La théorie du Darknet

Philippe Davadie
Membre de la Chaire Cybersécurité & Cyberdéfense

juin 2015, Article n°IV.7

Qu'est-ce qu'un *darknet* ?

Évolution de la définition

Employer dans une conversation le terme *darknet* suscite presque immédiatement une polémique, tant le terme est controversé. Pour certains, le *darknet* serait la face cachée (dark) de l'Internet (net), pour d'autres, ce serait une zone de non-droit du cyberespace (net) dans laquelle ne se commettraient que des activités illégales (dark). Pour d'autres encore, ce serait un mélange des deux.
Avant de poursuivre, il est indispensable de préciser la définition de certains termes qui sont confondus avec le terme *darknet* : le deep web, le web invisible, le web profond et le web caché. Ces quatre termes sont synonymes les uns des autres et recouvrent la partie de l'Internet accessible en ligne mais non indexée par le moteurs de recherche classiques généralistes (Google, Yahoo !, etc.). Il convient cependant d'être prudent, et de bien préciser que le web invisible est inaccessible aux moteurs de recherche classiques, car de plus en plus de moteurs de recherche spécifiques se développent. Ainsi le moteur de recherche shodan[1], créé en 2009, référence l'ensemble des objets connectés à l'Internet, quelle que soit leur destination.
Le *darknet* fascine, les recherches effectuées sur ce terme via Google ont d'ailleurs fortement augmenté ces derniers temps :

[1] Ainsi nommé d'après Sentient Hyper-Optimized Data Access Network (réseau sensible d'accès aux données hyper optimisé) qui est le nom d'une intelligence artificielle, principal ennemi, dans les jeux vidéo System Shock et System Shock2.

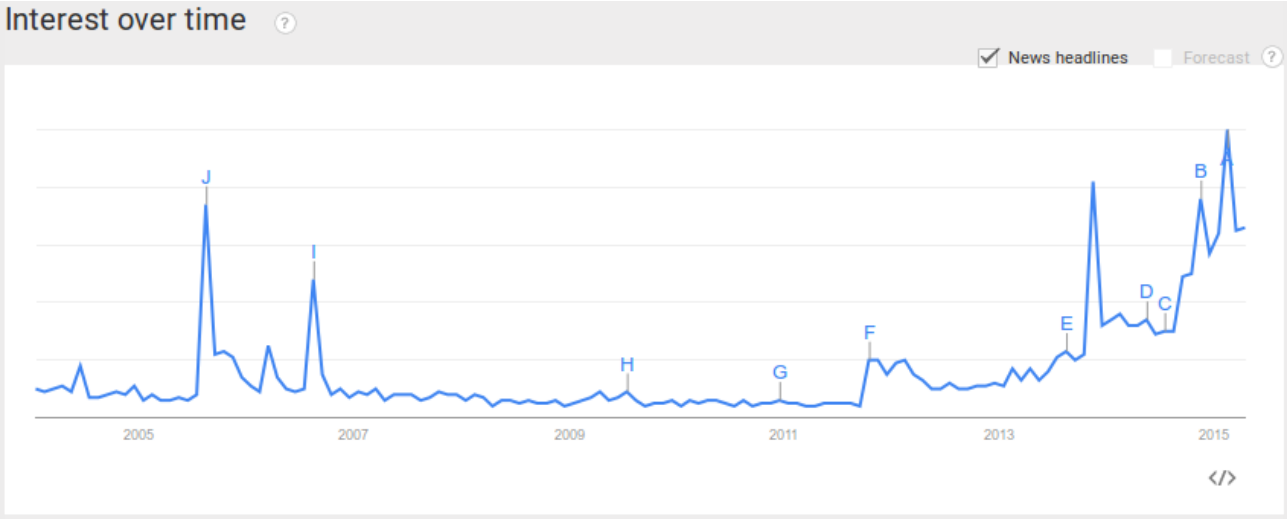

Illustration 1: Requêtes du terme darknet depuis 2005 (Google Trends)

Cette illustration, partielle car ne recensant que les requêtes effectuées via Google, peut interroger, dans la mesure où deux pics apparaissent en 2005 et 2006 avant de laisser la place à une raréfaction des recherches, puis une reprise à partir de 2012. Cela peut s'expliquer par la parution d'un livre de Joseph Daniel Lasica en 2005 intitulé *Darknet, la guerre d'Hollywood contre la génération numérique*. Par la suite, l'intérêt a pu retomber, avant de reprendre fin 2011 avec notamment l'opération Darknet menée par le collectif Anonymous que nous exposerons infra.
En faisant abstraction des pics de requêtes, nous remarquons que la tendance est à l'augmentation du nombre de recherche du terme *darknet*.

Qu'en est-il exactement ?

Si l'on consulte l'histoire, somme toute récente de l'Internet, il apparaît que le terme *darknet* a été créé dans les années 1970 pour identifier les réseaux que leurs utilisateurs souhaitaient déconnecter volontairement d'Arpanet.
Selon Andrew Lewman, directeur exécutif du projet Tor (The Onion Router) jusqu'en avril 2015, *« le terme darknet provient d'une présentation faite par Google ou Alta Vista – si vous vous souvenez de ce moteur de recherche d'il y a 15 ans – sur le sujet des données cachées derrière des péages, des écrans de connexion, dans les réseaux d'entreprise. Et si votre objectif est de rechercher toute l'information disponible, ce qui pour vous est sombre (dark) est tout ce à quoi vous ne pouvez accéder. »* [Lew] À cette époque ce qui s'y cachait du public n'était donc pas forcément illégal. Nous nous rendons compte que le terme *darknet* représentait pour les auteurs de cette présentation ce que nous appelons maintenant web invisible.
En 2002, il a été repris par Peter Biddle, Paul England, Marcus Peinado et Bryan Willman, tous quatre employés de Microsoft pour expliquer dans un article [Bid] que ce type de réseaux nuisait à la protection du droit d'auteur et que le développement des DRM (gestion des droits numériques) pouvait les contrer. Le terme *darknet* y est défini de la manière suivante : *« un ensemble de réseaux et de techniques utilisés pour partager du contenu numérique. Le darknet n'est pas un réseau physiquement à part, mais une couche applicative et de protocole qui fonctionne sur des réseaux préexistants. »* Si cette définition ne suggère rien d'illégal, le contexte d'emploi du terme oriente vers le contraire : le *darknet* favoriserait l'illégalité.
En 2011, Symon Aked définit un *darknet* ainsi : « les darknets sont des réseaux de données cryptées

qui assurent la confidentialité (interception, modification, observation, lecture) envers les tierces parties. Ils peuvent aussi être conçus pour assurer à leurs membres l'anonymat ou un pseudo-anonymat lorsqu'ils le souhaitent. » [Ake]

Au vu de ces divergences d'opinion, il semble difficile de poser une définition faisant l'unanimité. Andrew Lewman estime aussi que *« le terme darknet est inapproprié ; le réseau est souvent qualifié de sombre (dark) parce que les moteurs de recherche ne peuvent le voir. »* [Lew]

Quel que soit le rapport à la légalité suggéré par les différentes définitions, nous pouvons remarquer que dans toutes ces présentations du terme, la mise à l'écart du reste de l'Internet est un dénominateur commun.
Cette mise à l'écart est soulignée par Anne Souvira, chef de la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), pour qui les *darknets* sont des réseaux privés, « *souvent très sécurisés pour en limiter l'accès* », et protégés par mots de passe, certificats, captchas, etc. [GSM]. D'accès réservé, on ne peut y accéder que sur recommandation, quelle que soit la forme de celle-ci. Les *darknets* sont donc à distinguer du *deepweb*, celui-ci ayant été étudié par ailleurs [Ber2].

Le darknet est-il forcément illégal ?

Cette restriction d'accès nourrit la croyance selon laquelle les *darknets* seraient forcément des repaires de trafics illégaux. C'est ainsi qu'aux théories du complot dans le monde réel fait écho la théorie du *darknet* dans le cyberespace. Il est cependant certain qu'une telle restriction d'accès au réseau est une condition (nécessaire mais pas suffisante) pour faire prospérer des activités illégales. Aked écrit d'ailleurs : *« Les sites internet des média, tant techniques que non techniques, font des darknets des paradis pour le partage clandestin de fichiers. Ils sont souvent nimbés d'une aura mystique ; là où tout type de contenu n'est qu'à un clic de souris. »* [Ake]
On trouve effectivement dans ces réseaux tout ce qui constitue les activités illégales et criminelles : vente et échanges d'informations confidentielles, articles contrefaits (cigarettes, faux papiers, etc.), collecte de fonds au profit d'organisations criminelles, pédopornographie, « pirates à gage » (comme il existe des tueurs à gage), sites vitrines d'organisations malfaisantes, logiciels malfaisants, trafics d'armes et de drogues, etc.

L'illustration ci-dessous le prouve.

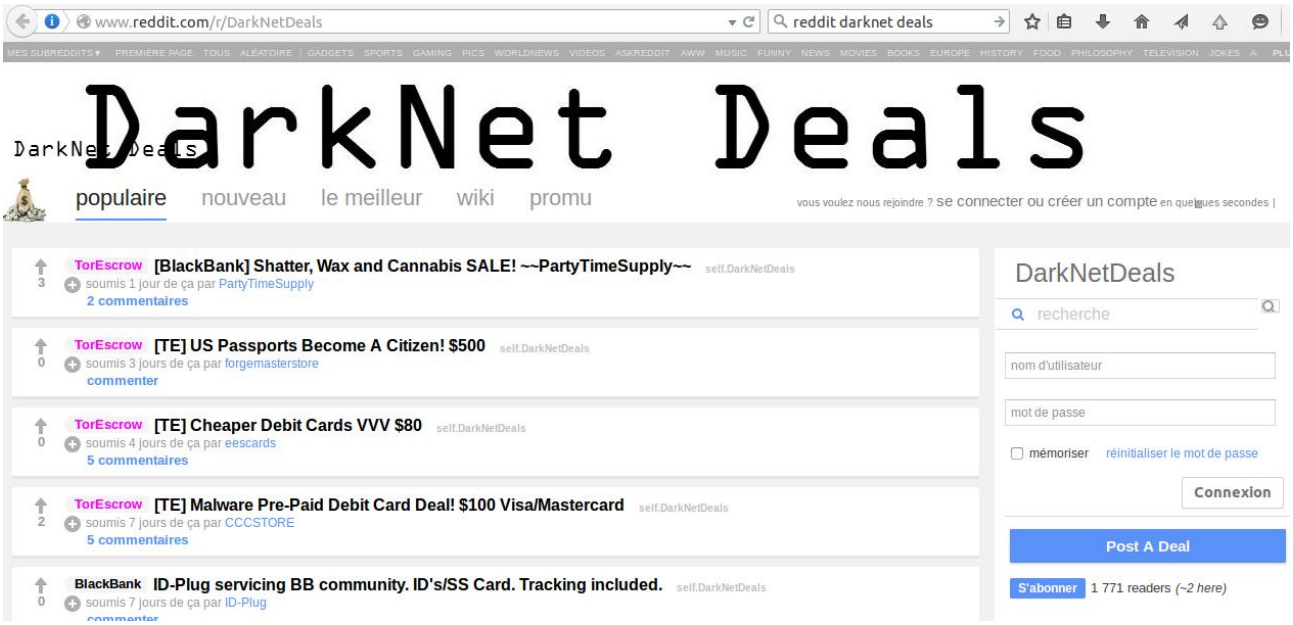

Illustration 2: Ventes possibles via des darknets

L'existence de ces réseaux protégés permet aux criminels de développer leurs activités avec le sentiment d'une certaine impunité, ce qui les a poussés à mettre au point des forums spécialisés[2]. Ce développement a été mis en avant dans le rapport de la RAND *Markets for Cybercrime Tools and Stolen Data*[3] publié en 2014. Il en ressort que ces places de marché se sont organisées et sont devenues des prolongements de ce qui se fait dans le monde réel de la criminalité. Selon Michael Callahan, vice-président marketing des produits de sécurité chez Juniper Networks, ce serait un signe de maturité de ce type d'économie : *« L'étude de la RAND montre que si une économie remplit les critères suivants : élaborée, spécialisée, fiable, accessible et résiliente, alors elle a atteint la maturité. »* [Rand]

De la possibilité de réaliser des affaires criminelles dans les *darknets* à la généralisation de l'affirmation selon laquelle toute personne naviguant dans les *darknets* est un malfaiteur, il n'y a qu'un pas, qu'il serait cependant précipité d'accomplir. En effet, les malfaiteurs ne sont pas les seuls à hanter ces réseaux, puisque l'enquête sous pseudonyme[4] permet aux enquêteurs de les infiltrer, qu'ils sont aussi l'objet de l'attention de certains scientifiques et enfin, on ne peut nier le fait que certains internautes les consultent par simple curiosité.
Symon Aked relativise cette vision négative des *darnets* en précisant [Ake] *« Le centre du crime de haute technologie australien estime que « les darknets peuvent être détournés par des cybercriminels qui y distribuent de façon sécurisée leur propagande, des images pédopornographiques, ou des fichiers numériques protégés par le droit d'auteur pour être à l'abri des agences de lutte contre le crime. »*

De plus, rien n'empêche plusieurs personnes honnêtes de créer un *darknet* afin de communiquer entre elles en toute sécurité, à propos d'un projet légal, tel le lancement d'un nouveau produit.

---

[2] Cf. page http://www.informationweek.com/cybercrime-black-markets-grow-up/d/d-id/1127911

[3] Téléchargeable via le site http://www.rand.org/pubs/research_reports/RR610.html

[4] Prévue par l'article 706-87-1 du Code de procédure pénale.

Pour toutes les raisons exposées précédemment, la définition du *darknet* que propose wikipedia semble pertinente. Selon wikipedia le *darknet* est un *réseau privé virtuel dont les utilisateurs sont considérés comme des personnes de confiance. La plupart du temps, ces réseaux sont de petite taille, souvent avec moins de dix utilisateurs chacun. Un darknet peut être créé par n'importe quel type de personne et pour n'importe quel objectif, mais la technique est le plus souvent utilisée spécifiquement pour créer des réseaux de partage de fichiers en pair à pair anonymes.*
Les darknets sont distincts des autres réseaux pair à pair distribués car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas partagées publiquement) et donc les utilisateurs peuvent communiquer avec peu de crainte d'interférence gouvernementale ou d'entreprise.
Notons cependant que l'utilisation du terme *confiance* semble inadaptée, plus particulièrement dans le cas où le darknet est utilisé par des criminels d'obédiences différentes.

Outils et mécanismes

Entrer dans le darknet

Si l'on se base sur les travaux déjà cités de Biddle, England, Peinado et Willman [Bid], certains *darknets* ont utilisé des logiciels conçus pour l'échange de fichiers de type pair à pair tels que Napster et Gnutella. Ce dernier logiciel a dû être abandonné, car selon ces auteurs, il ne permettait pas de préserver l'anonymat.
Il semble qu'actuellement, Freenet (réseau informatique anonyme et réparti fonctionnant comme un espace de stockage partagé et réparti) [Ake], I2P (réseau anonyme offrant une simple couche réseau logicielle de type réseau *overlay* que les applications peuvent employer pour envoyer, via une communication chiffrée de bout en bout, des informations entre elles) [Ake] et GNUnet (réseau pair à pair garantissant l'anonymat) soient les plus utilisés. D'autres logiciels permettent la création de tels réseaux, comme Retroshare (libre) et SafetyGate Invisible (commercial).

Évoquer les *darknets* nécessite d'évoquer Tor, logiciel fortement associé au *darknet* et qui cristallise beaucoup de remarques négatives et d'efforts de rétro-ingénierie afin d'en percer les secrets.
Une recherche du terme *darknet* via google trends montre d'ailleurs que ceux qui recherchent ce terme l'associent fortement avec Tor.

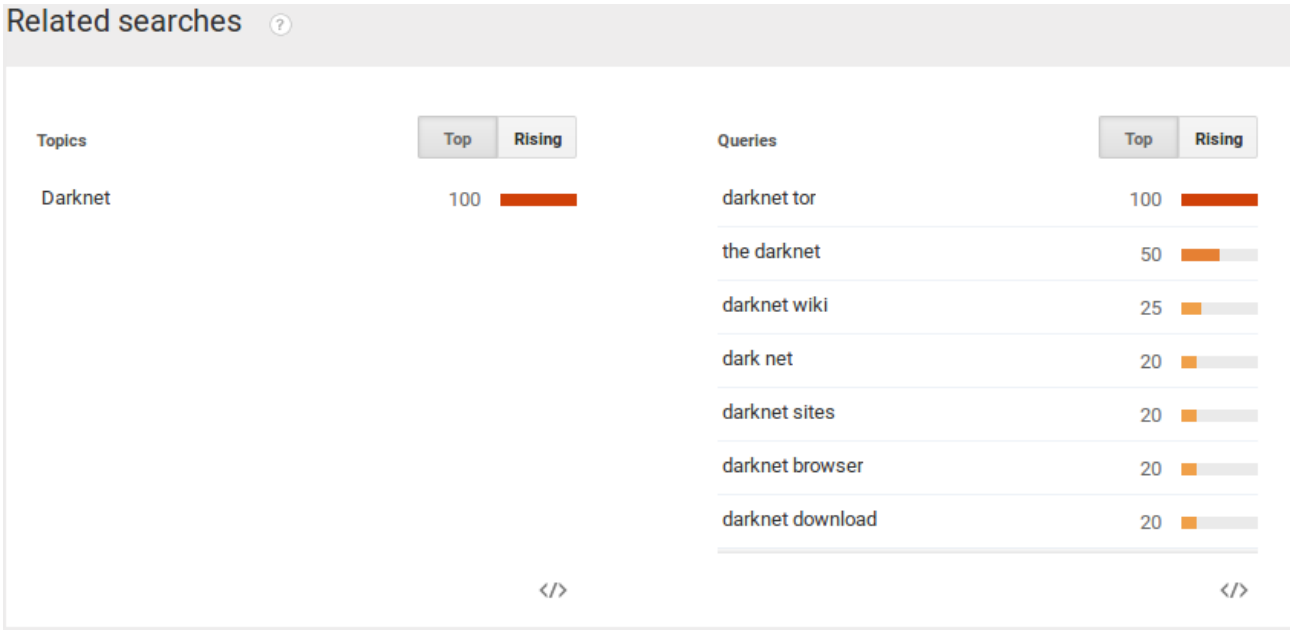

Illustration 3: Requêtes associées au terme darknet (Google Trends)

Alors que le protocole majoritairement utilisé sur l'Internet est HTTP (Hyper Text Transfer Protocol), Tor utilise son propre protocole et Andrew Lewman le définit comme un *« navigateur anonyme qui vous permet de contrôler vos données personnelles. »* Le même ajoute : *« Tor existe pour préserver la liberté de l'Internet et rendre aux internautes la maîtrise de leurs données. C'est ce que nous continuerons de faire, et nos recherches iront dans ce sens. »* [Lew]
D'après les estimations d'Andrew Lewman, Tor serait utilisé quotidiennement par environ 2,5 millions de personnes, localisées principalement aux USA et en Europe où la protection de la vie privée est un sujet de préoccupation [Lew].
N'utiliser que Tor ne permet cependant pas de garantir une confidentialité totale des échanges et des usages. Andrew Lewman explique que *« je pense que si votre seul adversaire est la NSA ou le GCHQ, alors vous avez probablement déjà perdu la bataille, parce que ce sont des agences disposant de plusieurs millions de dollars, de moyens fantastiques, face à un seul outil… De même que vous ne pouvez pas construire une maison avec seulement un marteau, il vous faut une boîte à outils complète et des savoir-faire pour battre de tels adversaires. »* [Lew]
Pour maximiser le temps durant lequel la confidentialité sera préservée, il est conseillé d'utiliser des VPN en plus de Tor. Deux possibilités sont offertes à l'utilisateur :
- se connecter à un VPN d'abord, puis à Tor. Le chemin suivi est : l'ordinateur, le VPN, Tor puis l'Internet. Le FAI ignore que vous êtes connecté à Tor, et votre VPN ne peut pas suivre votre activité.
- se connecter à Tor d'abord, puis au VPN. Le chemin suivi devient : l'ordinateur, Tor, le VPN, l'Internet. Le VPN ne connaît donc pas votre adresse IP, et les éventuels logs du VPN sont protégés pas Tor. Cette solution renforce l'anonymat.

Plusieurs acteurs se positionnent sur la technologie utilisable pour créer un *darknet*. Mozilla s'est engagé à œuvrer au projet Polaris avec d'autres acteurs du Web concernés par les questions de vie privée pour *« collaborer plus efficacement, plus explicitement et plus directement »* et ainsi intégrer *« davantage de fonctions liées à la vie privée dans nos produits. »* [Moz] Cet engagement a fait suite aux résultats d'un sondage réalisé en octobre 2014 sur un échantillon de plus de 7000

internautes adultes qui montrait que selon 74 % d'entre eux, la protection de la vie privée sur la toile avait régressé en un an et que les principaux acteurs de l'Internet connaissaient trop de faits privés sur eux.

Naviguer à partir du darknet

Une fois le *darknet* créé et l'anonymat préservé, se pose la question de la navigation sur la toile. En effet, alterner la navigation dans le *darknet* et celle sur la toile ouverte est de nature à compromettre, à terme, l'anonymat. Ces techniques et logiciels ne peuvent donc suffire. Une fois le *darknet* créé, il faut s'y maintenir et y trouver des fonctions similaires à celles proposées sur l'Internet public.
Cependant, comme les *darknets* ont pour caractéristique un secret certain, on ne peut y accéder via les moteurs de recherche publics. Il est nécessaire de passer par des wiki cachés ou *hidden wiki* qui sont notamment des annuaires d'adresses de sites répartis dans les *darknets*. On peut également utiliser des moteurs de recherche spécialisés tels que Grams, dont l'ergonomie est proche de celle de Google.

Illustration 4: Présentation de la page d'accès de Grams

Le créateur de Grams déclarait d'ailleurs : *« je travaille sur l'algorithme afin qu'il ressemble à celui de Google, il aura un système de notation fondé sur sa popularité, le nombre de transactions, le nombre d'avis positifs. Ainsi, vous verrez d'abord les plus populaires. Je vais ajouter un filtre sur les sites marchands cette semaine afin qu'un utilisateur ne recherche que les sites dans lesquels il a un compte. J'ai écrit le code pour le convertisseur de devises mais ne l'ai pas encore implémenté. »* [Red] L'URL d'accès à ce navigateur est : *URL-grams7enufi7jmdl.onion*

On peut également utiliser *onion city*, le moteur de recherche de Tor http://onion.city/ qui au bout d'une semaine indexait déjà 350000 pages.

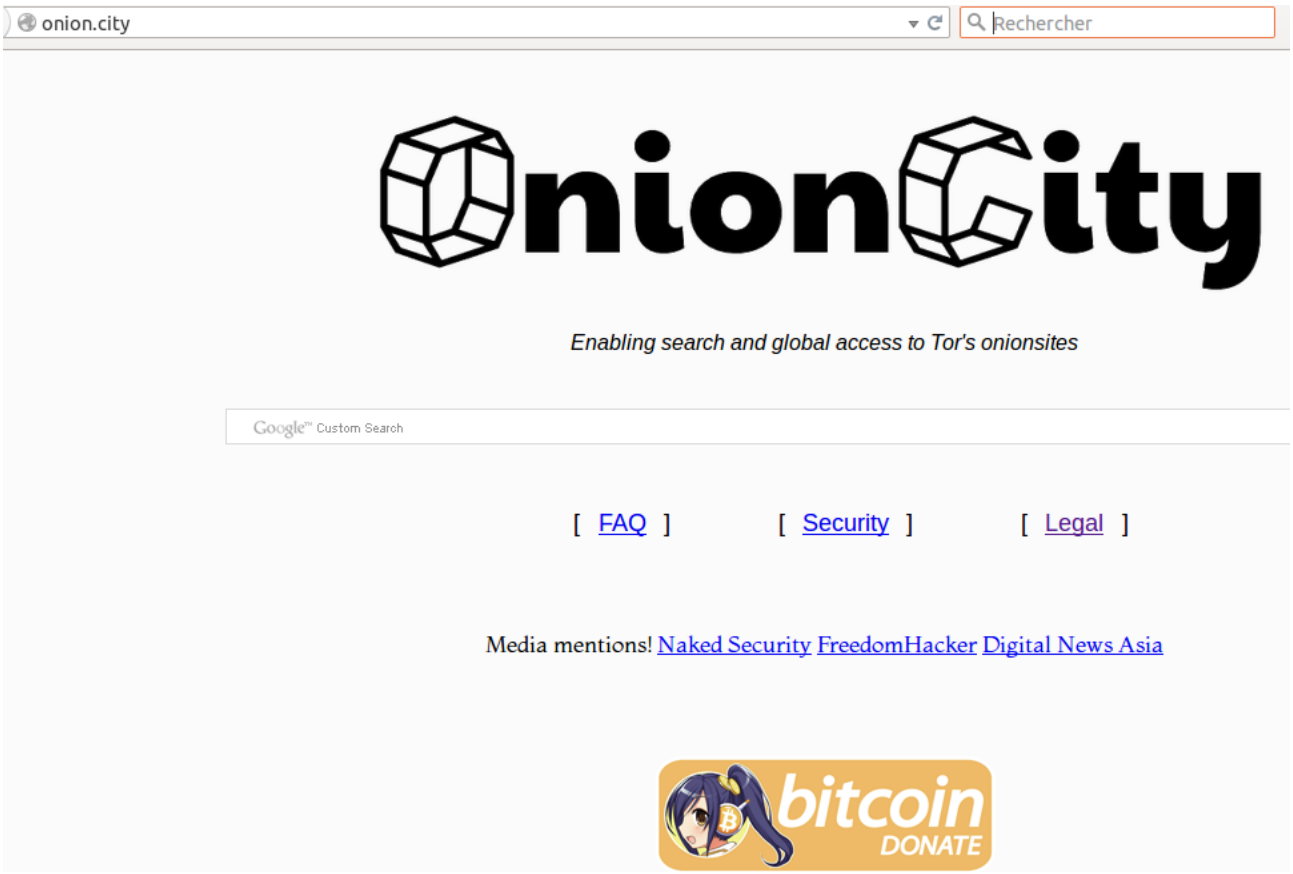

Illustration 5: Page d'accueil d'onion city

Controverses

Les *darknets* ne peuvent que susciter la controverse à une époque où les intrusions de plus en plus fréquentes dans la vie privée sont le fruit d'évolutions législatives qu'accompagne le leitmotiv « cela ne gêne pas ceux qui n'ont rien à cacher ». La plus importante ne concerne pas tant l'existence des *darknets*, qui peut être vue comme la preuve que tout groupe humain cherche à préserver ses secrets, mais surtout sur les outils permettant de préserver l'anonymat sur l'Internet. Et Tor semble en être le porte-drapeau.
Les controverses à son sujet n'ont jamais cessé, le fait qu'il soit le fruit d'un projet de la marine américaine lancé en 2002 n'en étant pas la moindre, toute paradoxale qu'elle soit. Andrew Lewman ajoute à ce paradoxe lorsqu'il déclare : *« Les membres du gouvernement américain qui nous subventionnent veulent que la vie privée et l'anonymat continuent d'exister. »* [Lew]

Selon une étude de Gareth Owen de l'université de Portsmouth exposée lors de la rencontre du Chaos Computer Club de 2014, 80 % des consultations via TOR seraient en lien avec la pédophilie [Wir2]. Ce résultat est controversé, car *« les forces de l'ordre et les groupes de défense des enfants qui patrouillent dans les darknets pédophiles pour mesurer leur influence et les suivre peuvent être comptés comme des visiteurs. »* [Wir2]. Sans compter les tentatives de dénis de service visant ces sites ni les consultations effectuées par des botnets.
Conscient de ces limites, l'auteur de l'étude précisait : *« Nous ne connaissons pas la raison de cette*

forte fréquentation (des sites pédopornographiques) et ne pouvons affirmer de manière certaines qu'elle n'est due qu'à des humains. » [Wir2]. Ces sites ne représenteraient cependant que 2 % des sites atteignables via TOR.
Cette controverse ne revient-elle pas à confondre le moyen et l'objet ? Car ceux qui cherchent des sites pédophiles le feront le plus souvent sous couvert d'anonymat. Se baser sur cette étude pour en déduire que TOR a partie liée avec le crime revient à lancer une campagne contre l'anonymat et le pseudonymat quelles qu'en soient les circonstances.
Aked, dans son étude déjà citée, liste le type de documents qu'il a pu trouver en utilisant divers logiciels pour entrer dans les *darknets* [Ake]. Sur le I2P BitTorrent, il n'a pas trouvé de documents pédopornographiques, alors que c'est le cas avec les réseaux I2P eDonkey et Gnutella, ainsi qu'avec Freenet Frost. Il reconnaît cependant lui-même les limites de son étude qui n'est pas exhaustive.

Utilité et avenir

Volatilité du darknet

Il semble qu'une bonne part de ce que l'on trouve dans un *darknet* soit volatile. Lorsqu'on parcourt les publications traitant du sujet, on y note que la durée de vie des sites indexés par Tor ne serait que de quelques jours à quelques semaines.
Cela n'est cependant pas étonnant, que l'activité protégée par le *darknet* soit légale ou pas. Une activité illégale doit sa longévité à sa discrétion et sa furtivité. Si la discrétion peut être procurée par les logiciels cités précédemment, sa furtivité résulte forcément d'une action humaine. Dans le monde réel, changer souvent de lieu de trafic est un moyen de prolonger sa durée de vie. Il est logique d'observer la même chose dans le cyberespace.
Quant aux activités légales, si leurs auteurs estiment nécessaire d'utiliser un *darknet*, c'est qu'ils craignent d'être écoutés ou pistés. Un changement fréquent de paramètres du *darknet* leur permet de déjouer la surveillance dont ils veulent se prémunir.

Les utilisateurs du darknet

Au fil du temps, les *darknets* sont passés du partage de fichiers confidentiels au partage de fichiers piratés (musique principalement, à la fin des années 90), puis à un partage de produits illégaux et enfin à la défense de la vie privée. Les réduire au seul moyen de protection d'activités illégales est réducteur. D'ailleurs, Biddle, England, Peinado et Willman reconnaissaient que Gnutella ne permettait pas que des choses illégales [Bid].

Étant donné les éléments contradictoires circulant sur les *darknets*, il est logique de se demander si ces réseaux sont vraiment utilisés ou s'ils ne sont qu'une légende urbaine cybernétique. Une étude [Kad] menée en 2014 et 2015 qui avait pour but de calculer la part du trafic réseau attribuée aux services cachés et de compter le nombre d'adresses uniques (en .onion) montre que *« 30 000 services cachés du réseau Tor représentent environ 3,4 % du trafic total du réseau, selon une étude du projet Tor. »*

Cependant, comme nous l'avons souligné précédemment, on ne trouve pas que des sites ou objets réputés illégaux dans les *darknets*. Ainsi, facebook a lancé en 2014 un service spécifique via Tor : https://facebookcorewwwi.onion/ [Fac].

Répression par les éditeurs de contenu

En 2002, Biddle, England, Peinado et Willman estimaient que la lutte contre les *darknets* était difficile : *« les réseaux tels que Gnutella sont difficiles à réguler car ils sont largement répartis et ils comportent des centaines de millions de nœuds. En y regardant de plus près, on y trouve de multiples vulnérabilités*[5] *»* [Bid]
La répression était néanmoins possible par l'absence de réel anonymat des utilisateurs : *« Toutes les attaques que nous avons identifiées exploitent le défaut d'anonymat du point final de la communication et sont aidées par les effets du 'free riding'. Des mesures légales se sont avérées efficaces sur toutes les technologies de pair à pair utilisées pour fournir un large accès à des contenus protégés par le droit d'auteur. Des serveurs centralisés ont été fermés. Napster a dû fermer. Gnutella et Kazaa sont menacés à cause des faiblesses des utilisateurs du 'free riding' et du manque d'anonymat du point final de la communication. Ce manque d'anonymat est la conséquence directe de l'utilisation d'une base de données totalement accessible, et c'est l'existence même de cette base de données qui distingue les darknets les plus récents des plus anciens. Il est difficile de savoir si le darknet pourra conserver cette base de données sur le long terme, mais il semble clair que les retards de la loi sur la technique pair à pair continueront d'être importants. »*
Les mêmes auteurs estimaient cependant que si Gnutella fermait, d'autres logiciels tels que Freenet ou Mnémosyne prendraient leur place.
Ils en déduisaient alors que la seule solution était de limiter les entrées de fichiers dans les *darknets* via le développement des DRM, du *watermarking* (insérer une marque invisible dans le contenu du fichier) et du *fingerprinting*. La différence entre ces deux procédés étant que le *fingerprinting* est un contrôle *a posteriori* tandis que le *watermarking* l'est *a priori*.
Dans ce même document, ils évoquaient également le futur des *darknets*. *« L'avenir légal des technologies utilisées pour les darknets est incertain, mais nous croyons que, au moins pour quelques utilisateurs, et vraisemblablement pour la population entière, des darknets efficaces continueront d'exister*[6]*. »*
« Il est évident que les darknets continueront d'exister et de fournir des services de haute qualité, à bas coût, pour de nombreux consommateurs. Ce qui signifie que sur de nombreux segments commerciaux, les darknets entreront en compétition avec le commerce légal[7] *»*
Ce dernier argument laisse penser que les *darknets* ne sont pas un phénomène en bout de course, mais que des moyens techniques continueront d'être développés pour assurer leur pérennité. Cette hypothèse est confirmée par la RAND qui estime qu'*« il y aura plus d'activité dans les darknets, plus de contrôles et de filtrage des participants, d'utilisation de cryptomonnaies, de plus grandes capacités d'anonymat des maliciels, et plus d'attention au cryptage et à la protection des communications et transactions. »* [Rand]

---

[5] §2.4.3
[6] §5
[7] §5.2

Répression légale

Puisque les *darknets* vont poursuivre leur développement, au prix de mutations techniques si nécessaire, il est logique que les forces de sécurité s'y invitent (dans la mesure du possible) pour contrôler les activités qui y sont menées.
Une récente étude de Thierry Berthier et d'Olivier Kempf [Ber] relative à la cybercriminalité dans son ensemble, montre que 10 % des cybercriminels sont responsables de 90 % des cybernuisances. Si on applique un taux similaire aux *darknets* (10 % de leurs utilisateurs seraient responsables de 90 % des atteintes), il est alors évident que les efforts des forces de l'ordre se concentreront contre certains *darknets*, dans la mesure où il est impossible de tous les fermer simultanément.

C'est ce qu'a fait le FBI lorsqu'il s'est attaqué à *Silkroad* en octobre 2013, puis à sa résurgence quelques temps après.
En novembre 2014 l'opération *Onymous* menée par le FBI et Europol a réussi à faire fermer plus de 400 sites qui vendaient drogues et armes, ce qui a plongé les développeurs de Tor dans la perplexité : l'anonymat procuré par Tor a-t-il été brisé ? Le porte-parole d'Europol est resté volontairement discret sur ce point afin de conserver la possibilité de réitérer ce type d'opération, tandis qu'Andrew Lewman minimisait la probabilité de corruption de Tor [Wir3].
À ce sujet, la présentation qu'Alexander Volynkin et Michael McCord, chercheurs à l'université Carnegie Mellon, devaient effectuer lors de la conférence Black Hat de 2014 fut précipitamment annulée (sans que la raison de cette annulation soit publiée) et l'équipe de Tor conseilla aux utilisateurs du logiciel de le patcher [Hil].
Ces résurgences de Silkroad, agrémentées ou non de mutation techniques, nous montrent un nouvel avatar de la lutte entre le bouclier et la cuirasse.

Dans ces occasions, les forces de l'ordre américaines ne sont pas avares de communiqués de victoire, comme ce fut le cas en avril 2015 à l'occasion du démantèlement d'un réseau de fausse monnaie [NYT1]. Pour attester de leur victoire, les policiers américains n'hésitent pas à revêtir le site internet désormais clos, du gonfanon de la victoire, maintenant bien codifié :

Illustration 6: Gonfanon de la victoire

Ce qui ne présage pas des suites judiciaires de l'affaire, même si Ross Ulbrecht, fondateur de silkroad, vient d'être condamné à perpétuité par un tribunal américain.

Au vu du paradoxe énoncé précédemment, cette lutte peut paraître étrange car la DARPA a décidé d'aider Tor à améliorer la qualité de ses services : *« Kate Krauss, directrice de la communication de Tor a déclaré au Daily Dot : La DARPA finance, à horizon d'un à trois ans, de multiples projets visant à améliorer les services cachés rendus par Tor.* » [Dd1]. Les liens entre la DARPA et Tor sont assez serrés, puisque Tor devrait être largement utilisé dans le projet Memex[8] : « *À terme, Memex devrait offrir des fonctionnalités de crawling du Dark Web intégrant les spécificités cryptographiques du système Tor. On peut raisonnablement imaginer que ces fonctions stratégiques faisaient bien partie du cahier des charges initial du projet Memex dont le budget est estimé entre 15 et 20 millions de dollars. »* [Ber2]

Notons aussi que la lutte contre les activités illégales n'est pas l'apanage des forces de l'ordre. Ainsi, le 17 octobre 2011, le collectif Anonymous a lancé l'opération Darknet contre une quarantaine de sites pédophiles en bloquant les comptes de 1589 utilisateurs. Il demandait notamment le retrait de toute pornographie infantile de ces sites. Comme ces opérations ne sont bien sûr pas coordonnées avec celles des forces de l'ordre, ces dernières ne les voient pas toujours d'un bon œil, car elles cherchent à recueillir des preuves de l'infraction afin de traduite les auteurs en justice, ce qui n'est pas le souci du collectif.

[8] Cf. http://www.darpa.mil/newsevents/releases/2014/02/09.aspx

 *Illustration 7: Opération Darknet*

Faut-il aller dans les darknets ?

Pourquoi aller dans les darknets ?

La question de la veille des *darknets* par les entreprises, voire des intrusions en leur sein, est de plus en plus souvent posée. L'argument justifiant leur veille est de savoir ce qui se dit sur l'entreprise (atteinte à la réputation), de déceler des signes avant-coureurs d'une attaque, de savoir si certaines de ses ressources sont utilisées dans un *botnet*, et enfin de connaître les moyens qui seront utilisés pour mener à bien une attaque informatique.
En clair, les seuls *darknets* concernés par cette veille sont donc ceux qui abritent des activités illégales. La précision s'impose avant de poursuivre.

Selon Adrien Petit, consultant en cybercriminalité, il est nécessaire de veiller plusieurs vecteurs de communication [GSM] :

- *Les réseaux sociaux : par exemple, les cybercriminels spécialisés dans le rançonnage du groupe Rex Mundi ont publié des documents de leurs récentes victimes (Domino's pizza et Labio) sur leur site .onion ;*
- *Les bases de données de pasties (pastebin.com, JustePaste.it…) : on y retrouve, entre autres, des instructions d'attaques DDoS, des exemplaires de cartes bancaires récoltées… ;*
- *D'autres outils sont également à observer : channels IRC, sites de diffusion, forums de conseils de piratage, et tout autre lien vers le Dark Web… En effet, les cybercriminels utilisent massivement ces différents canaux pour se faire de la publicité, mener à bien leurs revendications et recrutements ou encore faire du recel.*

Si l'intention peut sembler louable, l'inconvénient majeur réside dans le fait que ces actions sont effectuées *a posteriori* ou alors excèdent les moyens propres des entreprises (analyse des bases de données de *pasties*). Elles sont de ce fait peu recommandables, notamment pour des PME.

Toutefois, en admettant que veiller les *darknets* permette à l'entreprise d'être au courant de ce qui se trame à son encontre, cette veille soulève plusieurs questions :
- comment l'entreprise peut-elle se faire accepter dans un *darknet* ?
- est-elle sûre de la véracité des données échangées ?
- toute l'information illégale ne transite pas exclusivement par les *darknets*. Youtube est aussi une

plate-forme utilisée pour la publicité des criminels [CEIS].

Peut-on se fier à ce qu'on y trouve ?

Une fois admis dans un *darknet* hébergeant du contenu illicite ou illégal, peut-on prendre pour argent comptant les informations qu'on y trouvera ?
Avant de répondre à cette question, il convient d'étudier les modalités d'admission dans un *darknet*. Nul ne peut y être admis s'il n'a pas prouvé, d'une manière ou d'une autre, son appartenance à la communauté d'utilisateurs de ce réseau. Cela ressort de l'étude de la RAND : *« Dans les premiers temps, le filtrage des participants était rare ; il était assez facile de postuler et d'être admis dans un darknet. Aujourd'hui, le filtrage est plus strict et le ticket d'entrée plus difficile à obtenir, car les arrestations augmentent et les infiltrations par les forces de l'ordre ou les entreprises de sécurité sont plus nombreuses. »* [Rand]
Si le bon sens semble porter à la plus grande méfiance, on peut aussi prendre en compte les résultats d'une étude menée par des chercheurs du *Privacy Security and Automation Lab* de l'université Drexel (Pennsylvanie, USA). Ceux-ci se sont penché sur les forums de cybercriminels afin de savoir comment fonctionnaient les organisations criminelles sur l'Internet : « *Nous avons essayé de répondre à la question suivante : que signifie le crime organisé dans le cyberespace ?* » expliquait Vaibhav Gard, membre de l'équipe.
Un de leurs constats est (on s'en serait douté) que la question de la confiance doit être évacuée, Rebekah Overdof déclarant « *Le plus grand défi d'une organisation cybercriminelle est l'absence de confiance entre semblables* » [Ddig]. D'ailleurs « *un nouvel arrivant n'est pas forcément libre de pouvoir tout réaliser : il lui faut d'abord prouver sa valeur et que la confiance soit bien établie, ce qui lui permet de grimper dans la hiérarchie.* » [Ddig]
Malgré toutes ces précautions, les participants à ces activités illégales ne sont pas à l'abri de déceptions. Ainsi, en 2015, la place de marché Evolution a disparu après s'être fait voler 42000 bitcoins. Il semblerait que les auteurs de ce vol soient les administrateurs de cette place de marché, connus sous les pseudonymes de Verto et Kimble [Dd3].
Les chercheurs de l'université Drexel se sont aussi rendu compte que les organisations fonctionnaient de deux façons différentes, en gang (avec un chef unique clairement identifié) ou en cartel (avec plusieurs cadres dirigeants). Dans le premier cas, toute opportunité de profit est bonne à prendre, alors que les cartels sont une interconnexion de communautés et cherchent à rentabiliser leurs filières d'action.
Nous nous rendons alors compte que, quand bien même une entreprise aurait été acceptée au sein d'un ou plusieurs *darknets*, il lui serait difficile de savoir si l'information recueillie est fiable, mais il faudrait également qu'elle sache comment fonctionne l'organisation criminelle qui l'anime afin de prédire ses cibles. Le temps risque donc de lui manquer pour prévoir la façon dont elle sera frappée.
Enfin, cette étude est à relativiser car les données qui lui ont servi de base proviennent d'un piratage. Elles sont donc partielles et ne peuvent refléter l'intégralité des réseaux criminels et de leur fonctionnement sur l'Internet. En tirer des lignes de conduite obligatoires serait imprudent.

La question de la pertinence de la veille des *darknets* se pose d'autant plus que l'abondance de documents de tout genre publiés sur l'Internet permet de saturer rapidement les capacités de recherche humaine. De plus, le camouflage de termes peut ajouter à la complexité de la recherche : chercher sans savoir à quoi ressemble l'objet cherché revient à tenter de découvrir une aiguille dans

une botte de foin.
Il faut cependant garder à l'esprit qu'il n'est pas toujours nécessaire de fréquenter les darknets pour récupérer des acquis frauduleux. L'exemple de Payivy est là pour nous le rappeler, puisqu'il y a peu de temps, des internautes se sont rendus compte qu'il était possible d'y acheter des numéros de comptes PayPal piratés, tout en payant par… Paypal ! *« PayIvy est devenu un circuit majeur pour écouler vers un grand nombre de services internet des comptes et identifiants volés. »* [Kre]

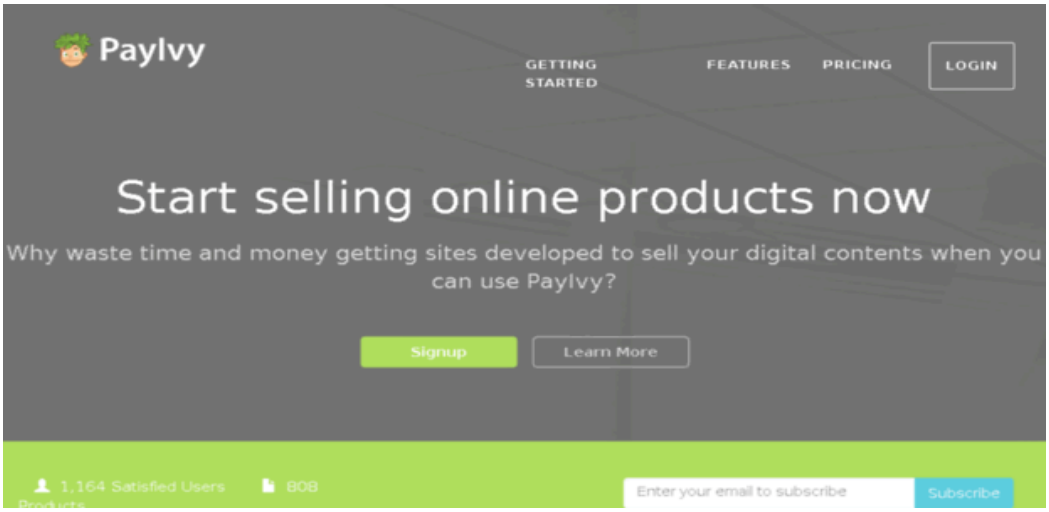

Illustration 8: Site commercial Payivy

Conclusion

Le *darknet* est donc un réseau privé neutre, dans le sens où il n'est pas substantiellement malfaisant. Cette neutralité ne doit cependant pas inciter à la naïveté. La confiance n'y règne pas *a priori*. Il est alors conseillé de ne s'y aventurer qu'en toute connaissance de cause, sans garantie de la véracité des informations trouvées. Les *darknets* peuvent être assimilés, dans leur partie illégale, à un territoire tenu par une bande ou une organisation criminelle : n'y entrent que les invités et seulement parce qu'on en attend quelque chose.
La simple prudence conseille alors de ne pas s'y aventurer, même au nom de l'entreprise : elle n'est pas sûre que sa quête soit couronnée d'un résultat certain, et les risques de compromission du matériel utilisé sont avérés.
À terme, il sera intéressant de voir comment la doctrine juridique considérera les *darknets*. Au vu des débats actuels, notamment sur le vol de données numériques et l'identité numérique, il n'est pas impossible que prochainement se pose la question de savoir si un *darknet* ne doit pas être considéré comme un domicile privé, au même titre qu'une chambre d'hôtel.

Références

[Ake] Aked Symon : An Investigation into Darknets and the Content available via anonymous peer-to-peer file sharing, School of Computer and Security Science , Edith Cowan University, Perth Western Australia. 2011
[Ber] Berthier Thierry et Kempf Olivier : De la cyberveille à la prévision des agressions. Actes du C&ESAR 2014.
[Ber2] http://www.huffingtonpost.fr/thierry-berthier/enjeux-et-defis-deep-web_b_7219384.html?utm_hp_ref=france
[Bid] Peter Biddle, Paul England, Marcus Peinado et Bryan Willman : The Darknet and the Future of Content Distribution. 2002
[CEIS] CEIS : Cybercriminalité et réseaux sociaux : liaisons dangereuses. Janvier 2015.
[Ddig] http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626
[Dd1] http://www.dailydot.com/politics/next-generation-tor-darpa/
[Dd2] http://www.dailydot.com/politics/facebook-tor-explained/
[Dd3] http://www.dailydot.com/crime/evolution-dark-net-black-market-bitcoin-scam/
[Fac] https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237
[GSM] Global Security Mag : http://www.globalsecuritymag.fr/Dark-Web-visite-guidee-de-la-face,20150420,52388.html
[Hil] Kashmir Hill, How Did The FBI Break Tor? http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/
[Kad] George Kadianakis and Karsten Loesing : Extrapolating network totals from hidden-service statistics. Janvier 2015
[Kre] PayIvy Sells Your Online Accounts Via PayPal, disponible sur le site http://krebsonsecurity.com/2015/05/payivy-sells-your-online-accounts-via-paypal/
[Lew] Andrew Lewman : interview sur le site http://www.bbc.com/news/technology-28886465 Août 2014
[Moz] https://blog.mozilla.org/privacy/2014/11/10/introducing-polaris-privacy-initiative-to-accelerate-user-focused-privacy-online/
[NYT1] http://www.nytimes.com/aponline/2015/04/02/us/ap-us-counterfeiting-uganda.html?_r=0
[Rand] RAND : Markets for Cybercrime Tools and Stolen Data, 2014.
[Red] http://www.reddit.com/r/DarkNetMarkets/comments/22jg6b/darknet_markets_search_engine/
[Wir1] http://www.wired.com/2014/04/grams-search-engine-dark-web/
[Wir2] http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/
[Wir3] http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/