**Netcom**
Réseaux, communication et territoires

**32-1/2 | 2018**
**Expéditions géographiques en Terres Numériques, fronts pionniers et nouvelles limites - Hommage à Henry Bakis**

# Un « Deep / dark web » ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor

*A "deep/dark web"? About the metaphors of depth and shadow related to Tor*

**Jean-François Perrat**

**Édition électronique**
URL : http://journals.openedition.org/netcom/3134
DOI : 10.4000/netcom.3134
ISSN : 2431-210X

**Éditeur**
Netcom Association

**Édition imprimée**
Date de publication : 16 décembre 2018
Pagination : 61-86
ISSN : 0987-6014



**Référence électronique**
Jean-François Perrat, « Un « Deep / dark web » ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *Netcom* [En ligne], 32-1/2 | 2018, mis en ligne le 17 octobre 2018, consulté le 08 avril 2019. URL : http://journals.openedition.org/netcom/3134 ; DOI : 10.4000/netcom.3134

*Networks and Communication Studies,*
*NETCOM*, vol. 32 (2018), n° 1-2
pp. 61-86

# UN « DEEP/DARK WEB » ? LES METAPHORES DE LA PROFONDEUR ET DE L'OMBRE SUR LE RESEAU TOR

## *A "DEEP/DARK WEB"? ABOUT THE METAPHORS OF DEPTH AND SHADOW RELATED TO TOR*

**PERRAT JEAN-FRANÇOIS**[1]

***Résumé -*** The onion router *(Tor) est un réseau superposé (*overlay network*) à Internet, publiquement accessible depuis 2003, et qui permet à ses utilisateurs (clients) de naviguer sur le* World Wide Web *(WWW) sans révéler leur identité grâce à un protocole dédié et au chiffrement des échanges. Depuis 2004, il est possible de créer des* location-hidden services *exclusivement accessibles* via *Tor afin de dissimuler également l'identité des hébergeurs de contenu (serveurs). Cet article propose une analyse de la documentation technique, des représentations communes, et de données de terrain issus des* location-hidden services *pour évaluer la pertinence des expressions métaphoriques «* deep web *» et «* dark web *» souvent employés pour désigner ces espaces internétiques particuliers. Il propose d'éviter leur emploi dans les terminologies expertes, au profit de « web .onion ».*

***Mots-clés -*** *The Onion Router ; Tor ;* deep web ; dark web ; *web ; .onion ; terminologie.*

***Abstract -*** *Tor (*The Onion Router*) is a subnetwork of the Internet which makes it possible for mere users and contents providers to conceal their identity on special websites called location-hidden services. Based on the analysis of the technical documentation, the common representations and field-material from the location-hidden services, this article evaluates the relevance of the «* deep web *» and «* dark web *» metaphors often used to talk about the location-hidden services of Tor. It suggests to rather use the term « .onion web ».*

***Keywords -*** *The Onion Router ; Tor ;* deep web ; dark web ; *web ; .onion ; terminology.*

[1] Doctorant à l'École normale supérieure de Lyon, UMR 5600 « Environnement, ville, société ». Courriel : jeanfrancois.perratmabilon@ens-lyon.fr

## INTRODUCTION

*The onion router* (Tor[2]) est à la fois un réseau de serveurs et un protocole de communication sur Internet permettant de ne pas dévoiler son adresse *Internet Protocol* (IP) personnelle aux hôtes consultés. Il permet également la consultation de *location-hidden services* ou, par ellipse, *hidden services*[3], dont l'adresse IP est elle-même cachée aux internautes qui les consultent.

Tor est souvent décrit comme faisant partie du « *deep web* » ou du « *dark web* » (Solomon, 2015). Nous verrons que ces appellations sont d'un usage courant, que ce soit dans la presse, les conversations courantes ou même les publications scientifiques. Le terme « *deep web* » renvoie à l'idée que Tor et ses *hidden services* seraient comme séparés du reste des lieux du *World Wide Web* (WWW), qu'il y aurait une forme de discontinuité entre ces deux espaces. « *Dark web* » renvoie pour sa part à l'idée que des pratiques illégales (vente de drogue et pédocriminalité notamment) y seraient particulièrement courantes. Ces deux appellations s'appuient sur des métaphores spatiales renvoyant à l'idée de profondeur ou d'ombre pour décrire Tor. Bien que ces métaphores me semblent en partie révélatrices sur la nature de ce réseau et des lieux internétiques constitué par les *hidden services*, elles éloignent également le locuteur de leur réalité technique. Or, pour reprendre Bernard Debarbieux, « [la] production de représentations et des systèmes d'objets dont elles sont faites, a des finalités pratiques ; elle guide l'action et est, dans le même temps, motivée par elle. Elles font que chacun de ces objets, une fois désigné et circonscrit, une fois rapporté à une catégorie particulière, constitue un "horizon d'attente" (Ricoeur, 1985) qui oriente les pratiques des usagers de l'objet en question » (Debarbieux, 2004, p. 25). Il importe donc de questionner ces métaphores pour s'assurer de penser au mieux les objets qu'elles désignent et les spatialités qui y ont lieu. Quel « horizon d'attente » ces métaphores contribuent-elles à engendrer ? Peut-on envisager d'autres choix terminologiques plus adéquats à la réalité technique et empirique de Tor et de ses *hidden services* ?

Cet article vise donc à interroger cette production de représentations en regard de ce qui est fait de et dans Tor, en reprenant le triptyque de l'espace conçu-perçu-vécu d'Henri Lefebvre (Lefebvre, 1974). Il s'agira d'évaluer à quel point les termes de « *deep* » ou de « *dark web* » peuvent prétendre devenir des « catégorie[s] analytique[s] ou [des] concept[s] » s'appuyant utilement sur une « ressource métaphorique » (Debarbieux,

[2] Les développeurs du projet Tor recommandent l'utilisation de l'acronyme « Tor » et non « TOR », à l'encontre des conventions typographiques habituelles. Cette recommandation, passée dans l'usage, sera suivie dans cet article.

[3] Cette ellipse peut mener à des effets de sens indésirés : comme on le verra, les services en question ne sont pas du tout « *hidden* » ou « cachés » par définition, seule leur adresse IP (*Internet Protocol*) l'est. L'usage est toutefois si répandu, y compris chez les développeurs de Tor, que je le reprends ici. Il est toutefois exclu de traduire par « service caché », ce qui mènerait à un contresens.

2014, paragr. 31), ou s'il faut se concentrer sur « l'explicitation et (...) l'exploitation de leur caractère poétique » (*idem*).

Pour ce faire, nous ferons d'abord une présentation et une histoire succincte de Tor, visant à décrire la manière dont son espace est conçu d'un point de vue technique. Nous nous interrogerons ensuite sur les représentations les plus courantes du « *deep* » et du « *dark web* », qu'elles soient discursives ou iconographiques. Ces représentations seront mises en regard de la manière dont Tor et ses lieux sont empiriquement vécus par leurs utilisateurs.

## 1. LA CONSTRUCTION DE TOR ET DE SES *HIDDEN SERVICES*

### 1.1. Tor : un outil pour naviguer sur le WWW

Tor est à la fois un réseau de routeurs et un protocole de chiffrement, permettant une anonymisation forte des échanges en ligne. Il est fondé sur le principe du « routage en oignon » (Syverson *et al.*, 1997) qui multiplie les intermédiaires entre le client d'où est émis une requête internétique et le serveur auquel cette requête s'adresse, tout en chiffrant l'ensemble de la chaîne de transmission. Développé au sein des services de renseignement militaires états-uniens depuis le milieu des années 1990 (d'abord par l'Office of Naval Research, puis très vite la Defense Advanced Research Projects Agency également)[4] et disponible en source ouverte depuis 2003 (Syverson, 2005), sa fonction première est de permettre la consultation du WWW sans compromettre l'identité du client. Le *Transmission Control Protocol* (TCP), à savoir le protocole standard régulant le transfert des données entre un client et un serveur sur Internet, requiert de connaître les adresses *Internet Protocol* (IP) du client comme du serveur pour établir la transmission entre eux. Le protocole de Tor permet d'établir la transmission entre un client utilisant Tor et un serveur classique sans que l'adresse IP du client soit divulguée au serveur : le client Tor transmet sa requête à un premier *proxy* Tor (le point d'entrée[5]), qui la transmet à un deuxième *proxy* ne connaissant lui-même que l'adresse du nœud précédent, et qui le transmet ensuite à un troisième et dernier *proxy* qui assumera la connexion avec le serveur (on parle de nœud de sortie). Ainsi, le serveur ne connaît que l'adresse IP du nœud de sortie, et les *proxys* Tor eux-mêmes ne connaissent que l'adresse du maillon qui les précède et de celui qui les suit immédiatement dans la chaîne de transmission (voir Figure 1). C'est la raison pour laquelle ce type de routage est dit « en oignon » : il rajoute toute une série de « couches » successives dans la transmission de l'information, qui font obstacle aux attaques visant à connaître le contenu d'un échange *via* Tor ou l'identité du client, notamment les attaques dites de l'homme du milieu.

[4] Les techniques de chiffrement numérique étaient alors soumises à un très fort contrôle par les pouvoirs publics, étant considérées comme des « armes et munitions soumises à contrôle », de nature militaire. Ce régime est assoupli par l'*executive order* n° 13026 du 15 novembre 1996, signé par le président Clinton, puis les outils de chiffrement sont retirés de la liste en 2000 à l'initiative d'Al Gore (Tréguer, 2017, p. 308).

[5] Plus précisément, Tor crée d'abord un serveur *proxy* virtuel en local sur la machine cliente.

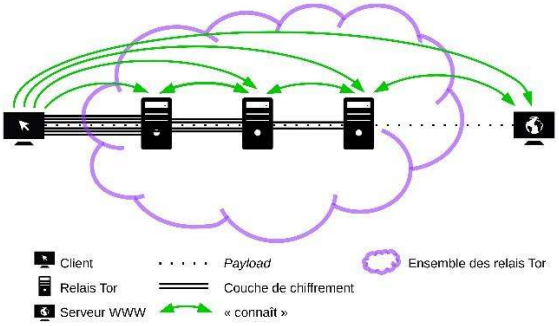


***Figure 1** : La pseudonymisation de l'adresse IP dans les échanges* via *Tor.*
Réalisation Jean-François Perrat. Icônes par Freepik pour www.flaticon.com

### 1.2. Les *hidden services* de Tor

Bien que le réseau Tor soit donc largement connecté au WWW[6] et que ce dernier soit presque entièrement accessible *via* Tor, l'inverse n'est pas vrai. Depuis 2003, il est possible non plus seulement pour les clients Tor, mais aussi pour les serveurs adéquatement configurés, de cacher leur adresse IP – qui reste inconnue aux clients leur adressant des requêtes à travers le réseau Tor. Cette fonctionnalité a permis la création de services appelés *location-hidden services*, plus couramment, *hidden services* (Dingledine *et al.*, 2004), et parfois *Onion services* dans la documentation du projet Tor[7]. Ces services sont accessibles uniquement *via* le réseau Tor. Bien que spécifiques à Tor, ils ont eux aussi une URL (*Uniform Resource Locator*). Leur nom de domaine de premier niveau (TLD) est .onion (et non .com, .fr, ou autres domaines plus répandus). Tor a en effet son propre système chiffré de résolution de nom de domaine (DNS), à savoir l'opération qui consiste à fournir l'adresse IP d'un serveur à un client pour lui permettre d'initier la connexion. Dans le protocole de Tor, la connexion client-serveur se fait sans que le client ni le serveur ne connaissent leurs adresses IP respectives. Les annuaires DNS classiques, quant à eux, ne recensent pas les adresses .onion. Le TLD .onion est néanmoins reconnu officiellement par les instances de régulation technique d'Internet (ICANN, IANA et IETF) depuis le 9 septembre 2015 et l'entrée en vigueur du *request for comments* (RFC) 7686. Le domaine .onion appartient désormais à la liste des « domaines spéciaux », eux-mêmes encadrés par le RFC 6761.

En rendant presque impossible de retrouver l'IP et donc l'identité légale des personnes y interagissant, le protocole de Tor a fait émerger les *hidden services* comme des lieux de pseudonymat quasi inviolable. Ils constituent une forme paroxystique de ce

[6] Cette interconnexion n'est pas complète. Certains sites web et certains pays, comme la Chine, l'Iran ou la Turquie, entravent la navigation des internautes passant par Tor.
[7] Voir « Tor: Onion Service Protocol » à l'adresse https://www.torproject.org/docs/onion-services [en ligne], consulté le 14/08/2018.

qui est couramment appelé le « *deep web* »[8], quand ils ne sont pas appelés « *dark web* » pour insister sur l'illégalité des pratiques qui y ont ou qui sont censées y avoir lieu (Moore & Rid, 2016). Il est à noter que cette terminologie n'est pas employée dans la documentation officielle du Tor Project. D'autres sous-réseaux dont les finalités pratiques sont comparables à celle de Tor existent, comme Freenet, Invisible Internet Project (I2P), ou encore GNUNet, mais Tor est à la fois le plus étendu et le plus connu.

Le site metrics.torproject.org, officiellement rattaché au projet Tor, fournit des statistiques d'utilisation du réseau. De 2014 à nos jours, le nombre d'utilisateurs uniques quotidiens de Tor est estimé à environ 2 000 000. Parmi eux, la majeure partie semble utiliser Tor pour se connecter au WWW : le débit total moyen sur le réseau Tor à l'été 2018 est légèrement supérieur à 100 Gbits/s, contre un peu plus de 1 Gbits/s pour le débit total moyen vers ou depuis les services .onion. Il semble donc raisonnable de dire que la connexion au WWW est le principal usage de Tor.

### 1.3. La disjonction entre le WWW et le web .onion

En première approximation, le réseau Tor n'est donc qu'une partie du réseau Internet. Il s'agit d'un réseau superposé dont les serveurs sont des serveurs internétiques, et dont les échanges de données se font à travers la même infrastructure matérielle. Mais si l'on suit la réflexion plus générale initiée par Alexander Galloway à propos d'Internet, c'est finalement en mettant la question du « protocole » (Galloway, 2004) de Tor au centre de la réflexion qu'on comprend en quoi il institue une forme de discontinuité entre Internet et les *hidden services*, ainsi qu'entre le WWW et le web des sites .onion. Il est en effet impossible d'accéder au web .onion sans configurer son navigateur pour router ses données vers un *proxy* Tor local, ou en utilisant simplement le *Tor Browser* déjà configuré à cette fin. Les différences de protocole de communication utilisés au niveau de la couche transport créent donc la discontinuité entre ces deux types d'espaces. Cela explique en partie pourquoi les appellations de « *deep* » ou de « *dark web* », par opposition à ce qui est souvent appelé « *surface web* » ou « *clear web* », sont si communes. C'est plus particulièrement l'absence de recours au protocole DNS qui distingue les *location-hidden services* du reste d'Internet en termes d'accessibilité, en protégeant au passage leur adresse IP et incidemment l'identité légale de leur hébergeur.

Pour autant, il ne faut pas exagérer cette différence dans la conception de ces deux espaces. En effet, les protocoles et langages de plus haut niveau employés sur Tor et les *hidden services* ainsi que sur Internet et les sites du WWW sont les mêmes, en particulier HTTP (*HyperText Transfer Protocol*) et HTML (*HyperText Markup Language*). Ainsi, le *Tor Browser* n'est lui même qu'une variante légèrement modifiée d'une version

[8] Le terme de « *deep web* » a une définition assez large. L'usage courant le décrit comme l'ensemble des sites et ressources internétiques qui ne sont pas indexés par les moteurs de recherche comme Google ou Bing. Ils sont accessibles par Internet, mais plus difficilement – quand ils ne requièrent pas l'utilisation de programmes spécifiques, comme le navigateur *Tor Browser*, pour accéder aux *hidden services*. Il est difficile de clairement tracer la ligne entre « *deep web* » et « *clear web* » dans ces acceptions.

dite ESR (*Extended Support Release*) du navigateur *Mozilla Firefox*. N'importe quel navigateur permet de se rendre sur le web .onion, pour peu qu'il soit configuré pour utiliser le client Tor indépendamment installable. Les bases pratiques de la navigation sur le WWW ou le web .onion du point de vue de l'utilisateur sont donc les mêmes, avec des pages web classiques, des adresses web (quoiqu'elles finissent en .onion), des liens hypertextes, etc.

### 1.4. *Les hidden services*, des « lieux » d'Internet ?

Cette approche technique n'explicite cependant pas quelle est la géographicité de Tor : dans quelle mesure un réseau informatique et des protocoles dédiés, qu'il s'agisse d'Internet en général ou de Tor en particulier, peuvent-ils faire émerger de l'espace ? En quoi les pratiques en ligne sur Tor relèvent-elles d'une géographie du numérique ?

La prise en compte des TIC comme une thématique légitime dans le champ de la géographie française commence dans les années 1970 et s'affermit dans les années 1980, notamment sous l'impulsion d'Henry Bakis (Bakis, 1980). S'il s'est d'abord agi d'aborder la question sous l'angle de la géographie industrielle, en étudiant par exemple l'inscription spatiale d'une firme comme IBM (Bakis, 1977), il a rapidement été question d'interroger plus fondamentalement quels pouvaient être les effets des TIC sur l'espace géographique et les pratiques spatiales, dans la mouvance de travaux comme ceux de Thorngren, sur le développement régional en Suède (Thorngren, 1970 ; 1977), ou de Abler sur le téléphone et le système métropolitain aux États-Unis (Abler, 1977). En matière de mobilités, la thématique de la substitution (ou non) des déplacements par la télécommunication, très active depuis les années 1960, est dépassée dans les années 1980 par la question du rapport entre les télécommunications et la forme même des villes (Schwanen, 2017), ou encore par la question de la structuration de l'espace industriel par les réseaux de télécommunication et non plus seulement la localisation des matières premières ou des réseaux de transport (Bakis, 1985).

Ces réflexions sont prolongées et amplifiées dans les années 1990 avec l'émergence du réseau mondial Internet et du World Wide Web. Une tendance à penser que les TIC pourraient s'exonérer de l'espace matériel et des territoires au profit des télécommunications, à la fois quasi instantanées et peu coûteuses en énergie, est alors montée en puissance (Bakis & Vidal, 2007). Les possibilités concrètes offertes par le télétravail ou le commerce en ligne, ainsi que le succès des thématiques du « village global » (McLuhan & Fiore, 1967) ou du « cyberespace » (Gibson, 1994), y ont largement contribué. L'urbaniste et architecte William J. Mitchell va par exemple jusqu'à avancer que « le Net nie la géométrie » (Mitchell, 1999, p. 8). Nous serions alors entrés à l'ère d'un « espace de flux » (Castells, 1996). Cette remise en cause de l'utilité de la coprésence physique aurait même dû pour certains précipiter la fin des villes. La « fin de la géographie » annoncée n'a évidemment pas eu lieu : la prégnance des facteurs de localisation, des économies d'échelle et des effets d'agrégation n'a pas été abolie par Internet en ce qui concerne les biens matériels (Lasserre, 2000). Plus encore, Internet a même renforcé le besoin d'une approche territoriale du numérique et des TIC dans la

mesure où la présence d'infrastructures de télécommunication et des capacités locales à en tirer parti contribuent à accentuer concurrences et hiérarchies territoriales (Bakis & Vidal, 2007). Contre le mythe de l'aspatialité d'Internet, les aménageurs ont eux-mêmes théorisé le problème de la « fracture numérique » entre les territoires (Dupuy, 2007). Cette « impasse » théorique de la fin de la géographie serait née d'une trop grande « préoccupation pour les usages » d'Internet, faisant fi de sa « matérialité » (Duféal & Grasland, 2003, paragr. 1).

Entre la fin des années 1990 et les années 2000, un consensus largement partagé s'est établi autour de l'idée qu'il fallait aborder Internet dans une approche territoriale, spatialisée, en rupture avec les apories sus-citées comme avec les approches trop sectorielles des économistes (Duféal, 2004, chap. 1 et 2). Internet ne devait pas être conçu comme abolissant l'espace, mais comme « [augmentant] » les capacités d'interaction des territoires, de leurs habitants et de leurs institutions (Musso, 2008, p. 33) dans des approches interrogeant l'interspatialité entre espace en ligne et espace territorial. Selon un terme forgé par Henry Bakis, l'espace géographique du XXIe siècle serait un « géocyberespace » hybridant le géoespace traditionnel au « cyberespace » informationnel (Bakis, 2007[9]; Bakis & Vidal, 2007) en un complexe où les délimitations seraient de plus en plus floues. Dans sa thèse, Marina Duféal a ainsi retrouvé la même structure dans les liens entre sites institutionnels des communes de l'arc méditerranéen que dans leur système urbain géospatial (Duféal, 2004). Elle suggère aussi qu'un phénomène territorial comme l'insularité corse se retrouve dans son « inscription spatiale » en ligne (Duféal, 2005). Thierry Joliveau développe quant à lui l'idée de « géoweb » pour décrire les services cartographiques en ligne tels que Google Maps (Joliveau, 2011), et plus largement de « géonumérisation » pour décrire le « processus de transcription au moyen d'outils informatiques des objets, êtres, phénomènes, activités, images, textes ... localisés sur la surface terrestre » (Joliveau, 2007), terme également repris par Henri Desbois (2015).

Prenant acte de l'aporie de l'aspatialité d'Internet, d'autres approches géographiques interrogeant davantage les spatialités en ligne pour elles-mêmes n'en émergent pas moins dans les années 2000 et 2010. D'une part, autour de Frédérick Douzet et de la chaire Castex (Paris VIII-IHEDN), créée en 2011, qui cherchent à préciser la notion de « cyber » d'un point de vue géopolitique, et qui abordent le « cyberespace » comme un « théâtre d'opérations » ou un « domaine » à part entière, y compris dans sa dimension informationnelle (Desforges, 2018; Douzet *et al.*, 2014). La matérialité du réseau et les acteurs territoriaux, en particulier les États, restent bien sûr prépondérants aussi dans cette approche. D'autre part, Boris Beaude propose d'envisager plus radicalement les spatialités propres d'Internet. En s'appuyant sur la théorie de l'espace notamment développée par Jacques Lévy (1994), il avance

[9] Le concept date de 1997 : Bakis, H., (1997), From Geospace to Geocyberspace; Territories and Teleinteraction, pp. 15-49, in Roche E. M. & Bakis H. (eds., 1997), *Developments in telecommunications. Between global and local*, Avebury. (NDLR).

qu'Internet est un espace « réticulaire », immatériel et de métrique topologique (Beaude, 2013). Dans cette conception relationnelle de l'espace, la référence au territoire / géoespace n'est plus essentielle : l'espace n'est pas réductible à l'étendue terrestre, il est « [une] des dimensions de la société, correspondant à l'ensemble des relations que la distance établit entre différentes réalités » (Lévy & Lussault, 2013). Malgré son immatérialité, « Internet est [donc] un espace réel et actuel » (Beaude, 2012, p. 43). Pour reprendre le triptyque d'Henry Bakis, il s'agit peu ou prou de considérer le « cyberespace » également pour lui-même, sans s'obliger à en envisager systématiquement l'interspatialité avec le géoespace à travers la notion de géocyberespace[10]. Boris Beaude propose ainsi de considérer Internet comme un ensemble de « lieux » au sens plein, non métaphorique, à savoir un ensemble d'« [espaces] dans [lesquelles] la distance n'est pas pertinente » (Lévy, 2003). Dans ces « lieux réticulaires (...), la non-pertinence de la distance est fondée sur la communication » (Beaude, 2012, p. 51). Mais ce qui fait d'Internet un espace, à la différence de « moyens de transmission antérieurs » (téléphone, radio, télévision…), c'est la « permanence » de ses lieux (idem, p. 54-55). Cette propriété permet non plus seulement la synchronisation d'acteurs distants, comme pouvait déjà le faire le téléphone, mais leur « synchorisation » (Beaude, 2012, chap. 2), c'est-à-dire le partage non d'un temps (formé sur *khrónos*) mais d'un espace commun (formé sur *chôra*). L'intérêt de cette propriété avait déjà été identifié par le philosophe de la technique Andrew Feenberg dans les années 1990 pour le travail collaboratif sur des documents partagés, ou pour les réunions de malades en ligne (Feenberg, 2004; Feenberg *et al.*, 1996). La conceptualisation de la synchorisation à propos des lieux dits réticulaires est l'apport majeur de Boris Beaude en géographie du numérique – et ce qui fait la différence entre Internet comme espace et, par exemple, le réseau téléphonique comme simple technologie spatiale. Le concept de synchorisation ne s'applique bien sûr pas spécifiquement aux lieux internétiques : tout lieu est un espace de synchorisation. Mais les propriétés d'Internet, notamment la vitesse de transmission et son accessibilité grandissante (canaux multiples, couverture croissante…), en font « l'un des plus puissants espaces qui organisent le monde contemporain » (Beaude, 2012, p. 66-67).

Boris Beaude appelle ainsi à faire une lecture spatiale de ce qu'il appelle les lieux réticulaires, ou lieux d'Internet. Dans un texte de 2015, il présente par exemple Wikipedia autant comme un site web que comme le lieu réticulaire qui rend possible la production même de cette encyclopédie participative (Beaude, 2015). L'anthropologue Sandra Houot questionne pour sa part les nouvelles relations permises au sein de communautés musulmanes diasporiques à travers leurs spatialités numériques (Houot, 2016). Le géographe Jean-Christophe Plantin estime quant à lui que le concept de synchorisation est utile pour dépasser l'utilisation de graphes dans « [l'analyse] des pratiques de communication en ligne » (Plantin, 2014, paragr. 26). Et c'est dans cette approche émergente que le présent article s'inscrit à son tour.

[10] Dans la même mesure où il est possible d'avoir une approche géographique de réalités matérielles sans nécessairement mettre au premier plan leur inscription en ligne.

En somme, on peut donc dire que le web .onion est un espace internétique au sens plein, et que les *hidden services* sont autant de lieux d'Internet, malgré le fait que Tor s'appuie sur certains protocoles spécifiques dans la couche transport. En particulier, il n'y a pas de spécificité de Tor en ce qui concerne le navigateur, et donc pas de spécificité des pratiques usuelles de navigation des internautes passant par Tor. En tant qu'espaces d'interaction en ligne, le WWW et le web .onion différent donc moins par le répertoire des spatialités qui peuvent s'y déployer que par les ressources et les compétences spatiales requises pour y circuler.

## 2. UN ESPACE REPRESENTE COMME RADICALEMENT AUTRE

Bien que Tor soit fondamentalement un réseau de serveurs superposé à Internet, et que les *hidden services* soient des hôtes utilisant des protocoles de haut niveau banals, ils sont souvent représentés comme participant d'un espace autre, singulier, en rupture avec le reste d'Internet et du WWW : le « *deep/dark web* ». Cette tendance ne s'applique bien sûr pas à tous les discours sur Tor, mais elle s'observe en revanche dans tous les types de discours - notamment journalistiques, politiques, artistiques ou même scientifiques, ainsi que dans les discours ordinaires, plus ou moins experts sur la question. Un « imaginaire social » (Debarbieux, 2015, chap. Introduction) de Tor est à la fois instituant de et institué par ces discours, dans un processus de co-construction dynamique. Nous allons voir que les thématiques de l'ombre et de la profondeur sont structurantes dans cet imaginaire.

### 2.1. Le « *deep/dark web* », un espace de non-droit ?

#### *2.1.1. Dans le discours de la presse écrite*

On peut tenter d'objectiver ce sentiment que Tor, le « *deep web* » et leurs avatars sont caricaturés comme des zones de non-droit, à la fois sulfureuses et subversives, en analysant un corpus large d'articles de presse, comme le font de plus en plus de géographes sur des sujets variés (Comby *et al.*, 2011). À cette fin, j'utiliserai la base de données d'articles de presse du service Factiva[11]. La requête, faite le 13 août 2018, a porté sur l'ensemble du contenu des articles recensés dans la base (titres et corps de texte). Pour cibler au mieux le sujet et obtenir une sélection d'articles évoquant Tor à coup sûr, la formule en était « "*onion router*" *or* "*routeur en oignon*" », en conservant les guillemets. Les deux expressions étant sans équivoque dans les deux langues, le résultat ne contenait pas de bruit, et n'a pas nécessité d'affiner davantage la requête. L'ajout de termes comme « *dark net* », par exemple, ne fait que limiter le corpus et biaiser le résultat. Le corpus résultant contient 1 125 références, dont 985 en anglais et 139 en français

[11] Factiva est une base de données destinée aux chercheurs, et aux professionnels de l'analyse de réputation des entreprises et des marques. Le service est proposé par Reuters et Dow Jones & Company. Elle permet de manipuler d'importants corpus, notamment des articles de presse, et donne accès aux bases de la plupart des grands journaux. Factiva est l'un des meilleurs services de ce type, et se targue de donner accès à plus de 32 000 sources dans 28 langues différentes.

(dont 2 résultant de la requête « routeur en oignon » seule). Seuls le français et l'anglais ont été retenus dans la mesure où je n'aurais pas été capable de déterminer la part de résultats non pertinents dans d'autres langues. Par ailleurs, le corpus est déjà significatif à 1 125 références, contre un peu moins du double (2 124) toutes langues incluses. En termes de distribution temporelle, on observe une rupture très nette en 2013, qui correspond au moment des révélations d'Edward Snowden, et à la fermeture très médiatisée d'un *hidden service* de vente de drogue, *Silk Road*, par la police fédérale (FBI) des États-Unis : 996 articles, soit 87 % de la base, ont été publiés depuis 2013, dont 223 (20 %) pour cette seule année.

Intéressons-nous désormais au traitement qui est fait de Tor dans les articles retenus. Factiva affecte 1 092 articles d'un ou plusieurs « sujet(s) » (100 types de sujets, 2 085 sujets affectés en tout), à savoir un mot-clé rendant compte de la thématique générale de l'article (voir Illustration 2). Les trois premiers « sujets » renvoient clairement à la criminalité, et même la pornographie est légèrement plus mentionnée que la protection de la vie privée (en sixième position). Cette dernière, pourtant fondamentale dans la conception de Tor, apparaît comme un sujet presque minoritaire (70 documents), largement concurrencé par le « cybercrime », la drogue, la pornographie, voire la pédopornographie (le sujet de la « maltraitance sur les enfants » spécifiquement compte 45 documents). Ce, même si un certain nombre d'articles des catégories « informations politiques générales » et « informations sociétaires (sic) et industrielles » pourraient s'en rapprocher, et que cette catégorisation ne donne que la tonalité générale de l'article, sans exclure que d'autres sujets soient également abordés sur un mode mineur. La moitié des articles du corpus traitent essentiellement d'activités criminelles sur Tor (crime, enlèvement, trafic d'êtres humains, terrorisme, recel, pédopornographie...). Factiva propose enfin un nuage de mots et expressions, fondé sur la récurrence des mots et groupes nominaux dans le corpus. Le terme « *dark web* » est le plus employé (355), devant « *deep web* » (198) et « *dark net* » (98) qui restent parmi les occurrences les plus nombreuses. Ce, bien avant « *personnal data* », qui a néanmoins le mérite d'apparaître.

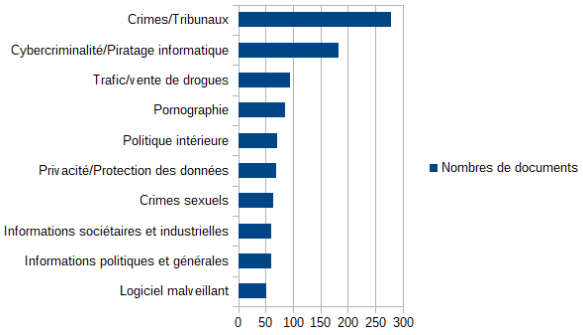


***Figure 2** : Les dix premiers "sujets" des articles de presse incluant le terme "onion router" selon Factiva au 13/08/2018.*

Il va sans dire que ce discours médiatique n'est pas neutre. Certes, il est fait de Tor bien des usages illégaux, voire criminels (voir la partie ). Pour autant, le fait que ces pratiques soient préférentiellement mises en avant nourrit et légitime indirectement une

volonté de contrôle de cet espace. Au-delà de la sphère médiatique, dont on peut supposer que la recherche de sensationnel est le principal moteur, les discours alarmistes permettent surtout au pouvoir politique d'asseoir la régulation policière de l'espace des *hidden services*.

### *2.1.2. Dans le discours des pouvoirs publics*

Depuis 2015, c'est souvent à travers la lutte antiterroriste que Tor est évoqué dans les médias, en particulier par les pouvoirs publics. Alors ministre de l'Intérieur, Bernard Cazeneuve a même explicitement déclaré que « Ceux qui nous frappent utilisent le *Darknet* et des messages chiffrés pour accéder à des armes » à l'Assemblée nationale le 22 mars 2016, à la suite des attentats de Paris et Bruxelles. Ce, même si l'achat d'armes pour les attentats de 2016 est vraisemblablement passé par des voies plus classiques[12].

Plus récemment, en juin 2017, le président français Emmanuel Macron déclarait quant à lui vouloir encore « améliorer les moyens d'accès aux contenus cryptés (sic), dans des conditions qui préservent la confidentialité des correspondances, afin que ces messageries ne puissent pas être l'outil des terroristes ou des criminels »[13]. Une telle déclaration cible directement l'utilisation de moyens de communication chiffrées de pair à pair, et plus indirectement des solutions comme Tor. Dans tous les cas, il s'agit de rendre possible le déchiffrement de contenus chiffrés, par les pouvoirs publics et plus seulement par les interlocuteurs concernés.

En août 2018 enfin, les représentants des services de renseignement de l'Australie, des États-Unis, de la Grande-Bretagne, du Canada et de la Nouvelle-Zélande, qui collaborent très activement dans la collecte et le traitement de masse de données personnelles, ont à leur tour réaffirmé leur opposition au principe du chiffrement de bout en bout, dans le but affiché de lutter contre la criminalité et contre le terrorisme (« Five Country Ministerial 2018 », 2018). Là encore, des protocoles comme celui de Tor sont visés. La divulgation de documents professionnels internes à la NSA et au GCHQ par Edward Snowden avait par ailleurs déjà révélé en des termes on ne peut plus clairs l'opinion de membres de ces services de renseignement : « Tor pue » (« *Tor stinks* »), car il permet de dissimuler la majorité des identités de ses utilisateurs (Ball *et al.*, 2013). On peut raisonnablement estimer que cette opinion était et reste répandue dans ces milieux, et qu'elle donne encore une clé de lecture pertinente des déclarations plus récentes sus-évoquées.

Les sorties de M. Macron ou de M. Cazeneuve et, plus largement, les revendications policières réclamant toujours plus de dérogations pour utiliser les données personnelles des citoyens et passer outre leur chiffrement, participent donc

---

[12] Voir l'article « Coulibaly aurait acheté des armes à un Carolo », F. D., La Dernière Heure, 14 janvier 2015. En ligne : http://www.dhnet.be/actu/monde/coulibaly-aurait-achete-des-armes-a-un-carolo-54b589723570c2c48acc1704. Consulté le 01/XI/2016.

[13] Déclaration d'Emmanuel Macron lors de la déclaration conjointe avec Theresa May le 13 juin 2017. En ligne : http://www.elysee.fr/declarations/article/declaration-d-emmanuel-macron-lors-de-la-declaration-conjointe-avec-theresa-may/ (consulté le 13/08/2018).

surtout d'une logique séculaire du pouvoir policier : l'intérêt est d'avoir un accès facile à un maximum d'informations dans tous les espaces de la vie sociale[14]. Cette volonté de lutte contre les moyens de chiffrement, dont Tor, s'inscrit historiquement dans la suite des *Crypto Wars* américaines et françaises (Tréguer, 2017, chap. 9), qui ont vu la progressive « libéralisation » (*idem*) des moyens de chiffrement pour les citoyens, sans contrôle étatique. Avec les attentats de New York le 11 septembre 2001 (Tréguer, 2017, p. 413-414), puis ceux de Paris en janvier et novembre 2015, la volonté des pouvoirs publics de limiter l'effectivité des solutions de chiffrement est de plus en plus (ré)affirmée. Entretenir la réputation sulfureuse d'outils comme Tor permet de justifier la restriction des libertés individuelles dans le domaine. Cette représentation pour le moins dépréciative de Tor a même été inscrite au *Journal officiel de la république française* n°0225, texte n°110, en septembre 2017. La traduction officiellement préconisée pour « *dark net* » y est « internet clandestin », dont la définition précise qu'elle s'étend également « par extension, [à] l'ensemble des activités, souvent illicites, qui y sont pratiquées ». Cette définition officialise un des usages courants qui fait du « *dark web* » la partie illégale du « *deep web* » - ce dernier terme étant traduit de manière plus neutre par « abysses » ou « toile profonde ».

### 2.2. *Le Marianas Web* : une mise en fiction du *deep web*

Au-delà de ces représentations plus ou moins idéologiques sur les *hidden services* dans les médias ou dans les discours politiques, ces derniers inspirent la production d'images, voire de véritables fictions, portant plus spécifiquement sur la notion de « profondeur » du *deep web*. Une imagerie souvent reprise est par exemple celle de l'iceberg, dans laquelle la partie émergée figure le WWW, et la partie immergée le « *deep* » voire le « *dark web* ». Mais le recours aux métaphores de la profondeur et de l'ombre pour décrire le web .onion peut également dépasser le simple intérêt illustratif ou didactique pour prendre une dimension complètement fictionnelle, sans qu'il soit toujours évident de faire la part des choses entre l'erreur, la désinformation, voire la légende urbaine ou le canular.

Je m'intéresserai particulièrement ici au discours sur le « *Marianas web* », qui est le meilleur exemple de dérive à partir de la métaphore de la profondeur. Tout un discours sur les prétendus « niveaux » d'Internet s'est développé avec l'émergence du web .onion, dans lequel l'incompréhension technique le dispute à la désinformation, voire à l'affabulation pure et simple. La description de ces niveaux est assez fluctuante, même s'ils sont souvent au nombre de cinq. Une infographie humoristique (voir Illustration 3) publiée le 1er septembre 2012 sur le site de partage imgur.com semble en être l'origine. Il est difficile de faire l'histoire d'une légende urbaine et de lui attribuer une origine unique. Elles naissent autant d'un événement déclencheur que d'un substrat plus confus d'idées et de préconceptions qui les rendent possibles et leur donnent forme.

[14] Dans *Surveiller et Punir*, Foucault décrit la police, depuis le XVIIIe siècle, comme « (…) un appareil qui doit être coextensif au corps social tout entier et non seulement par les limites extrêmes qu'il rejoint, mais par la minutie des détails qu'il prend en charge. Le pouvoir policier doit porter "sur tout" (...) » (Foucault, 1975, p. 249).

Néanmoins, la journaliste Violet Blue propose une lecture du phénomène et a tracé l'origine de cette légende urbaine dans un article pour le site web Engadget (Blue, 2015).

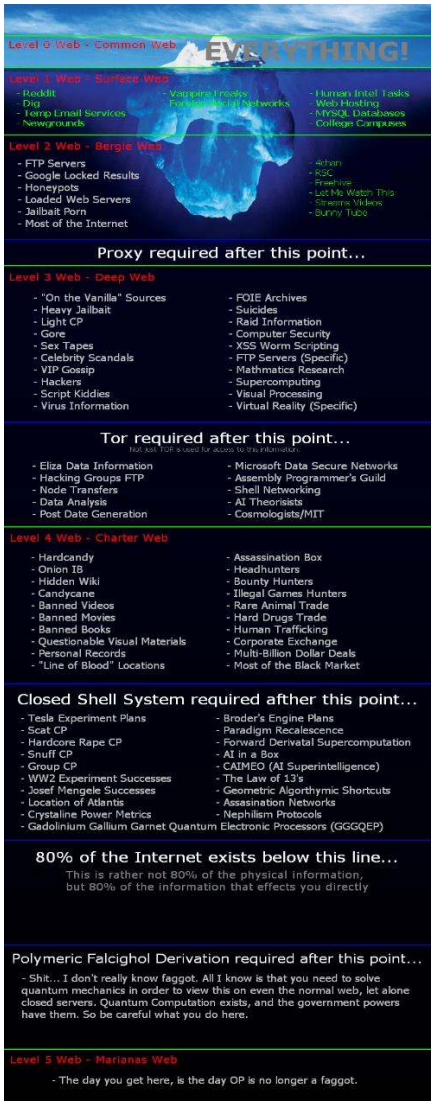


***Figure 3*** *: Les prétendus "niveaux du Web" selon une infographie humoristique (source: https://imgur.com/vvXru).*

Le premier niveau est généralement le « web clair », à savoir le WWW, dont la définition est plus ou moins bien rendue. Du deuxième au quatrième niveau, on oscille entre « *deep web* » simple (*hidden services*, intranets gouvernementaux, réseaux de hackers) et « *dark markets* » (les plateformes de vente en ligne proposant des produits illégaux, comme des armes, des logiciels de piratage ou des drogues). Le cinquième niveau est presque toujours le mythique *Marianas web*, à propos duquel les opinions varient. Nommé en l'honneur de la fosse des Mariannes dans l'océan Pacifique, il pourrait être

l'infrastructure de base absolue d'Internet, ou encore un réseau occulte tenu par les services de renseignement ou par les hackers les plus talentueux. Les informations qui y circuleraient seraient hautement confidentielles. Les protocoles de communication y seraient si radicalement différents qu'il faudrait un « ordinateur quantique » pour le parcourir.

Elle n'était qu'une farce au départ, mais l'image est devenue virale, et certains l'ont prise au sérieux. Soit, au second degré, pour en faire par exemple le prétexte à un blog littéraire[15]. Soit, au premier degré, dans des espaces de conversation variés (forums, sites de partage, blogs, commentaires des vidéos sur des sites comme YouTube, etc.). Certains rapportent même « y avoir été », quand ils n'ont pas carrément pu en ramener, non sans risque, des éléments probants[16]. Le *Marianas Web* s'inscrit en fait plus largement dans une sous-culture numérique adolescente, où l'on aime jouer à se faire peur et à effrayer ses amis crédules, tout en se prévalant de compétences informatiques supérieures pour les impressionner. La plupart des contenus signalés comme venant du *Marianas Web* ne font que reprendre les discours complotistes et négationnistes habituels, revisités sous un nouvel angle pseudo-technique.

L'espace de Tor et de ses *hidden services* tel qu'il est représenté dans les exemples vus jusqu'alors est révélateur de l'imaginaire social de personnes qui ont finalement une connaissance technique et empirique limitée des protocoles et des lieux de Tor. Les désignations métaphoriques telles que « *deep web* » ou « *dark web* » semblent jouer un rôle prééminent dans la construction de cet imaginaire. Cela concourt à donner de Tor et de ses *hidden services* l'image d'un réseau à part, presque disjoint d'Internet et du WWW. Mais au-delà de ces représentations très souvent exogènes et de la conception du protocole, qu'en est-il des spatialités des utilisateurs de Tor ?

## 3. UN ESPACE DE PRATIQUES EN LIGNE PAS SI SPECIFIQUES

La médiatisation et les prises de position publiques à propos de Tor ne s'appuie généralement pas sur une expérience largement partagée de ces lieux d'Internet : l'espace .onion n'est pas *vécu* par une grande partie des personnes qui (se) le représentent. Si le domaine .onion n'est pas un domaine internétique tout à fait générique dans la mesure où il implique l'utilisation de protocoles qui lui sont propres, les spatialités qui ont cours sur le web .onion sont-elles si spécifiques que les représentations communes le suggèrent ?

---

[15] Le blog « *Search for Marianas Web* », initié en 2013 et toujours actif au 14 août 2018, est une des initiatives du genre les plus poussées. Il est consultable à l'adresse http://searchformarianasweb.tumblr.com.

[16] Un exemple, par ailleurs anecdotique, est celui de ce membre de YouTube qui fournit une liste des sites qu'il a pu y trouver à cette adresse : https://ghostbin.com/paste/fndv8. Trafic d'êtres humains, cultes sataniques, *snuff movies*… on retrouve l'éventail de fantasmes qui avaient cours à propos d'Internet à ses débuts, et des *hidden services* aujourd'hui.

### 3.1. « *Going deeper ?* »

La métaphore de la profondeur est la plus reprise quand il s'agit d'évoquer Tor et ses *hidden services*. Elle laisse notamment entendre qu'il y aurait plusieurs « niveaux » d'Internet, plus ou moins compartimentés. De fait, il s'agit d'un *topos* qu'on retrouve bien souvent dans les conversations à propos de réseaux comme Tor, et jusque dans des sites ou des forums qui sont eux-mêmes des *hidden services*. L'un des sites d'actualités dédiés les plus actifs, DeepDotWeb.com (aussi disponible *via* Tor à DeepDot35Wvmeyd5.onion), et créé fin 2013, reprend par exemple la métaphore de la profondeur dans sa devise : « *Surfacing the News of the Deep Web* ».

La volonté « d'aller plus profond » est suffisamment répandue parmi les (néo)utilisateurs de Tor pour que le réseau social Galaxy2, très actif avant sa désactivation en 2017, ait d'ailleurs dû y consacrer un paragraphe pour prévenir les nombreuses demandes de personnes qui se seraient mises à utiliser Tor à cette fin, ou pour partir en quête du *Marianas Web* : « [Question] *Going deeper?* [Réponse] *Depends on your definition of "going deeper". If you refer to the image with an iceberg and wants to get into the next "level", then you might have misunderstood some things at best, or be the target of a prank/troll at worst. "Going deeper" is more about exploring more taboo and/or hidden subject rather than entering a new "physical/virtual" level. The .clos network and Mariannas* (sic) *Web are also a scams* »[17]. Dépassant la seule mise au point technique sur l'absence de niveaux du Web, cette rubrique propose une explication de ce qui ferait l'intérêt métaphorique de la notion de profondeur appliquée aux *hidden services* de Tor : pouvoir parler de sujets considérés comme « tabous ».

La profondeur du « *deep web* » serait donc d'abord celle des échanges qui s'y tiendraient, par opposition à la superficialité supposée des conversations tenues sur le WWW. Contrairement à ce qu'Elizabeth Stoycheff a pu observer sur Facebook à propos notamment des pensées minoritaires ou subversives après les révélations Snowden, il n'y aurait pas de « *chilling effect* » (Stoycheff, 2016) inhibant la liberté d'expression sur Tor. S'il ne s'agit pas de dire qu'il est impossible d'exprimer des opinions minoritaires ou subversives sur le WWW, force est de constater qu'elles sont très répandues sur une large part des lieux de discussion .onion. À titre d'exemple, un groupe de discussion parmi les plus animés dans la durée sur Galaxy2 avait été initié par une femme curieuse de recueillir sans jugement la parole de pédophiles. Il semblerait que les restrictions éventuelles à la liberté d'expression dans les lieux de discussion .onion soient d'abord le fait des hébergeurs eux-mêmes, selon leurs valeurs éthiques personnelles.

---

[17] FAQ de *Galaxy2*, consultée le 29/11/2016, et auparavant accessible *via* Tor à cette adresse : http://w363zoq3ylux5rf5.onion/pages/view/45634/faq L'URL a été reprise par *Galaxy3*, nouveau site de réseautage social reprenant les codes graphiques de Galaxy2 mis en ligne le 25 juillet 2018.

L'idée qu'une différence de nature existerait entre le WWW et le web .onion semble globalement partagée et diffusée par une grande partie des utilisateurs et vulgarisateurs du web .onion, dans les conversations en ligne (Gehl, 2016) ou dans les textes introductifs à Tor. Elle fait d'ailleurs écho à la critique médiatique et politique récurrente sur le fait que la dissimulation possible des identités légales sur Tor ouvrirait précisément la porte aux pratiques les plus répréhensibles. Il y a un contraste fort entre ces deux groupes à propos de cette spécificité de Tor : volontiers effrayante et dangereuse pour les uns, elle est plutôt considérée comme positive et libératrice pour les autres. Robert W. Gehl, sur la base d'une étude anthropologique du forum .onion anglophone *Dark Web Social Network* et d'entretiens avec certains de ses membres, a ainsi identifié une tendance au « tehno-élitisme » (Gehl, 2016, p. 1228, trad. pers.), qu'il présente comme « structurante pour la communauté » (*idem*). Malgré le fait que le web .onion ne soit constitué que de pages web tout à fait classiques, majoritairement en HTML, il n'est en fait pas si facile d'y évoluer pour la plupart des internautes (Winter *et al.*, 2018). Ce techno-élitisme se manifeste par les spatialités en ligne spécifiques des personnes fréquentant ce forum, permises par leur plus grande « maîtrise spatiale » (Lussault, 2013, p. 44) d'Internet. Cette plus grande maîtrise se fonde notamment sur :

- leur « compétence d'emplacement » : ils connaissent les lieux d'intérêt du web .onion, ne serait-ce que par leur présence sur le *Dark Web Social Network* ;
- leur « compétence de franchissement » : ils savent utiliser l'outil technique permettant de naviguer tant sur le WWW que sur le web .onion.

On peut ici faire un parallèle entre les « [communautés] » (Gehl, 2016) .onion et la « Mouvance du logiciel libre » (Giraud & Schoonmaker, 2015), à laquelle appartient du reste le projet Tor. Dans les deux cas, il y a investissement d'une « marge » valorisant « l'idée de liberté (autonomie, déréglementation, souveraineté) » (Giraud & Schoonmaker, 2015, paragr. 5). Cette marge est celle « d'espaces d'avant-garde » (*idem*, paragr. 1) qui, en n'étant pas « [hypercentraux] » comme le sont Facebook ou Google sur Internet (Beaude, 2012), offrent la possibilité de les habiter autrement, et notamment sans régulation étatique / policière. Il s'agit en somme moins d'aller *plus profond* que d'aller là où l'on peut être libre, là où « l'anomie peut alors devenir autonomie ; [et] le contact avec la sauvagerie ou le chaos, une interface de commutation voire de compossibilité entre espaces de représentation différents » (Giraud & Schoonmaker, 2015, paragr. 1)[18]. Certains discours sur le web .onion francophone vantent ainsi l'absence de carcan et l'ouverture d'esprit supposée des personnes fréquentant le « DW » (« *deep web* ») par rapport au « *clear* » (le WWW) *:*

[18] Si l'on reprend le propos du livre d'Alexander Galloway en 2004 évoqué dans la partie 1.2., il est intéressant de noter que les *hidden services* relancent en pratique l'idée d'un Internet décentralisé, en ne conservant que la pile « horizontale » de protocoles TCP/IP, sans le contrôle « vertical », et notamment étatique, introduit par l'usage généralisé du protocole DNS.

> *« Arf faut dire ce qui est aussi, vous ne trouverez pas des exemples d'escroqueries ou des conseils pour tuer votre beau père sur le clear ou alors vous serez vite banni du forum.*
> *La liberté d'expression ici est bien plus importante et permet a la fois de trouver des renseignements que l'on a pas ailleurs mais aussi des liens ou des personnes pouvant vous aider a arriver a vos buts.*
> *Ici on croise toute sorte de gens, une Multiconnexion comme j'aime l'appelé, permettant de discuter et trouver son "bonheur" ou d'essayer de comprendre certaines personnent plus ouvertes a la discution.*
> *De plus nous pouvons parler librement de sujets dit "tabou" sur le clear, la vrai liberté d'expression je la trouve sur le DW. (...) »*

*(Extrait de message du sujet « votre point de vue du deep fr » sur le forum* French Deep Web *par Yaka, publié le 27 août 2018 : http://fdwochsnity6vzwd.onion/viewtopic.php?pid=667696#p667696).*

On remarquera cependant que la « vrai (sic) liberté d'expression » vantée par ce participant au forum *French Deep Web* se manifeste par le type de renseignements disponibles, la qualité et la diversité des interlocuteurs potentiels, mais d'abord et avant tout par la possibilité d'aborder des sujets illégaux, voire criminels, sous un angle très pragmatique. Le web .onion est-il donc aussi « *dark* » que le présentent volontiers ses détracteurs ?

### 3.2. Criminalité et « *dark web* »

À l'instar des représentations iconographiques exogènes, beaucoup de pages .onion adoptent l'imagerie de l'ombre et de la dissimulation, sans forcément proposer de contenus illégaux par ailleurs. Les thèmes graphiques sombres sont très communs, et contrastent avec les couleurs plus claires qu'on retrouve sur la plupart des sites web classiques. Il ne faut cependant pas exagérer l'importance de ces choix graphiques : nombres de sites .onion très fréquentés ne les reprennent pas. Les *hidden wikis*, qui proposent des listes thématiques de liens .onion, utilisent pour la plupart le moteur MediaWiki développé pour Wikipédia, et reprennent son fond blanc. Même de grandes places de marché illégales (ou « *dark markets* ») comme Dream Market ou Silk Road 3, ou des méta-moteurs de recherche sur ces places de marché, comme Grams, reprennent l'esprit des chartes graphiques de sites du WWW comme eBay ou Google. On peut même faire l'hypothèse que bien des sites .onion reprenant jusqu'à la caricature l'imagerie du « *deep dark web* » cherchent à attirer les utilisateurs novices en quête des contenus sulfureux qu'on ne trouverait que sur le « *dark net* », selon la connaissance qu'ils en ont eu à travers les discours les plus courants. La page d'accueil du site Shadow Web**Erreur ! Source du renvoi introuvable.**, une arnaque ancienne et bien connue du web .onion, en est une bonne illustration. La couleur de fond est noire, l'image centrale présente une descente d'escalier suggérant l'accès à des contenus plus « profonds ». Le texte d'accompagnement insiste sur le caractère « secret » et trop « sombre pour le *deep web* » (trad. pers.) des contenus proposés.

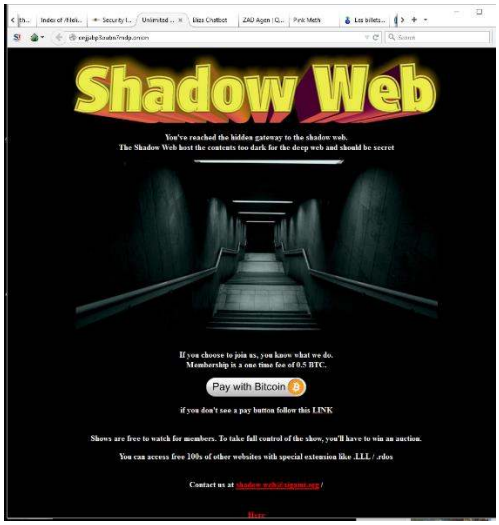


***Figure 4**: Page d'accueil du site .onion Shadow Web (11/05/2016).*

Mais au-delà de l'imagerie et des arnaques de ce type, qu'en est-il de la prévalence de la criminalité sur le web .onion, dont on a vu qu'il était volontiers présenté comme un moyen privilégié d'accéder à des contenus, des services, ou encore des biens illégaux ? Deux estimations se voulant exhaustives ont notamment été proposées.

En 2016, la société Intelliag a estimé que 48 % des 30 000 sites .onion recensés par leur *spider* proposaient des contenus ou services illégaux au sens des droits des États-Unis et du Royaume-Uni (Intelliag, 2016). Cette estimation se fonde sur les résultats d'un algorithme d'apprentissage profond, entraîné à partir de la catégorisation manuelle de 1 000 sites .onion. Les sites de partage illégal de fichiers soumis à droit d'auteur et de diffusion illégale de fichiers (« *leaked data* ») compteraient pour près de 60 % de la quinzaine de milliers de sites illégaux recensés. La chercheuse indépendante Sarah Jamie Lewis nuance ces résultats dans son premier *OnionScan Report* (Jamie Lewis, 2016) : elle avance qu'une part importante des sites recensés comme illégaux par Intelliag étaient hors ligne au moment de son propre *scan*, et que nombre des pages d'accueil des sites restants étaient des clones parfaits après comparaison à l'aide d'une fonction de hachage. Si tant est que la procédure d'identification des sites illégaux par Intelliag soit pertinente, la proportion de 48 % de sites illégaux lui semble devoir être fortement revue à la baisse. Ce, à plus forte raison que cette pratique de multiplication de sites identiques avec des adresses différentes est généralement le fait des arnaqueurs prétendant proposer des contenus illégaux contre rémunération, ou encore des éditeurs souhaitant multiplier les adresses possibles pour un même site (par souci de redondance ou encore pour répartir la charge des connexions). Sarah Jamie Lewis n'est cependant pas en mesure d'indiquer si la proportion de clones et de sites hors-ligne est la même en ce qui concerne les services .onion considérés comme légaux dans la base de données d'Intelliag, ce qui limite également la portée de sa critique.

Une autre évaluation du nombre de services .onion illégaux a été proposée par Daniel Moore et Thomas Rid début 2016 (Moore & Rid, 2016). Ils ont également procédé à un *crawl* entre janvier et mars 2015 qui leur a permis de recenser 5 205 sites actifs, dont 2 723 proposant du contenu textuel. Ils ont ensuite recouru eux aussi à un traitement algorithmique à l'aide d'une machine à vecteurs de support entraînée à partir d'un échantillon de sites labellisés manuellement. Au terme du traitement, 1 547 sites .onion relèveraient d'activités illégales, soit 57 % du total. Les deux auteurs ont identifié douze types d'activités illégales. Parmi les sites jugés illégaux, les deux premières catégories sont « Drogues » et « Finance », ce qui ne correspond pas aux résultats obtenus par Intelliag.

| Category | Websites |
|---|---|
| None | 2,482 |
| Other | 1,021 |
| Drugs | 423 |
| Finance | 327 |
| Other illicit | 198 |
| Unknown | 155 |
| Extremism | 140 |
| Illegitimate pornography | 122 |
| Nexus | 118 |
| Hacking | 96 |
| Social | 64 |
| Arms | 42 |
| Violence | 17 |
| Total | 5,205 |
| Total active | 2,723 |
| Total illicit | 1,547 |

***Tableau 1** : Décompte et catégorisation des sites .onion illégaux d'après Moore et Rid (2016).*

La différence de résultats entre Intelliag et Moore & Rid en ce qui concerne leur typologie ou le nombre de services recensés n'est pas étonnante : on ne sait rien de précis du *crawler* d'Intelliag, mais son programme diffère *a priori* de celui du *crawler* de Moore et Rid, ainsi que leurs jeux respectifs d'adresses initiales, et leurs dates de collecte. Il est plus surprenant que les types d'activités illégales en ligne proposés dans ce rapport et cet article diffèrent à ce point. Néanmoins, tous deux pointent le fait que les contenus et services illégaux, y compris ceux visant à arnaquer des aspirants arnaqueurs, sont très présents sur les *hidden services*. Même si les activités délictuelles et criminelles sont présentes aussi sur le WWW, il ne fait guère de doute non plus que c'est en moindre proportion que sur le web .onion, tant en termes de nombres de sites concernés que d'échanges entre individus. La navigation *via* Tor, et en particulier sur le web .onion, est en effet moins aisée que sur le WWW du fait de temps de latence élevés, d'une capacité réduite, et de l'absence de moteurs de recherche efficaces. En outre, là où la majorité de la population est connectée à Internet, en particulier dans les pays développés, le nombre d'utilisateurs de Tor est en comparaison infime, limitant d'autant l'effet de réseau pour la sociabilité. Le web .onion est aujourd'hui surtout fréquenté par des personnes pour qui le gain en termes de dissimulation de leur identité dépasse ces inconvénients non négligeables (Winter *et al.*, 2018). Divers types d'activités illégales ou criminelles ont bel et bien cours sur les *hidden services* de Tor.

Il ne fait guère de doute que le trafic de drogues concentre une grande part, sinon la majorité des activités illégales du web .onion : la vente par correspondance de drogue y est facile et assez peu risquée, et le web .onion fournit en outre des espaces d'échange entre consommateurs et/ou entre vendeurs propices à la réduction des risques (la rencontre physique avec un vendeur n'est plus nécessaire, les produits sont de meilleure qualité) et à la meilleure connaissance des produits et de leurs modes de consommation (Bancroft & Reid, 2015; Van Hout & Bingham, 2013). Ainsi, en deux ans et demi d'activité, la première version du célèbre « *dark market* » Silk Road (fermé par le FBI en 2013) aura généré un chiffre d'affaires d'1,2 milliards de dollars étatsuniens, essentiellement lié au commerce de drogues (Frediani, 2016).

La pédopornographie serait également un domaine d'activités criminelles très représenté sur les *hidden services* d'après le résultat des *crawls* sus-évoqués. Cependant, le partage de contenus pédopornographiques semble mieux adapté à des réseaux orientés vers le partage de fichiers de pair à pair, comme Freenet ou I2P, mode de partage qui ne permet pas la pseudonymisation de l'adresse IP dans le protocole de Tor (Aked, 2011). Des *hidden services* utilisant plutôt des protocoles comme FTP (*File Transfer Protocol*) *via* Tor n'en existent pas moins. Il existe également des sites .onion diffusant des contenus pédopornographiques sur des pages .html. Lolita City, site .onion fermé en 2011 par le collectif hacktiviste Anonymous (Gallagher, 2011), en a longtemps été la figure de proue. Il est difficile d'évaluer à quel point des réseaux comme Tor, I2P ou Freenet sont employés par des pédocriminels, l'accès à la plupart de ces contenus étant soumis à autorisation par les hébergeurs, souvent après un processus de cooptation. Le collectif Anonymous, qui s'inscrit dans une mouvance *a priori* favorable à l'utilisation généralisée de Tor et consorts, n'en a pas moins effectué en 2011 une attaque par déni de service contre le principal acteur .onion d'hébergement gratuit et non modéré, Freedom Hosting, après avoir affirmé qu'il hébergeait la majeure partie des fichiers pédopornographiques accessibles *via* Tor. Cette opération a été le prélude à la fermeture du service par le FBI la même année (Poulsen, 2013).

D'autres types d'activités illégales ont lieu assez couramment sur les *hidden services*, comme l'échange de numéros de cartes de crédit volées, la vente de logiciels piratés, de virus ou de contenus privés volés, etc. L'évaluation de leur importance relative est à ce jour difficile, ce qu'illustre les différences entre les recensions et les typologies proposées par Intelliag et Moore & Rid. Sur le web .onion francophone, le forum French Deep Web abrite ainsi de nombreux sujets dédiés à l'escroquerie (*carding*, usurpation d'identité bancaire…), au piratage informatique, ou encore à l'achat et à la consommation de drogues illégales, en plus de classiques sections d'actualités ou de présentation des membres.

On peut donc faire l'hypothèse que les délinquants et les criminels sont sur-représentés sur le web .onion par rapport au WWW. Eric Jardine avance que cette sur-représentation serait plus importante dans les pays démocratiques où la répression policière contre les activistes est moins forte (Jardine, 2015), même si cette assertion semble tenir surtout au fait qu'Eric Jardine distingue entre criminalité et certaines

formes d'activisme qu'il considère légitimes, là où ces formes d'activisme sont simplement considérées comme criminelles dans les régimes autoritaires qu'il évoque. Pour nuancer l'importance de la sur-représentation apparente des pages proposant des contenus illégaux sur le web .onion, il faut également préciser qu'il n'est pas toujours aisé de faire la part des choses entre les offres véritables et les arnaques ou *scams*. Le consensus général qui semble se dégager dans les échanges tenus en ligne par les utilisateurs de Tor est qu'une grande part des pages proposant des services illégaux sont en fait des arnaques elles-mêmes. En matière de drogues, si l'affaire *Silk Road* a fait grand bruit, une part non-négligeable du trafic en ligne n'en a pas moins lieu sur le WWW. Paradoxalement moins bien connu que le trafic sur les *hidden services*, il concernerait davantage les drogues de synthèse au statut légal flou, ou des drogues illégales dont la vente est organisée notamment sur des réseaux sociaux ou les messageries privées de forums de discussion du WWW, selon un rapport de l'European Monitoring Centre for Drugs and Drug Addiction (Mounteney *et al.*, 2016). En matière d'activités illégales en ligne plus généralement, il faut également noter que le site Infraud, fermé le 27 juin 2018 par les polices de plusieurs pays occidentaux, aura réalisé un chiffre d'affaire d'un demi-milliard de dollars étatsuniens en sept ans d'existence sur le WWW, soit plus longtemps que Silk Road 1 et Alphabay réunis (Greenberg, 2018). En matière de terrorisme, il apparaît de plus en plus clairement que la propagande, la radicalisation, et même une bonne partie des communications plus opérationnelles, se font essentiellement sur le WWW : les pouvoirs publics travaillent d'ailleurs surtout avec de grands acteurs du WWW comme Twitter, Facebook ou Google pour réguler la propagande terroriste (Crosset & Dupont, 2018).

En somme, bien que les utilisateurs eux-mêmes se représentent le web .onion comme spécifique et reprennent volontiers les métaphores spatiales de l'ombre et de la profondeur pour marquer cette différence, il s'agit plutôt d'évoquer la plus grande liberté d'expression qui y serait possible. Et la présence de contenus et de services illégaux et criminels sur le web .onion ou sur d'autres services internétiques proches *via* Freenet ou I2P, même importante, ne doit pas faire oublier que le WWW est largement touché aussi, malgré le fait que les internautes et les services y soient plus facilement traçables par défaut.

## CONCLUSION

J'ai proposé d'interroger la pertinence ou « [vivacité] » métaphorique (Ricoeur, 1975) des notions de profondeur et d'ombre motivant l'emploi des termes « *deep web* » et « *dark web* », à l'aune d'une lecture du réseau des *location-hidden services* de Tor comme un espace conçu, perçu et vécu (Lefebvre, 1974).

En abordant Tor d'un point de vue technique, comme un espace conçu, la légitimité de l'emploi des épithètes « *deep* » et « *dark* » accolées à « web » semble tantôt justifiable, tantôt inopportune, selon les protocoles considérés. L'intérêt de l'emploi du terme web semble en revanche plus évident : associé au WWW, il connote l'utilisation

de protocoles de la couche application et de langages utilisés également *via* Tor. En ce sens, l'opposition entre *World Wide Web* ou simplement Web (entendus comme nom propre et éventuellement naturalisés en français) et web .onion (désignant un réseau de sites et de pages web se distinguant par leur TLD) me semble intéressante. La logique semble pouvoir s'étendre sans problème de compréhension au reste du vocabulaire courant du Web : forum .onion, lien .onion, service .onion, etc. selon la norme suivie dans le présent article.

Plus spécifiquement, l'usage des métaphores désignant les *hidden services* renvoie à l'idée d'une profondeur cachée et d'une inaccessibilité pour le « *deep* », à laquelle il faut rajouter l'idée d'une illicéité, voire d'une monstruosité des usages pour le « *dark* » – les deux champs notionnels se recoupant aussi parfois. De ce point de vue, l'analyse de productions fictionnelles, textuelles et/ou iconographiques nous a permis de mettre au jour tout un imaginaire puissamment fécondé par ces métaphores, métaphores dont l'intérêt pour la production artistique est indéniable. L'analyse de discours médiatiques et politiques a, pour sa part, révélé une certaine crispation autour d'enjeux sécuritaires et policiers, qui font rejouer des peurs anciennes sur les dangers d'Internet à ses débuts – même s'il est désormais d'un usage banal – ou du chiffrement comme arme potentielle entre les mains des criminels et autres terroristes. Chez certains acteurs, il est finalement probable que la métaphore du « *dark* » engendre moins un « horizon d'attente » (Ricoeur, 1985, cité par Debarbieux, 2004) critique à l'égard du web .onion qu'elle n'est en fait engendrée par cet horizon d'attente, négatif *a priori*.

J'ai enfin proposé une lecture plus empirique du web .onion, à travers des études fondées sur la collecte systématique de données qu'on pourrait qualifier « de terrain », au plus proche de la réalité empirique des *.onion. Certaines craintes, exprimées surtout par des acteurs désireux de renforcer la régulation du web .onion, semblent plutôt fondées : la vente de drogue et la pédocriminalité y semblent particulièrement répandues en comparaison de ce qu'on observe sur le WWW. Bien que la concentration de certains types d'activités illicites sur le prétendu « internet clandestin » justifie sans doute une attention accrue des autorités, cela ne doit pas faire oublier que l'essentiel de l'activité criminelle a lieu sur le WWW, dont l'ombre porte beaucoup plus loin que celle des marchés noirs .onion.

Au bout du compte, on peut comprendre que les expressions « *deep web* » et « *dark web* » aient largement été reprises pour parler de Tor et de ses *hidden services* dans le langage courant. Ces métaphores sont même séduisantes à bien des égards. Pourtant, et même si le signifié d'une métaphore n'a pas vocation à être parfaitement adéquat à son signifiant, je préconise de ne pas ou plus employer les termes « *deep web* » et « *dark web* » pour évoquer les *location-hidden services* de Tor (et probablement pas non plus les *eepsites* d'I2P ni les *Freesites* de Freenet), en particulier dans la littérature scientifique. En effet, le flou de la définition de ces termes est aujourd'hui trop grand pour qu'ils soient sérieusement employés pour évoquer Tor, même sur un registre ouvertement métaphorique. Malgré « leur caractère poétique » (Debarbieux, 2014, paragr. 31), dont j'ai essayé de rendre compte, ces termes me semblent devoir être disqualifiés comme

« catégorie[s] analytique[s] ou concept[s] » (*idem*), au risque de donner caution à des expressions créant plus de confusion qu'elles ne concourent à l'intellection des objets qu'elles désignent.

## BIBLIOGRAPHIE


ABLER R. (1977), The telephone and the evolution of the American metropolitan system, In: *The social impact of the telephone*, MIT Press, Cambridge (États-Unis), pp. 318-341.

AKED S. (2011), An investigation into darknets and the content available via anonymous peer-to-peer file sharing, *Australian Information Security Management Conference*.

BAKIS H. (1977), *I.B.M : une multinationale régionale*, Presses universitaires de Grenoble, Grenoble (France), 205 p.

BAKIS H. (1980), Éléments pour une géographie des télécommunications, *Annales de géographie*, vol. 89, n° 496, pp. 657-688.

BAKIS H. (1985), Télécommunication et organisation spatiale des entreprises, *Revue Géographique de l'Est*, vol. 25, n° 1, pp. 33-46.

BAKIS H. (2007), Le « géocyberespace » revisité, *NETCOM*, vol. 21, n° 3-4, pp. 285-296.

BALL J., SCHNEIER B. & GREENWALD G. (2013, octobre 4), NSA and GCHQ target Tor network that protects anonymity of web users, *The Guardian*.

BANCROFT A. & REID P. S. (2015), Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge, *International Journal of Drug Policy*.

BEAUDE B. (2012), *Internet : changer l'espace, changer la société - Les logiques contemporaines de synchorisation*, Limoges (France) : Fyp éditions, 256 p.

BEAUDE B. (2013), *Internet*, *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France) : Belin.

BLUE V. (2015), The myth of Mariana's Web, the darkest corner of the internet, *Engadget*. <https://www.engadget.com/2015/12/18/the-myth-of-marianas-web-the-darkest-corner-of-the-internet/> (page consultée le 11/10/2018).

CASTELLS M. (1996), *The rise of the network society*, Oxford (Royaume-Uni): Blackwell, xvii+556 p.

COMBY É., LE LAY Y.-F. & PIEGAY H. (2011), La presse, une source pour l'étude spatiale et temporelle des attitudes. Potentialités et outils d'analyses des discours sur les crues, In : *Actes de Théo Quant*, Besançon (France).

CROSSET V. & DUPONT B. (2018), Internet et propagande jihadiste : la régulation polycentrique du cyberespace, The Internet and Jihadist Propaganda : The Polycentric Regulation of Cyberspace, *Critique internationale*, n° 78, pp. 107-125.

DEBARBIEUX B. (2004), « Présentation générale. De l'objet spatial à l'effet géographique », In : B. DEBARBIEUX et M.-C. FOURNY (éd.), *L'effet*

*géographique. Construction sociale, appréhension cognitive et configuration matérielle des objets géographiques*, Maison des Sciences de l'Homme - Alpes, Grenoble (France), pp. 11-33.

DEBARBIEUX B. (2014), Enracinement – Ancrage – Amarrage : raviver les métaphores, Rootedness – Anchoring – Mooring : Reviving Metaphors, *L'Espace géographique*, vol. Tome 43, n° 1, pp. 68-80.

DEBARBIEUX B. (2015), *Espace de l'imaginaire : Essais et détours*, CNRS Editions, 266 p.

DESBOIS H. (2015), La carte et le territoire à l'ère numérique, *Socio. La nouvelle revue des sciences sociales*, n° 4, pp. 39-60.

DESFORGES A. (2018), *Approche géopolitique du cyberespace : les enjeux pour la défense et la sécurité nationale, l'exemple de la France*, soutenue le 27 août 2018 à l'Institut français de Géopolitique, Université Paris 8 Vincennes/Saint-Denis, sous la direction de Frédérick Douzet, 398 p.

DINGLEDINE R., MATHEWSON N. & SYVERSON P. (2004), *Tor: The second-generation onion router*, Naval Research Lab, Washington DC (États-Unis), 18 p.

DOUZET F., DESFORGES A. & LIMONIER K. (2014), Géopolitique du cyberespace : « "territoire" », frontières et conflits Présenté à Fronts et frontières des sciences du territoire, Collège international des sciences du territoire, Paris (France), p. 7.

DUFEAL M. (2004), *Les sites web, marqueurs et vecteurs de dynamiques spatiales et économiques dans l'espace méditerranéen français* (Thèse de doctorat, Université d'Avignon et des Pays du Vaucluse).

DUFEAL M. & GRASLAND L. (2003), La planification des réseaux à l'épreuve de la matérialité des TIC et de l'hétérogénéité des territoires, Abstract, *Flux*, n° 54, p. 49-69.

DUPUY G. (2007), *La fracture numérique*, Paris (France) : Ellipses, 158 p.

FEENBERG A. (2004), *(Re)penser la technique : vers une technologie démocratique*, Découverte / M.A.U.S.S., Paris (France), 239 p.

FEENBERG A. L., LICHT J. M., KANE K. P., MORAN K. & SMITH R. A. (1996), The online patient meeting, *Journal of the Neurological Sciences*, vol. 139, pp. 129-131.

Five Country Ministerial 2018, (2018, août).

FREDIANI C. (2016), Deep Web, going beneath the surface, *Freedom from Fear*, vol. 2016, n° 10, pp. 18-21.

GALLAGHER S. (2011, octobre 23), Anonymous takes down darknet child porn site on Tor network, *Ars Technica*. <https://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars> (page consultée le 10/09/18)

GEHL R. W. (2016), Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network, *New Media & Society*, vol. 18, n° 7, pp. 1219-1235.

GIBSON W. (1994), *Neuromancer*, New York (États-Unis) : Ace Books, 278 p.

GIRAUD P.-A. & SCHOONMAKER S. (2015), La marge comme ressource pour l'action dans la mouvance du logiciel libre, *Journal des anthropologues*, n° 142-143, pp. 103-125.

GREENBERG A. (2018, juillet 2), Feds Take Down a Half-Billion Dollar Cybercrime Forum After 7 Years Online, *Wired*.

HOUOT S. (2016), Numérique et islam connectés des internautes européens, *Journal des anthropologues*, n° 146-147, pp. 179-198.

INTELLIAG (2016), *Deeplight : shining a light on the dark web*, 12 p.

JAMIE LEWIS S. (2016, avril 26), OnionScan Report: April 2016 - The Tor Network: Security and Crime, *Mascherari Press*. <https://mascherari.press/onionscan-report-april-2016-the-tor-network-security-and-crime> (page consultée le 05/09/18).

JARDINE E. (2015), *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (SSRN Scholarly Paper n° ID 2667711), SSRN Scholarly Paper, Social Science Research Network, Rochester, NY.

JOLIVEAU T. (2007, octobre 8), Géomatique et géonumérisation, *Monde géonumérique*, blog.

JOLIVEAU T. (2011), « Le géoweb, un nouveau défi pour les bases de données géographiques », *L'Espace géographique*, vol. 40, n° 2, pp. 154-163.

LASSERRE F. (2000), « Internet : La fin de la géographie ? », *Cybergeo : European Journal of Geography*.

LEFEBVRE H.- (1974), *La production de l'espace*, Paris (France) : Éditions Anthropos, 485 p.

LEVY J. (1994), *L'espace légitime : sur la dimension géographique de la fonction politique*, Paris (France) : Presses de la Fondation nationale des sciences politiques, 442 p.

LEVY J. (2003), Lieu, *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France) : Belin.

LEVY J. & LUSSAULT M. (2013), Espace, *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France) : Belin.

LUSSAULT M. (2013), *L'avènement du Monde : essai sur l'habitation humaine de la Terre*, Paris : Seuil, 296 p.

MCLUHAN M. & FIORE Q. (1967), *The medium is the massage*, The Londres (Royaume-Uni): Penguin Press, 157 p.

MITCHELL W. J. (1999), *City of bits: space, place, and the infobahn*, Cambridge (États-Unis): MIT Press, 225 p.

MOORE D. & RID T. (2016), Cryptopolitik and the Darknet, *Survival - Global Politics and Strategy*, vol. 58, n° 1, pp. 7-38.

MOUNTENEY J., GRIFFITHS P. & VANDAM L. (2016), Chapter 13 - What is the future for internet drug markets?, In: *The internet and drug markets*, European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), Lisbonne (Portugal).

PLANTIN J.-C. (2014), Qu'y a-t-il à côté d'un graphe de sites web ?, *Communication & Organisation*, n° 43, pp. 59-70.

POULSEN K. (2013, septembre 13), FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, *Wired*.

RICOEUR P. (1975), *La métaphore vivre*, Paris (France) : Seuil, 411 p.

SCHWANEN T. (2017), Information Technology and Mobility, In: *International Encyclopedia of Geography*, American Cancer Society.

SOLOMON J. (2015, mai 6), The Deep Web vs. The Dark Web, *Everything After Z by Dictionary.com*.

STOYCHEFF E. (2016), Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring, *Journalism & Mass Communication Quarterly*, vol. 93, n° 1.

SYVERSON P. (2005), Onion Routing: History. <https://www.onion-router.net/History.html> (page consultée le 22/12/17)

SYVERSON P. F., GOLDSCHLAG D. M. & REED M. G. (1997), Anonymous connections and onion routingPrésenté à IEEE Symposium on Security and Privacy, *IEEE Comput. Soc. Press*, Oakland (États-Unis), p. 44-54.

THORNGREN B. (1977), *Telecommunications and Regional Development in Sweden*, National Swedish Board for Technical Development.

TREGUER F. (2017), *Pouvoir et résistance dans l'espace public : une contre-histoire d'Internet (XVe -XXIe siècle)* (Thèse de doctorat, EHESS, Paris (France)).

VAN HOUT M.-C. & BINGHAM T. (2013), 'Surfing the Silk Road': A study of users' experiences, *International Journal of Drug Policy*, vol. 24, n° 6, pp. 524-529.

BAKIS H. & VIDAL P. (2007), De la négation du territoire au géocyberespace : vers une approche intégrée de la relation entre espace et TIC, In : C. BROSSAUD et B. REBER (éd.), *Humanités numériques 1 : nouvelles technologies cognitives et épistémologie*, Hermès - Lavoisier, Paris (France), vol. 1, pp. 101-116.

WINTER P., EDMUNDSON A., ROBERTS L. M., CHETTY M. & FEAMSTER N. (2018), How Do Tor Users Interact with Onion Services?, In: *Proceedings of the 27th USENIX Security Symposium*, Baltimore (États-Unis), p. 19.