainsi offrir un service d'une qualité optimale. RF : Franck Chauvel, « Méthodes et outils pour la conception de systèmes logiciels auto-adaptatifs », Université de Bretagne Sud, 2008, p. 11.	
bande passante	bandwidth
Quantité d'informations pouvant être transmises simultanément sur une voie de transmission. RF : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203431-bande-passante-definition-traduction-et-acteurs/ (consulté le 24/06/2018). NT : La bande passante s'exprime en bits/seconde.	

base de données	Database, DB
Collection de données organisées de façon à être facilement accessibles, administrées et mises à jour. RF : https://www.lemagit.fr/definition/Base-de-donnees (consulté le 24/06/2018).	
BitTorrent	BitTorrent
Système pair-à-pair de partage et de distribution de fichiers ayant vu le jour en 2001. RF : Willy Malvaut-Martiarena, « Vers une architecture pair-à-pair pour l'informatique dans le nuage », Université de Grenoble, 2011, p. 42.	
Bullrun, programme Bullrun	Bullrun
Programme lancé au début des années 2000 par la NSA ayant pour objectif de contourner les différents systèmes de chiffrement des informations. RF : https://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html?xtmc=cybersurveillance&xtcr=14 (consulté le 24/06/2018).	
chiffrement	encryption
Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8387607 (consulté le 24/06/2018).	
Clearnet	Clearnet
Par opposition au Darknet, partie ouverte et non chiffrée du réseau. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 163. EXP : La majeure partie du contenu situé sur le deep web appartient au Clearnet.	
cluster, grappe	cluster
(Freenet) Ensemble de fichiers regroupés sur le même nœud grâce à leur proximité lexicographique. RF : Laurent Gayard, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018, p. 170. EXP : Les clusters participent à l'optimisation du réseau Freenet. USG : Bien que « cluster » soit un anglicisme, c'est le terme le plus employé dans la littérature consacrée à Freenet.	
confidentialité	confidentiality, secrecy
Fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé. RF : https://www.journaldunet.com/solutions/expert/62755/ne-confondons-plus-confidentialite-avec-securite.shtml (consulté le 24/06/2018).	
contenu dynamique	dynamic content
Contenu d'un site capable de s'adapter automatiquement à divers contextes prédéfinis. RF : https://www.textbroker.fr/contenus-dynamiques (consulté le 24/06/2018).	
contrôle d'intégrité	integrity control, integrity check
Contrôle exercé sur les logiciels et les données afin d'assurer que les données appropriées sont utilisées, que le traitement de celles-ci ne comporte pas d'erreur et que les programmes ne sont pas susceptibles d'être manipulés sans autorisation. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=503115 (consulté le 24/06/2018).	
cryptographie	cryptography
Ensemble des techniques qui assurent l'inviolabilité de textes et, en informatique, de données. RF : https://www.larousse.fr/dictionnaires/francais/cryptographie/20864 (consulté le 24/06/2018).	

cryptographie symétrique, cryptographie à clé secrète, chiffrement symétrique, chiffrement à clé secrète	symmetric-key cryptography, secret-key cryptography, symmetric encryption, secret-key encryption
Cryptographie dans laquelle la même clé est utilisée pour chiffrer et déchiffrer les données. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8383536 (consulté le 24/06/2018). EXP : La cryptographie symétrique s'oppose à la cryptographie asymétrique, ou à clé publique, dans laquelle la clé utilisée pour chiffrer le message n'est pas la même que celle utilisée pour le déchiffrer.	
cycle d'instruction, cycle CPU	instruction cycle, CPU cycle
Cycle durant lequel le microprocesseur récupère une instruction en mémoire, la décode et l'exécute. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8373585 (consulté le 24/06/2018). USG : « cycle CPU » est un anglicisme, à éviter.	
dark web	dark Web
Ensemble des sites web d'un darknet. RF : Rayna Stamboliyska, *La face cachée d'Internet*, Paris, Larousse, 2017, p. 244.	
DES, algorithme DES, norme de chiffrement des données, norme DES	DES, Data Encryption Standard, DES algorithm
Algorithme de chiffrement à clé secrète adopté comme standard aux États-Unis en 1977. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 164. EXP : Initialement conçu pour utiliser une clé de 112 bits, l'algorithme d'IBM a vu sa taille réduite à 56 bits après un passage par la NSA. En 2001, il a été remplacé par l'algorithme AES.	
disque dur	hard drive, hard disk drive, HDD
Élément scellé qui stocke les données non volatiles de l'ordinateur. RF : Scott Mueller, *Le PC, architecture, maintenance et mise à niveau*, Paris, Pearson France, 2008, p. 451.	
durée de vie, durée de vie du paquet	Time To Live, TTL, IP time-to-live
Paramètre appliqué à un datagramme lors de son expédition en multidiffusion dans Internet, permettant de fixer l'étendue des informations qu'il contient et de limiter sa propagation. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8392720 (consulté le 24/06/2018).	
Electric Frontier Foundation, EFF	Electric Frontier Foundation, EFF
Organisation à but non lucratif fondée aux États-Unis en 1990, ayant pour objet la préservation de la liberté d'expression et la défense du droit à la confidentialité sur Internet. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 164. EXP : Depuis 2004, l'EFF participe au financement de Tor.	
espace de noms, espace de nommage	namespace
Compilation de noms, identifiée par un identificateur de ressource uniforme, qui sont utilisés dans des documents rédigés en XML en tant que noms d'éléments et noms d'attributs. RF : Règlement (CE) no 1205/2008 de la Commission du 3 décembre 2008 portant sur les modalités d'application de la directive 2007/2/CE du Parlement européen et du Conseil en ce qui concerne les métadonnées, disponible sur <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:326:0012:0030:FR:PDF> (consulté le 24/06/2018).	

fonction de hachage, algorithme de hachage	hash function, message digest function, hash algorithm, message digest algorithm
Fonction mathématique qui permet de transformer une chaîne de caractères d'une longueur indifférente en une autre chaîne de longueur fixe. RF : https://bitcoin.fr/quest-ce-quune-fonction-de-hachage/ (consulté le 24/06/2018).	
Fonction OU exclusif, OU exclusif, XOR, opération XOR	XOR, exclusive or
Opérateur logique de l'algèbre de Boole. À deux opérandes qui peuvent avoir chacun la valeur vrai ou faux, elle associe un résultat qui a lui-même la valeur vrai seulement si les deux opérandes ont des valeurs distinctes. RF : Adel S. Sedra et Kenneth C. Smith, *Circuits microélectroniques*, Louvain-la-Neuve, De Boecke Supérieur, 2016, p. 1209.	
Freemail	Freemail
Service permettant d'avoir une boîte mail anonyme sur Freenet. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 65.	
Freenet	Freenet
Réseau anonyme et distribué qui vise à permettre une liberté d'expression et d'information totale fondée sur la sécurité de l'anonymat. RF : https://tkpx.wordpress.com/2017/11/29/darknet-freenet-zeronet-et-i2p/ (consulté le 24/06/2018).	
friend-to-friend, F2F, ami-à-ami	friend-to-friend, F2F
Se dit d'un réseau où les échanges sont limités aux amis, c'est-à-dire à un ensemble d'individus spécifiquement sélectionnés. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 165. EXP : Les réseaux Freenet et Retroshare peuvent être réglés pour fonctionner en mode F2F. USG : « ami-à-ami » n'est que peu attesté dans les ouvrages spécialisés, à éviter.	
HTTP, protocole de transfert hypertexte, *Hypertext Transfer Protocol*	HTTP, Hypertext Transfer Protocol
Protocole de communication entre un client et un serveur pour le World Wide Web. RF : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203581-http-hypertext-transfert-protocol-definition-traduction/ (consulté le 24/06/2018).	
HTTPS, protocole de transfert hypertexte sécurisé, *Hypertext Transfer Protocol Secure*	HTTPS, Hypertext Transfer Protocol Secure
Variante sécurisée et chiffrée du HTTP. RF : Jean-Phillipe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 165. EXP : HTTPS est basé sur le protocole SSL ou TLS.	
hyperlien, lien hypertexte	hyperlink, hypertext link
Élément placé dans le contenu d'une page Web et qui permet, en cliquant dessus, d'accéder à un autre contenu sur le même site Web (lien interne) ou à un site Web différent (lien externe). RF : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203435-lien-hypertexte-definition-traduction/ (consulté le 24/06/2018).	

intranet	intranet
Réseau informatique mis en place au sein d'une entreprise ou de toute autre entité équivalente. RF : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203375-intranet-definition/ (consulté le 24/06/2018). EXP : Les intranets utilisent l'infrastructure d'Internet. Ils font généralement partie du deep web.	
magasin, magasin de données, datastore	datastore
(Freenet) Espace de stockage rendu disponible en lecture/écriture pour les autres nœuds. Il contient les adresses des nœuds auxquels il est connecté ainsi que les clés pour déchiffrer les données. RF : Laurent Gayard, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018, p. 106. EXP : Lorsque l'espace disponible du magasin est saturé, les fichiers qui n'ont pas été utilisés depuis longtemps sont supprimés. USG : « datastore » est un anglicisme, à éviter.	
métadonnée	metadata
Donnée contenant des informations sur d'autres données. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 165. EXP1 : On entend ainsi par métadonnées notamment le nom du fichier, le type de données qu'il contient, le nom du programme utilisé pour le créer, le nom de l'utilisateur propriétaire du fichier sur le système, les droits d'accès, les dates de sa création et de sa dernière modification et le nom de l'utilisateur associé, la date de la dernière lecture et le nom de l'utilisateur associé, etc. EXP2 : La liste exacte des métadonnées change d'un système informatique à l'autre. NT : « métadonnée » s'emploie le plus souvent au pluriel.	
mise en miroir, écriture miroir, réplication, mirroring	mirroring
Forme de redondance de stockage dans laquelle au moins deux copies identiques des données sont conservées sur des volumes distincts. RF : https://www.symantec.com/fr/fr/security_response/glossary/define.jsp?letter=m&word=mirroring (consulté le 24/06/2018). USG : « mirroring » est un anglicisme, à éviter.	
mix network, mixnet	mix network, mixnet
Structure réseau associant l'utilisation de relais et le chiffrement en couches pour dissimuler l'origine des communications et le contenu des échanges. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 166. EXP : Les mix networks ont été inventés en 1981 par David Chaum. Tor est une forme de mixnet.	
moteur de recherche	search engine
Programme qui indexe le contenu de différentes ressources Internet, plus particulièrement de sites Web, et qui permet, à l'aide d'un navigateur Web, de rechercher de l'information selon différents paramètres, en se servant de mots-clés, ou par des requêtes en texte libre, et d'avoir accès à l'information ainsi trouvée. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=2075047 (consulté le 24/06/2018).	

navigateur, navigateur web, logiciel de navigation	browser, Web browser, Internet browser
Logiciel qui permet de consulter sur Internet les pages Web et de circuler dans les différents moteurs de recherche. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=506713 (consulté le 24/06/2018). USG : « logiciel de navigation » est recommandé officiellement par la Commission d'enrichissement de la langue française depuis 1999 (Journal officiel du 16 mars 1999, vocabulaire de l'informatique et de l'internet). Cependant, il n'est pas entré dans l'usage et risque d'introduire une ambiguïté, dans la mesure où il peut également se rapporter à des outils de navigation maritime.	
nœud, nœud de réseau	node, network node
Dans un réseau, tout point constituant un carrefour d'où les informations sont acheminées. RF : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8391135 (consulté le 24/06/2018). NT : Sur Freenet, les nœuds sont constitués par les ordinateurs des utilisateurs eux-mêmes et permettent l'acheminement et le stockage des données.	
NSA, Agence pour la sécurité nationale, Agence de sécurité nationale américaine	NSA, National Security Agency
Agence de renseignement américaine spécialisée dans le renseignement électronique, la cryptographie et le traitement des systèmes d'information. RF : Laurent Gayard, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018, p. 174.	
nombre de sauts maximum, hops-to-live, HTL	hops-to-live, HTL
(Freenet) Durée de vie des requêtes. RF : Mohamed Bakhouya, *Approche auto-adaptative à base d'agents mobiles et inspirée du système immunitaire de l'Homme pour la découverte de services dans les réseaux à grande échelle*, Université de Franche-Comté, 2005, p. 21. EXP : Le nombre de sauts maximum est déterminé au moment de la formulation de la requête. Il fait écho à la durée de vie dans le protocole IP. USG : Bien qu'il soit d'usage courant, « hops-to-live » est un anglicisme à éviter.	
pair à pair, pair-à-pair, poste à poste, P2P, peer-to-peer	peer-to-peer, P2P
Se dit du mode d'utilisation d'un réseau dans lequel chacun des participants connectés dispose des mêmes droits et qui permet un échange direct de services sans recourir à un serveur central ; par extension, se dit d'un tel réseau. RF : JORF n° 0121 du 23 mai 2017, Vocabulaire de l'informatique, accessible sur <https://tinyurl.com/ydeqwqx4> (consulté le 25/06/2018). EXP : Les protocoles d'échange de fichiers comme Gnutella ou BitTorrent ainsi que certains darknets comme Freenet ou I2P sont des réseaux pair à pair. USG : « pair à pair » est le terme officiellement recommandé par la Commission d'enrichissement de la langue française depuis le 23 mai 2017 et remplace ainsi « poste à poste » ; « P2P » et « peer-to-peer » sont des anglicismes, à éviter.	

paquet, paquet de données, paquet IP, datagramme IP	packet, data packet, IP packet, IP datagram
Unité fondamentale de transfert de données entre appareils de transmission dans la couche réseau. RF : http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=PAQUET+DONNEES&index=alt&codom2nd_wet=1#resultrecs (consulté le 25/06/2018). EXP : Un paquet est composé de l'adresse de l'ordinateur d'origine, de celle de l'ordinateur destinataire, et de données, le tout respectant le protocole Internet. USG : Bien que « datagramme » soit plus précis que « paquet », c'est ce dernier terme qui est le plus employé.	
Pluggable Transports	Pluggable Transports
Mode de fonctionnement du réseau Tor permettant de dissimuler le trafic aux systèmes de *Deep Packet Inspection*. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 59. CTX : Il est possible de dissimuler son utilisation de Tor en activant le mode *Pluggable Transports*.	
point de défaillance unique, SPOF	single point of failure, SPOF
Élément dans une infrastructure donnée qui, s'il venait à défaillir, pourrait entraîner la chute du système. RF : https://www.lebigdata.fr/spof-definition (consulté le 25/06/2018). EXP : Le point de défaillance unique peut tout aussi bien être une personne, une étape d'un processus, qu'un composant d'une infrastructure.	
porte dérobée, trappe, porte dissimulée, backdoor	backdoor, trapdoor
Accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel. RF : https://www.cnil.fr/fr/definition/porte-derobee-ou-backdoor (consulté le 25/06/2018). EXP : L'activation d'une porte dérobée peut se faire au moyen d'un logiciel malveillant de type vers qui va exploiter une faille de sécurité dans le produit et se propager automatiquement à tous les ordinateurs d'un réseau. GRM : « backdoor », nom masculin en français.	
PRISM	PRISM
Programme de la NSA permettant d'accéder sans restriction à toutes les informations hébergées et traitées par les géants du web. RF : https://www.numerama.com/magazine/26171-prism-la-nsa-a-acces-aux-donnees-de-tous-les-geants-du-web.html (consulté le 25/06/2018). EXP : Le programme PRISM utilise des portes dérobées pour récupérer les informations. Sont concernés par PRISM : Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube (filiale de Google), Skype (filiale de Microsoft), AOL et Apple.	
protocole	protocol
Mode de communication entre deux équipements qui définit notamment le format des données et le mode d'association des éléments qui souhaitent échanger. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 167. EXP : Les deux protocoles les plus courants sur Internet sont TCP/IP et HTTP.	

recherche par escalade, recherche *hill-climbing*	hill-climbing search, hill-climbing strategy
Stratégie de recherche qui, au cours de l'exploration d'un graphe, consiste à essayer d'atteindre un but en choisissant les nœuds que l'on juge les plus proches de ce but. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8353524 (consulté le 26/06/2018). USG : « recherche *hill-climbing* » est un anglicisme, à éviter.	
redondance, redondance informatique	redundancy, computer redundancy
Duplication d'un élément essentiel au fonctionnement normal du système informatique, en vue de pallier la défaillance éventuelle de cet élément et d'assurer ainsi la continuité d'une fonction informatique vitale. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8355467 (consulté le 26/06/2018). EXP : La redondance en sécurité informatique peut s'appliquer aussi bien à un centre informatique qu'à des éléments d'information, à des matériels, à des installations de sécurité, à des procédures et aux éléments vitaux d'une machine.	
référencement, indexation	referencing, registration
Différentes techniques utilisées pour améliorer la position d'un site internet dans les pages de résultats affichées par les moteurs de recherche en réponse aux requêtes des internautes. RF : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203541-referencement-definition-traduction/ (consulté le 26/06/2018). EXP : Le référencement d'un site Web se fait, selon l'outil de recherche, en précisant l'adresse URL du site et l'adresse de courriel du webmestre, ou en ajoutant d'autres informations telles que le titre de la page d'accueil, un texte descriptif, une catégorie, quelques mots-clés, etc.	
réplication asynchrone	lazy replication, optimistic replication
Type de réplication dans laquelle la copie ne se fait pas en temps réel, mais en décalé. RF : http://www.journaldunet.com/solutions/0301/030127_faq_replication.shtml (consulté le 26/06/2018). EXP : La réplication asynchrone est largement répandue au sein des systèmes pair-à-pair.	
Retroshare	Retroshare
Réseau chiffré de type F2F utilisant le standard OpenPGP. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 73. EXP : Retroshare offre un service de partage de fichiers, une messagerie instantanée, des forums de discussion ainsi qu'un client mail.	
robot d'indexation, collecteur	crawler, spider, web crawler, web spider
Composante logicielle d'un moteur de recherche qui balaie en permanence le Web afin de détecter les pages Web, d'en extraire et d'en analyser le contenu, et d'alimenter l'index du moteur de recherche. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=2074825 (consulté le 26/06/2018). USG : « collecteur », recommandé officiellement depuis 2013 par la Commission d'enrichissement de la langue française.	

serveur mandataire, proxy	proxy, proxy server
Dispositif informatique associé à un serveur et réalisant, pour des applications autorisées, des fonctions de médiation, telle que le stockage des documents les plus fréquemment demandés ou l'établissement de passerelles. RF : http://www.marche-public.fr/Marches-publics/Textes/Definition/Definition-informatique-internet-19990316.htm (consulté le 26/06/2018). USG : « serveur mandataire », recommandé depuis 1999 par la Commission d'enrichissement de la langue française ; « proxy », anglicisme beaucoup plus répandu dans la littérature spécialisée.	
services oignons, services cachés, *hidden services*	onion services, hidden services
Services qui ne sont accessibles que par le réseau Tor. RF : https://tb-manual.torproject.org/fr/onion-services.html (consulté le 26/06/2018). EXP : L'adresse IP des services oignons est chiffrée, ce qui signifie que le trafic entre les utilisateurs de Tor et ces services est chiffré de bout en bout. USG : Torproject recommande dorénavant d'utiliser « services oignons » et non plus « services cachés » ; « *hidden services* » est un anglicisme à éviter.	
signalisation hors-bande	out-of-band signaling
Voie de signalisation utilisant une fréquence différente du signal audio. RF : David Bensoussan, *Téléphonie numérique et téléphonie IP*, Québec, Presses de l'Université du Québec, 2008, p. 57. EXP : La signalisation hors-bande peut s'effectuer via une fréquence inférieure à 300 Hz ou supérieure à 3 400 Hz.	
Silk Road	Silk Road
Plate-forme de mise en relation des vendeurs et acheteurs de stupéfiants. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 115. EXP : Situé sur le dark web de Tor, Silk Road a ouvert en 2011 et a été fermé par le FBI en 2013.	
table de routage	routing table
Table associée à un routeur, qui contient les indications sur le chemin que doivent emprunter les paquets de données, à travers un réseau, pour arriver à leur destination. RF : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8871947 (consulté le 26/06/2018).	
table de routage dynamique	dynamic routing table
Table de routage générée à partir des informations échangées par des protocoles de routage. RF : Michel Dutreix, *Unix : administration système AIX, HP-UX, Solaris, Linux*, Paris, ENI Éditions, 2003, p. 275. EXP : Le routage dynamique permet à un routeur d'échanger des informations de routage avec les routeurs avoisinants. Dès qu'un routeur est informé d'une modification quelconque de la configuration sur les réseaux (telle que l'arrêt d'un routeur), il transmet ces informations aux routeurs avoisinants. ANT : table de routage statique	
Tails (*The Amnesic Incognito Live System*)	Tails (*The Amnesic Incognito Live System*)
Système d'exploitation live basé sur Linux conçu pour offrir la meilleur garantie d'anonymat. RF : Jean-Philippe Rennard, *Darknet*, Paris, Ellipses, 2016, p. 167.	

TCP/IP	TCP/IP
Ensemble des protocoles utilisés pour le transfert et l'échange de données sur Internet. RF : Laurent Gayard, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018, p. 175.	
Telecomix	Telecomix
Groupe décentralisé de cybermilitants engagés en faveur de la liberté d'expression. RF : https://fr.wikipedia.org/wiki/Telecomix (consulté le 26/06/2018).	
Tor, *the onion router*	Tor, the onion router
Réseau informatique décentralisé permettant l'anonymat des clients. RF : https://doc.ubuntu-fr.org/tor (consulté le 26/06/2018).	
URL (*Uniform Resource Locator*)	URL (Uniform Resource Locator)
Adresse d'une ressource du web, sous la forme d'une chaîne de caractères. RF : https://www.linternaute.fr/dictionnaire/fr/definition/url/ (consulté le 26/06/2016).	
web, World Wide Web, toile d'araignée mondiale	Web, World Wide Web
Système hypertexte fonctionnant sur Internet, permettant, grâce à un navigateur, de consulter pages et sites Internet hébergés sur le réseau mondial. RF : Laurent Gayard, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018, p. 175. EXP : Le World Wide Web a été créé en 1990 par Tim Berners-Lee et Robert Cailliau. USG : « toile d'araignée mondiale », très peu employé par les spécialistes, est recommandé depuis 1999 par la Commission d'enrichissement de la langue française. NT : L'usage de la majuscule en français, recommandé par l'Office québécois de la langue française, fait débat.	
XKeyscore	XKeyscore
Outil central du système de renseignement américain, permettant d'examiner quasiment tout ce que fait un individu sur Internet. RF : https://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html?xtmc=cybersurveillance&xtcr=14 (consulté le 26/06/2018). EXP : XKeyscore, créé par la NSA, est opéré conjointement par les services de renseignement américains, britanniques, canadiens, australiens et néo-zélandais (les « *Five Eyes* »).	

3) Lexiques

Les termes faisant l'objet d'une fiche terminologique sont signalés en gras souligné, ceux définis dans le glossaire sont indiqués en gras.

a) Lexique anglais-français

Anglais	**Synonymes**	**Français**
adaptive		auto-adaptatif
Advanced Encryption Standard	AES, Rijndael	AES
AES	Advanced Encryption Standard, Rijndael	AES
anonymity		anonymat
ARPANET		ARPANET
asymmetric cipher	public-key cryptography, public-key encryption, asymmetric encryption, asymmetric cryptography, public-key cipher	cryptographie asymétrique
asymmetric cryptography	public-key cryptography, public-key encryption, asymmetric encryption, public-key cipher, asymmetric cipher	cryptographie asymétrique
asymmetric encryption	public-key cryptography, public-key encryption, asymmetric cryptography, public-key cipher, asymmetric cipher	cryptographie asymétrique
availability		disponibilité
backdoor	trapdoor	porte dérobée
bandwidth		bande passante
Big Data		Big Data
binary		binaire
Bitcoin		Bitcoin
BitTorrent		BitTorrent
blockchain		chaîne de blocs

browser	Web browser, Internet browser	navigateur
Bullrun		Bullrun
CHK	content-hash key	Clé CHK
Clearnet		Clearnet
client-server architecture	client-server model	architecture client-serveur
client-server model	client-server-architecture	architecture client-serveur
cluster		cluster
collision		collision
computer redundancy	redundancy	redondance
confidentiality	secrecy, privacy	confidentialité
content-hash key	CHK	clé CHK
CPU cycle	instruction cycle	cycle d'instruction
crawler	spider, Web crawler, Web spider	robot d'indexation
cryptocurrency		crypto-monnaie
cryptography		cryptographie
cyberdissident	hacktivist	cyberdissident
cybersecurity		cybersécurité
dark Web		dark web
Darknet		Darknet
data		données
Data Encryption Standard	DES, DES Algorithm	DES
data packet	packet, IP packet, IP datagram	paquet
database	DB	base de données
datastore		magasin
DB	database	base de données
decryption key		clé de déchiffrement

deep Web	invisible Web, hidden Web	deep web
denial of service attack	DoS attack, saturation attack	attaque par déni de service
DES	Data Encryption Standard, DES Algorithm	DES
DES Algorithm	DES, Data Encryption Standard	
descriptive string		chaîne descriptive
DHT	distributed hash table	table de hachage distribuée
dictionary attack		attaque par dictionnaire
digest	hash, message digest, digital fingerprint	empreinte
digital fingerprint	hash, digest, message digest	empreinte
digital signature		signature numérique
directory		dossier
disk space	storage space	espace de stockage
distributed architecture	DNA	architecture distribuée
distributed hash table	DHT	table de hachage distribuée
DNA	distributed architecture	architecture distribuée
DNS	Domain Name System	système des noms de domaine
Domain Name System	DNS	système des noms de domaine
DoS attack	denial of service attack, saturation attack	attaque par déni de service
dynamic content		contenu dynamique
dynamic routing table		table de routage dynamique
EFF	Electric Frontier Foundation	Electric Frontier Foundation
Electric Frontier Foundation	EFF	Electric Frontier Foundation
encrypted		chiffré
encryption		chiffrement

encryption key		clé de chiffrement
entry node		nœud d'entrée
exclusive or	XOR	fonction OU exclusif
exit node		nœud de sortie
F2F	friend-to-friend	friend-to-friend
failure		échec
Freemail		Freemail
Freenet		Freenet
friend-to-friend	F2F	friend-to-friend
hacktivist	cyberdissident	cyberdissident
hard disk drive	hard drive, HDD	disque dur
hard drive	hard disk drive, HDD	disque dur
hash	message digest, digest, digital fingerprint	empreinte
hash algorithm	hash function, function, message digest function, message digest algorithm	fonction de hachage
hash coding	hashing	hachage
hash function	message digest function, hash algorithm, message digest algorithm	fonction de hachage
hashing	hash coding	hachage
HDD	hard drive, hard disk drive	disque dur
hidden services	onion services	services oignons
hidden Web	deep Web, invisible Web	deep web
hill-climbing search	hill-climbing strategy	recherche par escalade
hill-climbing strategy	hill-climbing search	recherche par escalade
hops-to-live	HTL	nombre de sauts maximum

HTL	hops-to-live	nombre de sauts maximum
HTTP	Hypertext Transfer Protocol	HTTP
HTTPS	Hypertext Transfer Protocol Secure	HTTPS
hyperlink	hypertext link	hyperlien
hypertext link	hyperlink	hyperlien
Hypertext Transfer Protocol	HTTP	HTTP
Hypertext Transfer Protocol Secure	HTTPS	HTTPS
indirect addressing	indirection mechanism	adressage indirect
indirect file		fichier indirect
indirection mechanism	indirect addressing	adressage indirect
insert		dépôt
instruction cycle	CPU cycle	cycle d'instruction
integrity check	integrity control	contrôle d'intégrité
integrity control	integrity check	contrôle d'intégrité
Internet browser	browser, Web browser	navigateur
Internet of things		Internet des objets
Internet Service Provider		fournisseur d'accès à Internet, FAI
invisible Web	deep Web, hidden Web	deep web
IP address		adresse IP
IP datagram	packet, data packet, IP packet,	paquet
IP packet	packet, data packet, IP datagram	paquet
IP time-to-live	TTL, Time To Live	durée de vie
junk file		fichier indésirable
keyword-signed key	KSK	clé KSK
kile key		clé de fichier
KSK	keyword-signed key	clé KSK

layer (of encryption)		couche (de chiffrement)
lazy replication	optimistic replication	réplication asynchrone
local cache		cache local
loop		boucle
man-in-the-middle attack	MITM	attaque de l'homme du milieu
message digest	hash, digest, digital fingerprint	empreinte
message digest algorithm	hash function, hash algorithm, message digest function	fonction de hachage
message digest function	hash function, hash algorithm, message digest algorithm	fonction de hachage
metadata		métadonnée
mining		minage
mirroring		mise en miroir
MITM	man-in-the-middle attack	attaque de l'homme du milieu
mix network	mixnet	mix network
mixnet	mix network	mix network
namespace		espace de noms
National Security Agency	NSA	NSA
network		réseau
network node	node	nœud
node	network node	nœud
node operator		opérateur de nœud
NSA	National Security Agency	NSA
onion services	hidden services	services oignons
optimistic replication	lazy replication	réplication asynchrone
out-of-band signaling		signalisation hors-bande
overlay network	SDN overlay	réseau superposé

P2P	peer-to-peer	pair à pair
packet	data packet, IP packet, IP datagram	paquet
peer-to-peer	P2P	pair à pair
PGP	Pretty Good Privacy	PGP
plausible denial		déni plausible
Pluggable Transports		*Pluggable Transports*
PoW	proof of work	preuve de travail
PRISM		PRISM
privacy	confidentiality, secrecy	confidentialité
private key		clé privée
proof of work	PoW	preuve de travail
protocol		protocole
proxy	proxy server	serveur mandataire
proxy chain		chaîne de serveurs mandataires
proxy server	proxy	serveur mandataire
public key		clé publique
public-key cipher	public-key cryptography, public-key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher	cryptographie asymétrique
public-key cryptography	public-key encryption, asymmetric encryption, asymmetric cryptography, public-key cipher, asymmetric cipher	cryptographie asymétrique
public-key encryption	public-key cryptography, asymmetric encryption, asymmetric cryptography, public-key cipher, asymmetric cipher	cryptographie asymétrique
redundancy	computer redundancy	redondance
referencing	registration	référencement

registration	referencing	référencement
relay		relais
request		requête
retrieval		récupération
Retroshare		Retroshare
Rijndael	AES, Advanced Encryption Standard	AES
routing table		table de routage
saturation attack	DoS attack, denial of service attack	attaque par déni de service
SDN overlay	overlay network	réseau superposé
search engine		moteur de recherche
secrecy	confidentiality, privacy	confidentialité
secret-key cryptography	symmetric-key cryptography, symmetric encryption, secret-key encryption	cryptographie asymétrique
secret-key encryption	symmetric-key cryptography, secret-key cryptography, symmetric encryption	cryptographie asymétrique
Secure Hash Algorithm	SHA	SHA
Secure Socket Layer/Transport Layer Security	SSL/TLS	SSL/TLS
server		serveur
SHA	Secure Hash Algorithm	SHA
signed-subspace key	SSK	clé SSK
Silk Road		Silk Road
single point of failure	SPOF	point de défaillance unique
source code		code source
spider	crawler, web crawler, web spider	
splitting		fragmentation
SPOF	single point of failure	point de défaillance unique

spyware		logiciel espion
SSK	signed-subspace key	clé SSK
SSL/TLS	Secure Socket Layer/Transport Layer Security	SSL/TLS
storage		stockage
storage space	disk space	espace de stockage
surface Web		web de surface
symmetric encryption	symmetric-key cryptography, secret-key cryptography, secret-key encryption	cryptographie asymétrique
symmetric-key cryptography	secret-key cryptography, symmetric encryption, secret-key encryption	cryptographie asymétrique
Tails	The Amnesic Incognito Live System	Tails
TCP/IP		TCP/IP
Telecomix		Telecomix
The Amnesic Incognito Live System	Tails	Tails
The Onion Router	Tor	Tor
Time To Live	TTL, IP time-to-live	durée de vie
to cache		mettre en cache
to cipher	to encrypt	chiffrer
to decipher	to decrypt	déchiffrer
to decrypt	to decipher	déchiffrer
to encrypt	to cipher	chiffrer
to host (a file)		héberger (un fichier)
to query		interroger
to download	to retrieve	récupérer

to retrieve	to download	récupérer
Tor	The Onion Router	Tor
traffic analysis		analyse du trafic
trapdoor	backdoor	porte dérobée
TTL	Time To Live, IP time-to-live	durée de vie
Uniform Resource Locator	URL	URL
updating		mise à jour
URL	Uniform Resource Locator	URL
Virtual Private Network	VPN	réseau privé virtuel
VPN	Virtual Private Network	réseau privé virtuel
Web	World Wide Web	web
Web browser	browser, Internet browser	navigateur
Web crawler	crawler, Web crawler, Web spider	
Web of trust		toile de confiance
Web spider	crawler, spider, Web crawler	
XKeyscore		XKeyscore
XOR	exclusive or	fonction OU exclusif

b) Lexique français-anglais

Français	**Synonymes**	**Anglais**
adressage indirect		indirection mechanism
adresse IP		IP address
AES	algorithme AES, Rijndael, norme de chiffrement avancé, norme AES, standard de chiffrement avancé	AES
algorithme AES	AES, Rijndael, norme de chiffrement avancé, norme AES, standard de chiffrement avancé	AES
algorithme de hachage	fonction de hachage	hash function
algorithme DES	DES, norme de chiffrement des données, norme DES	DES
analyse du trafic		traffic analysis
anonymat		anonymity
architecture client-serveur	modèle client-serveur, environnement client-serveur	client-server architecture
architecture décentralisée	architecture distribuée, architecture répartie	client-server architecture
architecture distribuée	architecture répartie, architecture décentralisée	distributed architecture
architecture répartie	architecture distribuée, architecture décentralisée	client-server architecture
ARPANET		ARPANET
attaque de l'homme du milieu		man-in-the-middle-attack
attaque DoS	attaque par déni de service, attaque par refus de service, attaque par saturation	DoS attack
attaque par déni de service	attaque DoS, attaque par refus de service, attaque par saturation	DoS attack
attaque par dictionnaire		dictionary attack

attaque par refus de service	attaque DoS, attaque par déni de service, attaque par saturation	DoS attack
attaque par saturation	attaque par déni de service, attaque DoS, attaque par refus de service,	DoS attack
auto-adaptatif		adaptive
bande passante		bandwidth
base de données		database
Big Data		Big Data
binaire		binary
Bitcoin		Bitcoin
BitTorrent		BitTorrent
blockchain	chaîne de blocs	blockchain
boucle		loop
Bullrun	programme Bullrun	Bullrun
cache local		local cache
chaîne de blocs	blockchain	blockchain
chaîne de proxy	chaîne de serveurs mandataires	proxy chain
chaîne de serveurs mandataires	chaîne de proxy	proxy chain
chaîne descriptive		descriptive chain
chiffrage à clé publique	cryptographie asymétrique, chiffrement asymétrique, chiffrement à clé publique, chiffrage asymétrique	public-key cryptography
chiffrage asymétrique	cryptographie asymétrique, chiffrement asymétrique, chiffrement à clé publique, chiffrage à clé publique	public-key cryptography
chiffré		encrypted
chiffrement		encryption

chiffrement à clé publique	cryptographie asymétrique, chiffrement asymétrique, chiffrage à clé publique, chiffrage asymétrique	public-key cryptography
chiffrement à clé secrète	cryptographie symétrique, cryptographie à clé secrète, chiffrement symétrique,	symmetric-key cryptography
chiffrement asymétrique	cryptographie asymétrique, chiffrement à clé publique, chiffrage à clé publique, chiffrage asymétrique	public-key cryptography
chiffrement symétrique	cryptographie symétrique, cryptographie à clé secrète, chiffrement à clé secrète	symmetric-key cryptography
chiffrer		to encrypt
clé CHK		content-hash-key
clé de chiffrement		encryption key
clé de déchiffrement		decryption key
clé de fichier		file key
clé KSK		keyword-signed-key
clé privée		private key
clé publique		public key
clé SSK		signed-subspace key
Clearnet		Clearnet
cluster	grappe	cluster
code source		source code
collecteur	robot d'indexation	crawler
collision		collision
condensat	empreinte, condensé, hash	hash
condensé	empreinte, condensat, hash	hash
confidentialité		confidentiality

contenu dynamique		dynamic content
contrôle d'intégrité		integrity control
couche (de chiffrement)		layer (of encryption)
cryptographie		cryptography
cryptographie à clé secrète	cryptographie symétrique, chiffrement symétrique, chiffrement à clé secrète	symmetric-key cryptography
cryptographie asymétrique	chiffrement asymétrique, chiffrement à clé publique, chiffrage à clé publique, chiffrage asymétrique	public-key cryptography
cryptographie symétrique	cryptographie à clé secrète, chiffrement symétrique, chiffrement à clé secrète	symmetric-key cryptography
crypto-monnaie		cryptocurrency
cyberdissident	dissident en ligne, hacktiviste	cyberdissident
cybersécurité		cybersecurity
cycle d'instruction		CPU cycle
dark web		dark Web
Darknet		Darknet
datagramme IP	paquet, paquet de données, paquet IP	packet
déchiffrer		to decrypt
deep web		deep Web
déni plausible		plausible denial
dépôt	insertion	insert
DES	algorithme DES, norme de chiffrement des données, norme DES	DES
disponibilité		availability
disque dur		hard drive

dissident en ligne	cyberdissident, hacktiviste	cyberdissident
données		data
dossier		directory
durée de vie	durée de vie du paquet	time-to-live
durée de vie du paquet	durée de vie	time-to-live
échec		failure
écriture miroir	mise en miroir, réplication	mirroring
EFF	Electric Frontier Foundation	Electric Frontier Foundation
Electric Frontier Foundation	EFF	Electric Frontier Foundation
empreinte	condensé, condensat, hash	hash
environnement client-serveur	architecture client-serveur, modèle client-serveur,	client-server architecture
espace de nommage	espace de noms	namespace
espace de noms	espace de nommage	namespace
espace de stockage		disk space
F2F	friend-to-friend	friend-to-friend
fichier indésirable		junk file
fichier indirect		indirect file
fonction de hachage	algorithme de hachage	hash function
fonction OU exclusif	OU exclusif, XOR, opération XOR	XOR
fournisseur d'accès à Internet, FAI		Internet Service Provider
fragmentation		splitting
Freemail		Freemail
Freenet		Freenet
friend-to-friend	F2F	friend-to-friend
grappe	cluster	cluster

hachage		hashing
hacktiviste	cyberdissident, dissident en ligne	cyberdissident
hash	empreinte, condensé, condensat	hash
héberger (un fichier)		to host (a file)
hops-to-live	nombre de sauts maximum, HTL	hops-to-live
HTL	nombre de sauts maximum, hops-to-live	hops-to-live
HTTP	protocole de transfert hypertexte	HTTP
HTTPS	protocole de transfert hypertexte sécurisé	HTTPS
hyperlien	lien hypertexte	hyperlink
indexation	référencement	referencing
insertion	dépôt	insert
Internet des objets		Internet of things
interroger		to query
logiciel espion	spyware	spyware
magasin	magasin de données	datastore
magasin de données	magasin	datastore
métadonnée		metadata
mettre en cache		to cache
minage		mining
mise à jour		updating
mise en miroir	écriture miroir, réplication	mirroring
mix network	mixnet	mix network
modèle client-serveur	architecture client-serveur, environnement client-serveur	client-server architecture

moteur de recherche		search engine
National Security Agency	NSA	NSA
navigateur	navigateur web	browser
navigateur web	navigateur	browser
nœud		node
nœud d'entrée		entry node
nœud de sortie		exit node
nombre de sauts maximum	hops-to-live, HTL	hops-to-live
norme AES	AES, algorithme AES, Rijndael, norme de chiffrement avancé, standard de chiffrement avancé	AES
norme de chiffrement avancé	AES, algorithme AES, Rijndael, norme AES, standard de chiffrement avancé	AES
norme de chiffrement des données	DES, algorithme DES, norme DES	DES
norme DES	DES, algorithme DES, norme de chiffrement des données	DES
NSA	National Security Agency	NSA
opérateur de nœud		node operator
opération XOR	fonction OU exclusif, OU exclusif, XOR	XOR
OU exclusif	fonction OU exclusif, XOR, opération XOR	XOR
P2P	pair à pair, pair-à-pair, poste à poste, peer-to-peer	peer-to-peer
pair à pair	pair-à-pair, poste à poste, P2P, peer-to-peer	peer-to-peer
pair-à-pair	pair à pair, poste à poste, P2P, peer-to-peer	peer-to-peer
paquet	paquet de données, paquet IP, datagramme IP	packet

paquet de données	paquet, paquet IP, datagramme IP	packet
paquet IP	paquet, paquet de données, datagramme IP	packet
peer-to-peer	pair à pair, pair-à-pair, poste à poste, P2P	peer-to-peer
PGP	Pretty Good Privacy	PGP
Pluggable Transports		Pluggable Transports
point de défaillance unique	SPOF	single point of failure
porte dérobée	trappe, porte dissimulée	backdoor
porte dissimulée	trappe, porte dérobée	backdoor
poste à poste	pair à pair, pair-à-pair, P2P, peer-to-peer	peer-to-peer
Pretty Good Privacy	PGP	PGP
preuve de travail		proof of work
PRISM		PRISM
programme Bullrun		Bullrun
protocole		protocol
protocole de transfert hypertexte	HTTP	HTTP
protocole de transfert hypertexte sécurisé	HTTPS	HTTPS
proxy	serveur mandataire	proxy
recherche *hill-climbing*	recherche par escalade	hill-climbing search
recherche par escalade	recherche *hill-climbing*	hill-climbing search
récupération	téléchargement	retrieval
récupérer	télécharger	to retrieve
redondance	redondance informatique	redundancy
redondance informatique	redondance	redundancy
référencement	indexation	referencing

relais		relay
réplication	mise en miroir, écriture miroir	mirroring
réplication asynchrone		lazy replication
requête		request
réseau		network
réseau overlay	réseau superposé	overlay network
réseau privé virtuel	VPN	VPN
réseau superposé	réseau overlay	overlay network
Retroshare		Retroshare
Rijndael	AES, algorithme AES, norme de chiffrement avancé, norme AES, standard de chiffrement avancé	AES
robot d'indexation	collecteur	crawler
Secure Hash Algorithm	SHA	SHA
Secure Socket Layer/Transport Layer Security	SSL/TLS	SSL/TLS
serveur		server
serveur mandataire	proxy	proxy
services cachés	services oignons	onion services
services oignons	services cachés	onion services
SHA	Secure Hash Algorithm	SHA
signalisation hors-bande		out-of-band signaling
signature numérique		digital signature
Silk Road		Silk Road
SPOF	point de défaillance unique	single point of failure
spyware	logiciel espion	spyware

SSL/TLS	Secure Socket Layer/Transport Layer Security	SSL/TLS
standard de chiffrement avancé	AES, algorithme AES, Rijndael, norme de chiffrement avancé, norme AES	AES
stockage		storage
système des noms de domaine		DNS
table de hachage distribuée		distributed hash table
table de routage		routing table
table de routage dynamique		dynamic routing table
Tails		Tails
TCP/IP		TCP/IP
téléchargement	récupération	retrieval
télécharger	récupérer	to retrieve
Telecomix		Telecomix
The onion router	Tor	Tor
toile d'araignée mondiale	web, World Wide Web	Web
toile de confiance		Web of trust
Tor	*The onion router*	Tor
trappe	porte dérobée, porte dissimulée	backdoor
URL		URL
VPN	réseau privé virtuel	VPN
web	World Wide Web, toile d'araignée mondiale	Web
web de surface	web surfacique, web indexable, web visible	surface Web
web indexable	web de surface, web surfacique, web visible	surface Web
web surfacique	web de surface, web indexable, web visible	surface Web

web visible	web de surface, web surfacique, web indexable	surface Web
World Wide Web	web, toile d'araignée mondiale	Web
XKeyscore		XKeyscore
XOR	fonction OU exclusif, OU exclusif, opération XOR	XOR

Bibliographie

Avertissement au lecteur : les références incontournables pour aborder le Darknet sont signalées par le symbole  .

1) Sources en anglais

a) Ouvrages

 BARTLETT, Jamie, *The Dark Net*, New York, Melville House, 2015. Excellent ouvrage d'immersion dans l'univers du Darknet. Jamie Bartlett y livre une enquête de terrain solide et remet dans leur contexte les pratiques qui y sont décrites.

SENKER, Cath, *Cybercrime and the Darknet*, London, Arcturus, 2016. Comme l'indique le titre, cet ouvrage dépasse le strict cadre du Darknet et étudie également le crime en ligne. La partie consacrée au Darknet est digne d'intérêt et assez exhaustive : le côté obscur du dark web, mais également les revendications libertaires à l'origine du Darknet y sont expliqués.

b) Articles

BERGMAN, Michael K., « The Deep Web : Surfacing Hidden Value », *Journal of Electric Publishing*, 7 (1), 2001. Cet article fait encore autorité aujourd'hui bien qu'il commence à dater. Très intéressant pour qui veut comprendre le deep web et le fonctionnement des moteurs de recherche. On y trouve également une estimation du rapport entre deep web et web de surface.

BIDDLE, Peter *et al*., « The Darknet and the Future of Content Distribution », in *Digital Rights Managment*, Lecture Notes in Computer Science, vol. 2770, 2003, p. 344-365. Article fondateur qui introduit pour la première fois la notion de « Darknet », compris comme l'ensemble des réseaux décentralisés permettant de partager du contenu. Ce texte est cependant aujourd'hui obsolète.

GOLLNICK, Clare & WILSON, Emily, « Separating Fact From Fiction : The Truth about the Dark Web », Terbium Labs, 2016. Étude solide et argumentée sur les usages du dark web. Les auteures reviennent longuement sur la méthode adoptée et les termes employés sont définis.

MADDOX, Alexia, « Constructive activism in the dark web : cryptomarkets and illicit drugs in the digital 'demimonde' », *Information,Communication & Society*, 1-16, 2015. Cette étude originale est le résultat d'un long travail de terrain réalisé auprès des utilisateurs de feu Silk Road. Elle met en lumière un aspect souvent ignoré par les médias : le dark web comme lieu d'engagement politique et de construction d'une société numérique alternative.

MANSFIELD-DEVINE, Steve, « Darknets », in Computer Fraud and Security, 9 (12), p. 4-7, 2009. Bien qu'il soit bref, cet article est très éclairant. L'auteur y définit ce qui caractérise le Darknet et aborde rapidement la question de son usage. Pédagogique, ce texte s'adresse également aux néophytes.

MOORE, Daniel & RID, Thomas, « Cryptopolitik and the Darknet », Survival, 58:1, p. 7-38, 2016. Article de grande qualité qui analyse en détail le développement de la cryptographie informatique et l'usage du réseau Tor en analysant leurs enjeux d'un point de vue sociopolitique pour les gouvernements et pour les citoyens. Peu technique, ce texte est très abordable.

c) Ressources web

ARGONNE NATIONAL LABORATORY, DarkNet Terminology : Definitions of the DarkNet, the Dark Web, and the Deep Web, disponible sur <https://coar.risc.anl.gov/coar-attends-department-of-homeland-security-hosted-darknet-summit/> (consulté le 28/06/2018). Ce court article est intéressant pour son glossaire et l'illustration des rapports entre deep web, dark web et Darknet. Les auteurs évoquent Tor, Freenet et I2P.

DEEP DOT WEB, Jolly Roger's Security Guide for Beginners, disponible sur <https://www.deepdotweb.com/> (consulté le 28/06/2018). Manuel d'introduction aux différents outils permettant l'anonymat et la confidentialité, dont Tor, PGP, Tails et les VPN. Très clair et accessible.

DUKI DROR & TZACHI SCHIFF, Down the Deep, Dark Web, disponible sur <https://www.youtube.com/watch?v=y7rYLuMJy5g> (consulté le 28/06/2018). Malgré sa tendance au sensationnalisme, ce documentaire permet d'appréhender les enjeux du Darknet et de la cryptographie grâce à une bonne remise en contexte et l'interview de nombreux activistes.

ROLLING STONE, The Darknet : Is the Government Destroying 'the Wild West of the Internet'?, disponible sur <https://www.rollingstone.com/politics/politics-news/the-darknet-is-the-government-destroying-the-wild-west-of-the-internet-198271/> (consulté le 28/06/2018). Cet article fleuve retrace l'avènement de Tor, son utilisation par les dissidents politiques et les tentatives des agences de renseignement américaines d'en décrypter les communications.

THE TOR PROJECT, disponible sur <https://www.torproject.org/> (consulté le 28/06/2018). Site officiel de Tor, très riche en ressources pour comprendre le fonctionnement de ce darknet (documentation, FAQ, articles de presse sur le sujet, forum…).

THE FREENET PROJECT, About, disponible sur <https://freenetproject.org> (consulté le 28/06/2018). Site officiel de Freenet, où l'on trouve des explications sur le fonctionnement de ce système et des conseils pour protéger son anonymat sur Internet. Certaines ressources sont disponibles en français.

WIRED, Hacker Lexicon : What is the Dark Web, disponible sur <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/> (consulté le 28/06/2018). Article synthétique et accessible qui définit clairement le dark web et le distingue du deep web. L'auteur y explique le fonctionnement des mixnets en s'intéressant au réseau Tor.

2) Sources en français

a) Ouvrages

CHATELAIN, Yannick, *Surfez couvert !*, Paris, Ellipses, 2015. Clairement engagé pour la défense de la vie privée, Yannick Chatelain revient dans ce livre sur le bras de fer que se livrent depuis les années 1990 les hacktivistes et les gouvernements quant à la cryptographie. L'auteur y donne quelques conseils pratiques pour protéger sa vie privée en ligne.

GAYARD, Laurent, *Géopolitique du Darknet*, Paris, ISTE Éditions, 2018. Excellent ouvrage à mi-chemin entre l'histoire et la sociologie. L'auteur décrit clairement les enjeux posés

par la cryptographie et le Darknet et nous livre une histoire détaillée de ce dernier. Cet ouvrage est très didactique.

RENNARD, Jean-Philippe, *Darknet, mythes et réalités*, Paris, Ellipses, 2016. La référence absolue parmi les études francophones sur le Darknet. Très complet, ce livre revient longuement sur les techniques de cryptographie, les différents darknets, les crypto-monnaies et les enjeux politiques de l'anonymat et de la confidentialité en ligne. Souvent technique, ce livre reste difficile d'accès pour qui n'a pas les bases mathématiques sur lesquelles reposent la cryptographie.

STAMBOLIYSKA, Rayna, *La face cachée d'Internet*, Paris, Larousse, 2017. Ce livre consacré aux pratiques « alternatives » sur Internet (Anonymous, hackers, Darknet…) dépasse le cadre du Darknet. Un chapitre entier (environ 80 pages) lui est cependant consacré. Très clair et bien documenté, cet ouvrage constitue une bonne introduction à l'autre Internet.

b) Articles

VALETTE, Jean-Jacques, « Plongée dans le dark net », *We demain*, vol. 15, p. 30-35, 2016. Dans cet article immersif, l'auteur recense les différentes ressources qu'il est possible de trouver sur le dark web. Bien documenté et accessible, ce texte explique également le fonctionnement de Tor.

c) Ressources web

COLLECTIF, Guide d'autodéfense numérique, disponible sur <https://guide.boum.org/> (consulté le 28/06/2018). Rédigé par différents acteurs de la communauté du libre, cet ouvrage en deux volumes est un véritable manuel de protection de la vie privée. Très didactique et complet, ce livre aborde notamment les protocoles de communication Internet, la cryptographie asymétrique et le réseau Tor.

FRANCE CULTURE, Adieu Darknet, Bonjour Librenet, disponible sur <https://www.franceculture.fr/emissions/la-methode-scientifique/adieu-darknet-bonjour-librenet> (consulté le 28/06/2018). Cette émission, à laquelle participent Jean-Philippe Rennard et Amaelle Guiton, est une présentation générale du Darknet. Claire et accessible, elle s'adresse

surtout aux néophytes. La proposition de traduction, à laquelle le titre de l'émission fait référence, est tout à fait intéressante.

NUMERAMA, Non, le Darknet n'est pas un réseau « clandestin », disponible sur <https://www.numerama.com/politique/292452-non-le-darknet-nest-pas-un-reseau-clandestin.html> (consulté le 28/06/2018). Particulièrement intéressant pour les linguistes, cet article critique la traduction officielle de *Darknet* retenue par la Commission d'enrichissement de la langue française. Après avoir défini le Darknet, l'auteur montre pourquoi cette traduction fortement connotée n'est pas recevable.

RENNARD, Qu'est-ce que le Darknet ?, disponible sur <http://www.rennard.org/Darknet/presentation.html> (consulté le 28/06/2018). Cet article est une synthèse de l'ouvrage *Darknet, mythes et réalités*. Plus accessible, il se révèlera intéressant si l'on souhaite se faire une idée d'ensemble de ce phénomène sans trop entrer dans les détails.

TOILE DE FOND, Du deep web au dark web : immersion dans les abysses du web, disponible sur < https://toiledefond.net/deep-web-abysses-du-web/> (consulté le 28/06/2018). Bien documenté, ce texte présente objectivement le dark web, qu'il distingue clairement du deep web tout en relativisant les discours alarmistes à ce sujet.

Index