



Université Toulouse II Jean Jaurès, Master Recherche et Études Sociologiques

Subculture darknet : ethnographie d'une transgression

Présenté et soutenu par

RIHANI Karim

Sous la direction de

FIGEAC Julien

Mémoire de Master II

Année 2017-2018

Remerciements

J'aimerais remercier chaleureusement Julien Figeac, mon encadrant, pour la rigueur qu'il a apporté à mon suivi, ses conseils éclairés et l'intérêt qu'il a porté à mon sujet. Il m'est difficile d'espérer un meilleur encadrement que celui qui m'a été donné. J'ai beaucoup appris grâce à vous. Je remercie également les nombreux enseignant.e.s et chercheur.euse.s qui m'ont transmis leur passion de la sociologie tout au long de mon parcours universitaire.

Je remercie aussi Lucrèce Cousin de Mauvaisin de m'avoir accompagné et soutenu dès ma première année de licence, d'avoir partagé avec moi les moments de doute, de stress mais surtout de joie et d'utopies communes.

Un grand merci à Fanny Seffusatti pour son soutien, son amitié et l'immense aide qu'elle m'a apporté dans cette recherche. Pour toutes ces discussions éclairantes, ces rires et ces encouragements. Je suis fier d'être comme tu le dis, un petit aigle.

Mes pensées vont également à mes parents et à l'amour inconditionnel qu'ils me portent depuis ma naissance. À ma mère qui a toujours cru en moi, merci pour ta confiance.

Enfin, j'aimerais remercier tous mes ami.e.s et proches qui m'ont soutenu durant ces années de travail et de recherche.

Table des matières

Remerciements.....	2
Introduction.....	4
I / Contextualisation du sujet d'étude.....	7
A) Du <i>hacker</i> au <i>cracker</i> , la mutation d'un mouvement.....	7
B) - <i>Deepweb</i> / <i>Darknet</i> : mise à plat des termes.....	11
C) Le réseau Tor, une grande couverture médiatique mais de faibles répercussions universitaires	13
D) L'étude des subcultures au prisme de l'interactionnisme symbolique.....	16
D.1) Subculture transnationale et « groupculture » local.....	18
D.2) Interactions en ligne : « on the internet nobody knows you're a dog ».....	20
II) Définition et analyse d'une subculture en ligne.....	23
A) Mise en place de la méthodologie d'enquête : du recueil de données à l'analyse des pratiques et des représentations.....	24
B) L'observation non participante et le recueil de données.....	25
« Lurk more, it's never enough ».....	25
Répartition du nombre de connexions journalières de 2015 à 2018 pour les dix plus grand pays utilisateurs du réseau Tor.....	27
C) Ethnographie numérique: le cas du forum « DeepNetwork » sur le <i>darknet</i> Tor.....	28
D) Les entretiens exploratoires comme moyen d'accéder aux discours et aux représentations des acteurs.....	30
III / La contestation au travers des règles et des pratiques.....	33
A) Une communauté fondée sur une double prérogative : l'anonymat et la sécurité.....	33
B) L'élitisme technologique comme pratique structurante de la communauté.....	36
C) Normes sociales de la communauté.....	39
C.1) Le statut du règlement intérieur.....	39
C.2) Argot et sociolecte.....	42
C.3) Normes conversationnelles.....	43
C.4) Différenciation des argots en fonction des différentes pratiques.....	45
D) L'expression identitaire à travers la dichotomie de l'espace.....	47
IV / Idéologie de la subculture <i>darknet</i> : Éthique <i>hacker</i> et esprit <i>cracker</i>	50
Principe n°1 : Le <i>darknet</i> est un espace de libertés.....	51
« Freedom is good».....	51
Principe n°2 : L'assistanat est proscrit, soyez autodidacte.....	54
« No problem should ever have to be solved twice».....	54
Principe n°3 : Le <i>darknet</i> peut se montrer impitoyable.....	57
« Anonymous can be a horrible, senseless, uncaring monster».....	57
Principe n°4 : Le <i>darknet</i> est politique.....	60
A) Situer la cybercriminalité dans les <i>darknets</i>	63
B) Une subculture basée sur la transgression.....	65
V/ Conclusion.....	68
Bibliographie.....	71
Annexes.....	75
Résumé.....	77

« Je rêve d'une science - je dis bien une science - qui aurait pour objet ces espaces différents, ces autres lieux, ces contestations mythiques et réelles de l'espace où nous vivons. Cette science étudierait non pas les utopies, puisqu'il faut réserver ce nom à ce qui n'a vraiment aucun lieu, mais les hétérotopies, les espaces absolument autres »

Michel Foucault

Introduction

L'univers des *hackers* fait aujourd'hui l'objet de multiples intérêts et questionnements. Qu'elles soient universitaires, civiles, économiques ou culturelles, ces différentes sphères ne semblent plus ignorer ou méconnaître comme jadis, cette figure contestataire devenue aujourd'hui emblématique à l'ère du numérique. Depuis les *hackers* pionniers de la Sillicone Valley des années 70 aux mouvements Anonymous de 4chan¹ en 2011, la figure du *hacker* se retrouve aujourd'hui médiatisée ponctuellement sous différentes formes mais apparaît toujours sous la même appellation médiatique : « *hacker-s* ».

L'unidimensionnalité suggérée par cette appellation renvoie en réalité à un univers vaste² d'appartenances et de pratiques culturelles dans lequel des sous-groupes sont pourvus d'intérêts multiples.

C'est donc davantage sous la forme inclusive de « culture » *hacker* (ou plutôt « subculture ») que l'objet peut être saisi dans sa globalité sans être réduit à une entité homogène. Mais alors qu'est-ce qu'un *hacker* et à quoi renvoie sa culture ?

Selon Manuel Castells et Eric Raymond, les *hackers* sont une communauté d'experts en programmation et de génies des réseaux s'exprimant par un sentiment collectif fondé sur la participation active à une communauté qui se structure autour de coutumes et de principes informels d'organisation sociale³. Tantôt médiatisés comme « bidouilleurs » (Lallement, 2015) au travers des *hackers spaces* ou encore comme pirates informatique par la figure du *crackers*, on comprend dès lors que le « monde des *hackers* » est étendu et les facettes inexplorées de ce mouvement sont multiples. Aujourd'hui la figure du *hacker*-bidouilleur, animé par le désir créatif du détournement

1 Un image board connu pour son canal /b, berceau du mouvement Anonymous.

2 CASTELLS, Manuel (2001), *La galaxie internet*, Paris, Fayard

3 Raymond 1999, p.231 Castells, 2002, p.64

d'objets, reprend de l'ampleur au détriment de la figure plus contestée du *cracker* informatique. *Cracker* qui renvoie à des pratiques illégales de piratage, de déviances et qui est souvent assimilé à un autre univers tout aussi contesté : celui des *darknets*.

Le *darknet* le plus connu, le réseau «Tor », a eu une médiatisation assez conséquente ces dernières années et ce, depuis l'affaire de « *The silkroad* » en 2013, un marché noir en ligne.

La communauté journalistique qui ne tarda pas à couvrir le sujet⁴ après la fermeture du site, y vit une nouvelle charge de scandale et y décela un monde numérique souterrain où apparaissait une cybercriminalité qui leur était insoupçonnée jusqu'ici. Le réseau Tor qui totalise en 2018, près de 4 millions de personnes connectées dans différents pays⁵ est un pan de cette culture *hacker* qui reste largement méconnue et est souvent renvoyée à la déviance et aux simples échanges marchands⁶.

Ce logiciel gratuit qu'est Tor, donne ainsi la possibilité à ses utilisateurs de pouvoir naviguer sur internet de manière anonyme et cryptée grâce à son navigateur (Tor browser) mais également d'héberger des sites web au sein de son réseau et ce, avec les mêmes attributs de sécurité et d'anonymat que pour la navigation. Constituant un sous réseau ou « *darknet* », c'est cet ensemble de sites « cachés » qui est souvent mentionné dans la sphère publique comme étant le repaire de ces pirates informatiques. Hors de portée des regards, de l'influence des algorithmes et du référencement web⁷, ce cyberspace inquiète tout autant qu'il fascine et fait ainsi l'objet de multiples spéculations de la part des médias. Or c'est dans cet espace numérique que se déploie selon nous ces pratiques et ces représentations encore trop méconnues. Car au-delà des analyses purement techniques ou judiciaires⁸, les sciences sociales peinent encore à étudier ces espaces numériques nouveaux.

Nous voulons ainsi entamer dans ce travail, à la fois un retour sur les travaux entrepris sur ce réseau, mais aussi une proposition de recherche pertinente pour comprendre un des aspects qui nous paraît parfois délaissé, mais pourtant fondamental, dans l'analyse de ces pratiques numériques. Nous prenons le parti d'appréhender ces pratiques hors des représentations communes, les considérant comme une activité purement déviante et principalement axée sur le commerce illégal,

4 http://www.lemonde.fr/technologies/article/2013/10/03/silk-road-ferme-et-alors_3488971_651865.html (Consulté le 24 Août 2017)

5 Données recueillies sur <https://metrics.torproject.org>, un site regroupant quelques données statistiques sur le réseau Tor. (Consulté le 24 Août 2017)

6 Émission France-inter du 12 Juin 2015 sur le darknet Tor. <https://www.franceinter.fr/emissions/>

7 cf. CARDON, Dominique (2015), *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Paris, Seuil, La République des idées.

8 cf. RUDESIL D, CAVAERLEE J & SUI D, (2015) "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box", Science Technology Innovation Program, Stip03, Wilson Center.

pour nous intéresser aux aspects plus organisationnels de ces espaces. **Nous voulons tenter de comprendre comment ces espaces reclus sont régis, organisés et comment peuvent-ils être le vecteur d'une forme de production et d'alimentation d'une branche de cette subculture hacker que sont les crackers du *darknet*.** Nous voulons nous concentrer sur le caractère collectif que peut adopter l'utilisation de certains services cachés de Tor, sur comment ces derniers peuvent être à la fois un support mais également un vecteur de valeurs et de normes liées à des communautés du réseau. Nous mêlerons donc réflexions sur le mode de gouvernance appliqué au sein d'un forum du réseau Tor, le «DeepNetwork⁹» ainsi que sur les modes interactionnels propres à ses membres. Nous essayerons de comprendre ces thèmes à travers les constructions et négociations collectives au contact d'autres membres, ainsi qu'à travers la structure même du site conçue pour réguler l'accès des utilisateurs à certains contenus en fonction de leur avancement dans la *carrière*¹⁰ d'utilisateur du forum. Ainsi, nous inscrirons notre réflexion dans la lignée des *cultural studies* mais aussi de la sociologie des usages et des pratiques numériques. Nous proposerons également une argumentation sur les dispositifs de pouvoir et de liberté négociés dans ce forum. C'est donc une réflexion sur les divers aspects culturels que peut véhiculer cette communauté et qui permet à cette dernière de se structurer et de perdurer.

9 Nom anonymisé

10 BECKER Howard (1985), *Outsiders, Etudes de sociologie de la déviance*, Paris, Métailié.

I / Contextualisation du sujet d'étude.

A) Du *hacker* au *cracker*, la mutation d'un mouvement.

Depuis une vingtaine d'année maintenant, les recherches universitaires ont publié outre-atlantique, un certain nombre de travaux concernant ces nouveaux collectifs que sont les *hackers*. De la mise en concept de ces groupes jusqu'à leurs évolutions, les chercheurs anglo-saxons ont eu l'opportunité de saisir ce mouvement dès sa naissance et jusqu'à son internationalisation dans les années 90. Ainsi dès 1984, le livre de Steven Levi « *hackers: Heroes of the Computer Revolution* » fut un des premiers à faire état de l'esprit de ces collectifs, de cette « éthique *hacker*¹¹ » dont internet a hérité. Au début des années 2000, alors que la diffusion du mouvement *hacker* s'opérait grâce à la massification d'internet, la sociologie a enfin pu se saisir des ces collectifs à travers cette « utopie technique ¹²» qu'était la leur.

Ainsi Patrice Flichy définissait en 2001 la contre culture *hacker* par un « sentiment collectif fondé sur la participation active à une communauté qui se structure autour de coutumes et de principes informels d'organisation sociale ». Cette structuration « informelle » dont il fait état se caractérise par le fait qu'elle ne soit pas imposée par les institutions de la société mais relève d'une forme de gestion autonome. Les travaux récents sur ces collectifs se sont ainsi vu prendre le prisme de cette autodétermination dans le travail au travers des différents tiers-lieux que sont les *hacker spaces*, fab labs et maker spaces. La multiplication de ces nouveaux lieux de construction et de partage de connaissances dans le monde a aidé à accroître une littérature universitaire longtemps peu abondante sur ce sujet. Différents domaines de recherches universitaires aussi variés que la gestion, le management ou la sociologie commencent aujourd'hui à s'intéresser à ces lieux où s'organise une nouvelle organisation du travail et s'exprime cette subculture *hacker*.

Michel Lallement analyse ces cyberespaces comme des lieux où s'élaborent non seulement « une nouvelle grammaire du travail », mais aussi « un autre mode de vivre ensemble » basés autour de valeurs directement héritées de l'éthique *hacker*. Ces collectifs de « bidouilleurs », moteurs de nouvelles innovations techniques et managériales semblent être revenus sur le devant de la scène

11 Déontologie qui prône entre autre la liberté d'accès aux informations mais aussi le jugement à l'aune du travail effectué et non des diplômes accumulés.

12 Patrice Flichy, « L'imaginaire D'Internet » Paris. La découverte, 2001

numérique. L'image positive qu'ils renvoient de la contre culture *hacker* au travers de l'image du « maker » a été pendant longtemps sujette à divers scissions et mésinterprétations qu'elles soient dans ou en dehors du mouvement.

En effet avec la massification d'internet et l'accroissement des « spams », « virus » et autres arnaques sur internet, la figure *hacker*, héros de la révolution micro-informatique des années 60-80 a fait place dans l'imaginaire collectif à l'image du « hooligan »¹³ du net. Associé au pirate informatique, cette représentation commune a permis d'alimenter cette ambiguïté entre *hacker* et cracker encore courante aujourd'hui.

Partageant des valeurs communes sur plusieurs aspects, ces deux figures emblématiques de la contre culture *hacker* ont dès le début été désignées sous la même appellation de « *hackers* ». Dans l'ouvrage emblématique de Steven Levi, John Draper, pirate de ligne téléphonique, est pleinement associé au mouvement *hacker* et encore aujourd'hui des crackers, se revendiquent comme *hackers*. Cependant cette ambiguïté dans l'inclusivité de cette appellation ne fait pas l'unanimité au sein du mouvement et certains *hackers* n'hésitent pas à afficher et à revendiquer leur appartenance à un « camp » spécifique et qui s'oppose à un autre camp rival comme par exemple : les *white hats* et les *black hats*. Les premiers se désignent comme des « trues » *hackers*, voulant faire partager au monde leurs compétences ainsi que leur idéal socio-technique et renvoient les « *black hats* » aux pirates informatiques profitant des failles des systèmes pour alimenter leurs propres intérêts. Cet élément classique de la construction identitaire collective : « nous versus eux », n'est pas sans rappeler les différents travaux sur les mouvements subculturels tels que ceux élaborés par Becker (1963) ou encore Prus (1997).

Cette distinction opérée par les acteurs au sein même de leur propre groupe a été analysée comme une mutation des mondes de *hackers* dans une période de fortes tensions (Éric Dagiral, 2008). Cette évolution est marquée par un désenchantement et l'entrée en résistance d'une partie du mouvement *hackers* est due à la multiplication des procès à l'encontre d'homologues tombés sous le coup de la justice. Ce « *hacker crackdown*¹⁴ » est selon Helen Nissenbaum bien plus une affaire de modifications contextuelles au sein du monde du numérique que des changements dans les « hacks ». En effet l'institutionnalisation, la centralisation et de la normalisation progressive d'internet qui vont à l'encontre de l'éthique *hacker*, ont créé au sein du mouvement *hacker* des sous

13 Expression tirée de l'article de Helen Nissenbaum « *hackers and the contested ontology of cyberspace* », *New Media and Society*, 2004, 6, p. 198.

14 Ainsi nommé par Bruce Sterling, auteur américain de science-fiction souvent inclus dans les listes d'auteurs du mouvement Cyberpunk.

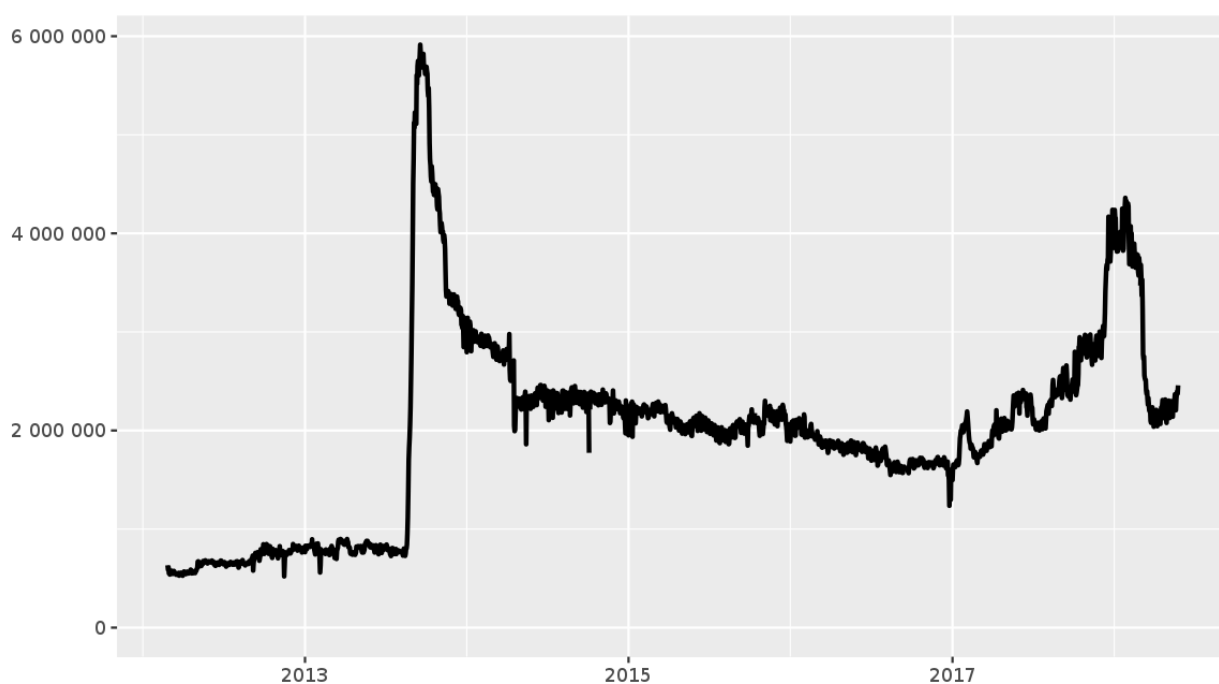
groupes d'affiliations (« white » et « black », mais aussi « grey » hats) se positionnant désormais par rapport au marqueur légal de leurs prouesses techniques.

Comme nous pouvons le voir, le monde des *hackers* est marqué par de multiples ramifications et appartenances qui traversent le mouvement depuis sa genèse.

La complexité de ce mouvement et la relative porosité des désignations peuvent laisser encore perplexes et plusieurs points sombres notamment sur les crackers « black hats », semblent demeurer. La littérature actuelle sur les mouvement hackers fait état de cette scission au sein du mouvement mais ne s'est concentrée que sur la partie la plus visible et accessible du mouvement, les « makers » (Lallement, 2015).

Malgré ces zones d'ombre, la figure du *hacktiviste* (pirate informatique revendiquant des causes politiques) rassemble un certain nombre de travaux qui tentent de cerner ce nouvel acteur contestataire contemporain. Par exemple, les actions du collectif Anonymous qui ont marqué les esprits par leurs piratages à visée politique, ont pu être analysés dans la littérature comme une « *totalisation dramaturgique* »¹⁵ d'un collectif d'appartenances et d'actions. C'est-à-dire que l'existence du mouvement passe par la mise en scène théâtralisée de leurs actions et de leur collectif. Mise en scène par la figure du citoyen-monde, anonyme et libre d'appartenance, le collectif Anonymus a surpris par la singularité de son modèle d'organisation totalement décentralisée et sans porte parole-désigné. Ce modèle de fonctionnement et cet attachement à l'anonymat est une composante très présente dans le mouvement hacktiviste et *cracker* de manière générale et se cristallise par l'adhésion au début des années 2000 aux *darknets*.

Directly connecting users



Évolution du nombre d'utilisateurs du réseau Tor entre 2012 et 2018

Ces espaces numériques anonymes et de « communication sans entrave » (Breton, 1990) sont devenus au fil des années des lieux de libertés soutenues par la composante la plus libertaire et la plus contestée du mouvement *hacker*. Par son caractère anonyme et dépourvu d'instances de contrôle, les *darknets* sont analysés comme étant des dispositifs techniques de pouvoirs et de libertés (Gehl, 2015) où les acteurs sont en constante négociation collective sur leur mode d'organisation, de recrutement ainsi que leur évolution dans le temps. Cet espace élitiste « à la disposition de ceux qui ont appris à naviguer » (Gehl, 2015), se démarque par un fort détachement des valeurs hégémoniques du « bien » du « mal » et n'hésitant pas à négocier ses propres règles indépendamment du cadre juridique. Sous un angle interactionniste, les *darknets* n'ont pas eu de répercussions dans le monde universitaire et l'angle pris dans les travaux que nous considérons comme les plus aboutis sur le sujet¹⁶ semblent faire l'impasse sur l'aspect de production et d'alimentation de savoir propres aux subcultures. En nous concentrant sur les revendications de ces *hackers* du *darknet*, nous entendons vouloir mettre en avant les formes d'adhésion à une subculture singulière issue du mouvement *hacker*.

En effet, les travaux sur les mouvements *hackers* semblent à la fois s'accorder sur le fait qu'il y ait une scission au sein du mouvement mais font en même temps l'impasse sur une partie non négligeable de ces groupes. Mais alors ne serait-t-il pas intéressant d'analyser le mouvement des *darknets* à l'aune des travaux sur les subcultures ? Quelle production culturelle s'exprime dans ces espaces si méconnus ?

16 Nous faisons surtout référence à l'article brillant de Robert W Gehl paru dans le journal « New Media & Society » en 2015.

B) - *Deepweb* / *Darknet* : mise à plat des termes.

Depuis quelques années et grâce à l'influence des médias de masse, les mots « *Deep web* », « *Darkweb* » et « *Darknet* » ont commencé à faire leur apparition dans l'espace public et ce, sans distinction claire de la part de ces médias. Qualifiant ces derniers de réseaux « obscurs »¹⁷ ou cachés, dans lesquels des personnes pouvaient naviguer et publier du contenu de manière anonyme et cryptée, les journalistes ne sont guère allés plus loin dans l'analyse de ce phénomène que celui de la déviance, de la criminalité et de la dissidence politique. Il suffit d'ailleurs de chercher quelques articles de grands journaux pour se rendre compte de la récurrence de certains mots-clefs faisant directement référence à ces sujets. C'est malheureusement au travers de ce discours majoritairement sensationnaliste qu'une partie du grand public a pris connaissance de l'existence de ces réseaux. D'abord cités pour la présence de criminalité et ensuite pour leur pouvoir de protection des libertés individuelles, ces réseaux restent encore incompris par la majorité de la population, faute de diffusion d'analyses sérieuses. Il convient alors, avant d'aller plus loin, de clarifier certaines confusions qui ont trait à l'appellation de ces réseaux numériques et ce pour plusieurs raisons. D'une part, cet éclaircissement permettra de mieux comprendre sur quel type de réseau se trouve notre groupe étudié et nous permettra ainsi de mieux comprendre dans quel cadre technique celle-ci se développe. L'environnement où se jouent les interactions influe sur ces dernières et, ignorer cet environnement, c'est commettre un biais sociologique évident. D'autre part, cette description permettra d'offrir un aperçu aux personnes qui ne sont pas particulièrement formées aux domaines des sciences humaines et de l'informatique et pour qui, ces réseaux restent encore méconnus.

L'appellation web profond ou « *deep web* » en anglais, a été popularisée par Michael K. Bergman au début des années 2000 dans un article¹⁸ où il expose les caractéristiques techniques de ce web profond et les raisons de la non indexation de ce contenu par les moteurs de recherches. Dans la définition de Michael K. Bergman, le *deep web* représente la partie de la toile accessible en ligne mais non indexable par les moteurs de recherches classiques. C'est à dire du contenu en ligne (sites entiers ou pages) accessible via la barre de recherche d'un navigateur web ou en passant de lien en lien mais qui reste introuvable en passant par les moteurs de recherche classiques et généralistes. En effet, la grande majorité des internautes ont prit l'habitude de naviguer sur internet en passant par

17 Terme recueilli dans la revue de presse « France 24 » : <http://www.france24.com/fr/20161101-2016-11-01-0720-revue-presse-francaise-migrants-calais-pauvrete-france-internet-cybercrimin> (Consulté le 24 Août 2017)

18 BERGMAN, M. K. (2000). "White Paper: The Deep Web: Surfacing Hidden Value". Journal of Electronic Publishing.

des moteurs de recherche et c'est à raison qu'on peut penser que la quasi-totalité du web y est indexée. La réalité en est tout autre puisque les moteurs de recherche, même les puissants, sont loin de pouvoir répertorier tout le contenu disponible sur la toile. Il est difficile d'en mesurer la taille mais dans les années 2000, le *deep web* a été estimé à 500 fois la taille du web indexé [Bergman, 2001]. Les raisons de cette non indexation sont nombreuses et peuvent être dues par exemple à :

- L'absence d'hyperliens dans le site.
- L'utilisation de balises spécifiques qui rendent difficile la compréhension de ces dernières par les robots d'indexation.
- La présence à la racine du site d'un fichier spécifique « robots.txt » excluant l'indexation de certains ou la totalité du contenu du site par les robots.

Ces dernières sont nombreuses et peuvent être volontaires ou non de la part des administrateurs. Il faut savoir aussi que pour certaines données, les algorithmes trouvent leurs limites et sont incapables d'indexer certains formats. Certains sites peuvent être aussi mal codés, abandonnés en cours de création ou n'ont tout simplement pas pour objectif d'être diffusés par leur créateur : ils peuvent par exemple faire office de pages personnelles dont seul le créateur ou un entourage restreint connaît l'adresse.

Un exemple parlant est celui du catalogue « Archipel » répertoriant les ouvrages des différentes bibliothèques du réseau Midi-Pyrénées. En effet, la page retournée à travers le formulaire de recherche de la plate-forme fait partie du *deep web*. Celle-ci est générée dynamiquement par l'interrogation d'une base de données et échappe aux moteurs de recherche. C'est pour cette raison qu'on ne peut pas trouver la localisation d'un ouvrage dans le réseau en interrogeant directement un moteur de recherche. Il est aussi important de rappeler qu'en l'absence de logiciels spécifiques de cryptage ou d'anonymisation (les VPN par exemple), la navigation sur un site du *deep web* n'est en aucun cas anonyme ; les individus se connectant à ces sites sont identifiables par leur adresse IP et le/les serveurs sur lesquels se trouve le site en question sont localisables sans difficulté particulière.

Les *darknets*, dont parlent le plus souvent les médias, sont quant à eux des sous-réseaux accessibles via des logiciels spécifiques et qui intègrent généralement des fonctions d'anonymisation à savoir « un ensemble de réseaux et de technologies utilisés pour partager du contenu numérique » (Biddle et al., 2002). Le web est composé d'une multitude de topologies de réseaux reliés entre eux (Étoile, bus etc.) et ces logiciels permettent de regrouper telle ou telle partie de ces ensembles en un sous-ensemble : un sous-réseau » (Rennard, 2016). Basiquement ce sont des

logiciels permettant de se connecter à un réseau volontairement isolé du reste de la toile. Ils peuvent servir au simple échange de fichier, comme des P2P privés mais peuvent aussi constituer un système complet - comme Tor - et héberger sites web, services de mails, de chats etc.

Les *darknets* sont donc des sous-réseaux accessibles par des logiciels spécifiques et qui sont volontairement cachés du web « classique ». Ils sont ainsi difficilement accessibles à travers les moteurs de recherche car leur création prévoit spécifiquement cette exclusion. Par exemple plusieurs entreprises sont dotées d'un *darknet* pour garantir l'anonymat de leurs données et éviter l'espionnage industriel ou encore, de nombreux journalistes d'investigation utilisent des *darknet* pour protéger leurs sources contre d'éventuelles représailles. Il n'y a donc pas à proprement parler d'un *darknet* mais des *darknets*. Certains comme Tor, sont mondialement connus et rassemblent des millions d'utilisateurs alors que d'autres réunissent des communautés plus modestes comme I2P ou Freenet. Le seul point commun entre tous ces *darknets* est le souci de la préservation de l'anonymat. « Socialement, le *darknet* s'incarne dans la quête de l'anonymat et de la confidentialité. C'est elle qui marque sa spécificité, c'est l'usage social d'instruments techniques qui fait particularité »¹⁹.

Nous étudierons dans notre sujet une population présente sur le *darknet* le plus populaire aujourd'hui : le réseau Tor, à savoir un écosystème indépendant et intégrant des outils d'anonymisation de ses utilisateurs. Par opposition on parlera de *Clearnet* pour qualifier l'internet classique, ouvert à tou-tes-s et accessible sans savoir-faire ou logiciels spécifiques.

C) Le réseau Tor, une grande couverture médiatique mais de faibles répercussions universitaires.

Dû au caractère trop récent du phénomène, le réseau Tor a jusqu'aujourd'hui du mal à gagner en légitimité auprès des sciences sociales. Souvent connu pour ces « marchés de la drogue »²⁰, les médias de masse qui ont contribué à véhiculer un sentiment de méfiance par rapport aux « services cachés » de Tor, ont paradoxalement diffusé un certain désintérêt quant aux communautés qui y sont présentes. L'activité numérique au sein de ces sites y est souvent vue comme suspecte si ce n'est purement déviante et ces utilisateurs, du moins occidentaux, soit comme des « geeks » ou de potentiels criminels²¹. Souvent axées sur l'aspect politique ou déviant, les premières recherches à

19 RENNARD, Jean-Philippe (2016) , *Darknet mythes et réalités*, Paris, Ellipses, p.11.

20 <http://www.latribune.fr/technos-medias/internet/le-marche-de-la-droque-en-ligne-se-porte-bien-591879.html> (Consulté le 23 Août 2017).

21 Marianne, avril 2013, marianne.net/societe/plongee-dans-les-entrailles-de-linternet-criminel (consulté le 16 Mars 2017)

avoir étudié le phénomène sont, comme nous le verrons par la suite, souvent d'ordre juridique ou technique et délaissent l'aspect social sous-jacent.

En parcourant la littérature autour du sujet, on découvre qu'il est souvent fait mention du degré de dangerosité de ce type de service (D. Sui, J. Caverlee, D. Rudesill 2015), de la localisation des services cachés sur le réseau (Øverlier/ Syverson, 2006) ou encore du degré d'anonymisation (González, 2013) de ces services. Par exemple, des recherches constatent que la prolifération de ces marchés présents sur le réseau Tor est une manifestation d'un commerce de plus en plus complexe, transnationalisé et lucratif. Par conséquent, le système juridique étasunien et les traités sur lesquels ils se fondent sont dans l'incapacité actuelle de répondre à l'encadrement juridique de ces pratiques (Julia Buxton, Tim Bingham, 2015). Si en effet les capacités d'anonymisation du réseau, la présence de criminalité ainsi que les efforts déployés par ces utilisateurs pour garantir la non traçabilité de leurs échanges représentent un défi majeur pour ces disciplines, cette même focalisation délaisse ce qui pour nous paraît essentiel dans ce phénomène, à savoir, l'aspect communautaire et donc social que produit ce nouveau réseau. D'autres recherches tentent, quant à elles, d'apporter un éclairage sur la structure et les pratiques qui ont cours dans ce réseau.

L'interface d'utilisation de Tor est ainsi vue comme un retour à l'internet des années 1990 : un média nouveau créé et utilisé par un nombre restreint de personnes, notamment des passionnés et dans lequel ils peuvent jouir d'un certain nombre de libertés permises par le manque de cadre légal (Papsdorf, 2016). Cet espace numérique est donc décrit comme un espace permissif où une certaine culture de l'open source peut s'exprimer. Les services utilisés dans ces réseaux sont décrits comme des transpositions de services déjà présents sur le web de surface mais avec des bases différentes, notamment celles de l'anonymat. Allant des logiciels de *chat* comme « cryptocat » au partage de fichiers comme « onionshare », les développeurs et utilisateurs s'attachent à suivre un « cahier des charges » cohérent avec une base idéologique qui privilégie l'anonymat et la sécurité (Rennard, 2016). Il y a donc un attrait de certains utilisateurs, inquiets des programmes de surveillance étatique comme PRISM et la marchandisation des données privées par des grandes firmes multimédias (Google, Amazon, Facebook) vers ces réseaux. (Papsdorf, 2016).

Suivant cette base, on pourrait être tenté de trouver des caractéristiques communes aux *hackers* décrits par Pekka Himanen dans son ouvrage «L'éthique *hacker* et l'esprit à l'ère de l'information» paru en 2001 où, «la liberté d'expression et le respect des données personnelles constituent des principes essentiels» (p.94). L'étude des communautés à l'intérieur de ces réseaux en est encore à ses débuts, mais certains auteurs se sont efforcés d'approcher le phénomène grâce à une méthodologie

adaptée à la situation, à savoir celle de l'ethnographie en ligne. Robert Gehl s'est entre autre attaché à analyser le mode de gouvernance d'un réseau social sur un *darknet*. Il expose dans sa recherche trois grandes pratiques diffusées dans le forum par les membres et les modérateurs du site, à savoir : la culture de l'anonymat, la prohibition de la pédopornographie et la production d'un élitisme technologique. Son étude révèle ainsi que ce forum « (...) -comme toute forme alternative de réseau social - doit être une expérimentation d'un modèle de gestion basée sur la tension exercée entre exercice du pouvoir et respect des libertés » (Gehl, 2014). Ce qu'expose l'auteur dans sa recherche, c'est une certaine contradiction structurant cette communauté dans ses agissements. Une négociation permanente entre les membres sur l'organisation du groupe. Le fait que la communauté défende l'anonymat et la liberté d'expression en même temps qu'elle soit consciente qu'il y a, au sein du site, une centralisation des informations et des droits de modération coercitifs et omniscients, amène une forme d'organisation qui, par son ambivalence, la rend extrêmement instructive sociologiquement.

L'auteur montre par conséquent que le rapport pouvoirs/libertés au sein de la communauté est réciproque et incompatible. C'est-à-dire que l'un ne va pas sans l'autre mais les deux se repoussent mutuellement; donnant ainsi lieu à des formes de négociation entre les utilisateurs sur:

- La place et le rôle de la communauté sur internet,
- Son degré d'accessibilité pour les nouveaux utilisateurs et enfin,
- La manière de gérer collectivement certaines pratiques prohibées, notamment celle de la présence ou non de pédopornographie à l'intérieur et à l'extérieure du site.

Parmi les pratiques diffusées par la communauté étudiée, l'auteur fait apparaître ce qu'il appelle un élitisme technologique : une forme de sélection sociale qui se base sur la capacité des individus au sein de la communauté à incorporer et utiliser un certain nombre d'outils informatiques inhérents au *darknet*.

Hormis les travaux de Robert Gehl que nous venons de citer précédemment, la portée sociologique des études en sciences sociales évoluant autour du sujet des *darknets* et des communautés les composants est selon nous encore à l'état exploratoire et a du mal à percer la sphère universitaire de manière pérenne.

D) L'étude des subcultures au prisme de l'interactionnisme symbolique.

Nous voulons dans cette partie exposer le cadre interactionniste sur lequel nous voulons baser notre analyse de la subculture des *darknets*.

De manière élargie, l'interactionnisme symbolique peut être compris comme l'étude de la manière dont « *Les humains agissent à l'égard des choses et en fonction du sens que ces choses ont pour eux.* » (Blumer). En effet, en partant de ce postulat théorique on peut retenir l'idée partagée par les interactionnistes que l'accomplissement de la vie en groupe doit être considérée comme un processus à la fois subjectif et intersubjectif où les individus développent des significations sur les objets par interactions avec leur groupe d'appartenance. Ces significations ainsi que les actions qui en découlent sont mouvantes dans le temps et leur évolution peuvent être conséquence de la transformation du groupe dans son ensemble. Ainsi comme le décrit Blumer sur le sens donné aux objets :

1. *Ce sens est dérivé ou provient des interactions de chacun avec autrui.*
2. *C'est dans un processus d'interprétation mis en œuvre par chacun dans le traitement des objets rencontrés que ce sens est manipulé et modifié*

Que ce soit dans l'analyse d'un groupe d'individus « *in real life* » ou sur internet, l'interactionnisme symbolique exige que le chercheur soit attentif à la manière avec laquelle les individus du groupe étudié partagent avec les autres membres le sens donné, à la fois aux objets, mais aussi aux situations que les membres traversent. Ainsi plutôt que d'analyser les comportements individuels à l'aune des seuls facteurs externes, les interactionnistes insistent sur la capacité qu'a un groupe de structurer un modèle de pensée global au niveau individuel. De plus, selon Blumer, la réalité est non seulement une construction sociale mais a aussi un « *caractère résistant* » (*obdurate character of reality*)²². C'est à dire que « *si les acteurs construisent leurs actions à travers un processus continu de définitions et d'interprétations, la réalité peut agir sur eux indépendamment de cette définition*

²² T. J. Morrione, "Persistence and change: Fundamental elements in Herbert Blumer's metatheoretical perspective", in Luigi Tomasi (dir.), *The Tradition of the Chicago School*, Ashgate, Aldershot, 1998, pp. 191-216.

de la situation. »²³.

Malgré l'adhésion mitigée de certains chercheurs aux théories interactionnistes en France, Howard Becker s'est positionné depuis les années 1980 comme porte-flambeau de l'analyse des mouvements déviants et notamment subculturels. L'apport majeur de son ouvrage « Outsiders » sur la théorisation ainsi que la compréhension des groupes déviants est aujourd'hui un classique pour celles et ceux voulant aborder ce sujet. Ainsi, pour ce travail sur l'analyse des *darknets*, il nous paraît évident que la définition des groupes déviants, tels qu'ils ont été théorisés par Becker sera d'un apport majeur pour positionner notre recherche. Ainsi, le préambule à la définition de cette dernière est selon l'auteur que ; l'acte déviant n'est en aucun cas immuable mais c'est la société qui définit ce qui est effectivement déviant de ce qui ne l'est pas. C'est donc une construction sociale ayant un caractère arbitraire et qui est mouvante dans le temps.

Étiquetage // Comportement	Obéissance à la norme	Transgression de la norme
Individus perçu comme déviant	Accusé à tort	Pleinement déviant
Individus perçu comme non déviant	Non déviant	Secrètement déviant

Pour les internautes des *darknets*, l'étiquetage de la déviance est assez majoritairement appliqué à ces groupes. Que l'acte déviant soit effectif ou non par les individus, c'est le contenu des *darknets* qui est majoritairement associé à la déviance (criminalité, pédopornographie, *cracking* etc.). Ainsi, naviguer sur un *darknet* en explorant son contenu ou faire partie d'un groupe d'internautes devient rapidement un motif d'affiliation à la déviance pour des individus exogènes.

Comme nous avons pu l'observer dans nos précédents écrits²⁴, l'analyse d'une communauté virtuelle sur le *darknet* a révélé un agencement pyramidal du groupe d'internautes. Différents rangs

23 Lionel Lacaze, « L'interactionnisme symbolique de Blumer revisité », Sociétés 2013/3 (n° 121), p. 41-52.

24 Rihani K. « Structuration et organisation d'une communauté virtuelle sur le réseau Tor » 2017

sont établis et hiérarchisés les uns par rapports aux autres et l'acquisition de ces rangs se fait sous des critères de participation à la vie de la communauté. Ainsi la contribution aux posts du forum, l'intégration et la mise en application des règles ainsi que la publication de contenus pertinents font partie d'une démarche au cœur du fonctionnement de la communauté. L'élitisme technologique, basé sur la capacité des internautes à intégrer et à restituer avec pertinence un capital informationnel -ou comme nous le verrons plus tard, un « capital subculturel »- met un évidence un concept essentiel dans l'œuvre de Becker avec lequel nous pouvons faire un parallèle dans notre travail : le concept de « carrière ». Ce dernier, transposé de l'étude des professions à l'analyse de la déviance peut s'appliquer dans le contexte de notre subculture : autant dans la démarche d'évolution dans la pyramide sociale de la communauté que dans l'élaboration d'une carrière déviante au sein de cette dernière.

Pour reprendre les mots de l'auteur et étayer les nôtres :

[à propos de la notion de carrière] « Cette notion désigne les facteurs dont dépend la mobilité d'une position à une autre, c'est-à-dire aussi bien les faits objectifs relevant de la structure sociale que les changements dans les perspectives, les motivations et les désirs de l'individu (...) on peut aussi l'utiliser pour distinguer divers types d'aboutissement des carrières, indépendamment de la question de la « réussite ». » P47

Cette citation met selon nous en avant les caractéristiques dynamiques que sous-tend la notion de carrière selon Becker. Cette dernière pouvant selon nous s'appliquer autant de manière synchrone qu'asynchrone à la déviance. En d'autres termes, un internaute peut mettre en place une carrière « simple » au sein de la communauté pour acquérir un statut, c'est-à-dire en agissant de manière conforme et en appliquant les exigences de la communauté comme une carrière « double », en choisissant de la coupler avec une carrière pleinement déviante, en se spécialisant dans la cybercriminalité par exemple.

D.1) Subculture transnationale et « groupculture » local.

L'étude des subculture est un sujet vaste auquel différentes approches peuvent être choisies en fonction du contexte d'application de cette dernière. Plusieurs auteurs ont ainsi intégré à leur analyse des mouvements subculturels, un angle situationnel pour mieux différencier le spectre des subcultures présentes. Le sociologue américain Robert Prus expose par exemple dans son ouvrage

« Subcultural mosaics and intersubjective realities » différentes échelles d'analyses pour contextualiser une subculture. Les distinctions que Prus établit entre subcultures transnationales et locales sont particulièrement intéressantes pour nous. Il affirme ainsi qu'il existe «un assortiment infini de contextes (et de niveaux) dans lesquels le concept de subculture peut être appliqué» (p43). Au risque de biaiser l'analyse, l'identification de l'échelle et du contexte d'application de la subculture se doit en effet d'être saisie avec justesse. D'autres chercheurs comme Fine (1987) et Gordon (1970) ont utilisés les termes *idiosubculture* et *groupculture* pour distinguer des plus petits segments d'une subculture « dominante ». Ces petits segments, dans lesquels une culture de groupe est créée, partagée entre individus qui se connaissent et revendiquent par ses pratiques une appartenance à un mouvement subculturel plus vaste. Ainsi le terme subculture est réservé pour décrire les unités sociales plus larges à travers lesquelles des plus petits groupes s'agglomèrent et font perdurer une culture plus large. A l'échelle d'une subculture transnationale (Prus, 1997) due à l'éclatement géographique des différents groupes qui la composent, les membres ne peuvent interagir directement les uns avec les autres, mais partagent au sein de chaque unité locale, une culture commune avec les autres groupes. A partir de cette idée, ces auteurs proposent ainsi un ensemble de définitions que les chercheurs doivent appliquer aux différents contextes ou niveaux d'analyse d'une subculture pour mieux en saisir la portée.

La subculture *darknet* correspondrait ainsi à ce que Prus (1997) décrit comme étant une subculture transnationale où l'espace géographique due au fait que la subculture est numérique, n'interfère que peu dans l'idéologie globale de chaque sous-groupe. Ces derniers partageant un imaginaire et des règles communes aux différents groupes de *hackers* du *darknet*, ils permettraient de faire perdurer un modèle organisationnel au-delà des frontières géographiques et linguistiques. Par leur capacité à partager des règles communes telles que la liberté de reproduction et de diffusion du savoir *l'open source*, la culture de l'entraide ou encore cette « *hacker attitude* » qui établit une vision du modèle social post-industriel (Hinamen, 2001), différentes communautés des *darknets* font perdurer un modèle de fonctionnement à travers la subculture qu'ils incarnent. Comme le précise Prus (1997), il n'est pas nécessaire dans une subculture transnationale que les membres interagissent en face-à-face ni que ces derniers connaissent l'existence de chaque sous-groupe pour que perdure cette subculture :

« Bien que subordonnée à cette dernière, la communication dans une subculture ne se limite pas à l'interaction en face-à-face, ni aux interactions directes entre tous les

membres de la subculture. Ainsi, alors qu'un grand nombre de subcultures sont construites directement sur des interactions en face-à-face, il n'est pas nécessaire que les personnes impliquées dans une subculture (transnationale) résident dans le même cadre géographique ou même connaissent l'existence l'un de l'autre. (page 41)

Les sous-groupes d'une subculture, ou *groupculture* selon Gordon (1970), agissent de manière autonomes les uns des autres et peuvent être identifiés comme relevant de l'exercice d'une subculture à une échelle locale. Si nous appliquons cette échelle d'analyse à notre propre terrain d'enquête, nous nous rendons compte que l'étude de la subculture *darknet* correspond tout à fait à ce que Prus (1997) et Gordon (1970) ont établi. La subculture *darknet* incarnerait cette échelle transnationale et les sous-groupes qui composent le réseau (telle que la communauté du forum que nous étudions) incarnerait quant à eux cette échelle locale que sont les *groupcultures*. Nous verrons dans la suite du mémoire comment le groupe d'internautes que nous étudions, incarne parfaitement ce partage de valeurs et de normes propres à la subculture *darknet*.

D.2) Interactions en ligne : « on the internet nobody knows you're a dog ».

The Joy of Tech™



© 2013 Geek Culture

by Nitrozac & Snaggy



joyoftech.com

Les réactions communes face aux mouvements et aux communautés en ligne tendent souvent à mettre l'accent sur l'absence de face-à-face dans les interactions et de fait, leurs capacités à créer des relations complexes par-delà cette dernière contrainte (Gelder, 2007). En effet même si les identités ne sont pas toujours ce qu'elles semblent être sur internet, des internautes participent à des communautés (parfois anonymes) où au fil des conversations, des relations de proximité affective se créent. Ainsi les visages et les prénoms s'effacent au profit de simples pseudonymes. Ces derniers deviennent l'élément central d'identification d'une personne sur un ou plusieurs sites web différents. Ainsi le pseudonyme se suffit à lui-même pour construire et alimenter des relations en ligne. Évidemment le propos ici n'est pas de débattre de ce fait mais de poser cette dernière affirmation comme un élément constitutif et indispensable à la participation à une communauté sur le *darknet* qui est totalement numérique et anonyme. Les travaux d'Hervin Goffman sur les types d'interactions et notamment son approche dramaturgique de ces dernières, ont certainement suscité un certain malentendu par son attention exclusive aux relations face-à-face²⁵. Loin de cela, nous pensons que l'interaction doit être pensée comme un processus social et un acte collectif qui dépasse la frontière du face-à-face. A titre d'exemple, les stratégies inter-individuelles, afin de ne pas « perdre la face » peuvent selon nous aisément s'appliquer dans un cadre d'interactions en ligne lors d'un débat houleux ou d'une tentative de trollage²⁶. Ainsi la focale théorique interactionniste pour analyser les subcultures en ligne s'applique avec pertinence dans un cadre autre que le strict face-à-face où internet devient le cadre d'interactions privilégiées.

En effet si certaines subcultures, comme celles des mouvements gothiques Londoniens²⁷ par exemple, utilisent internet pour échanger et communiquer, ce dernier reste un média au sens propre, et les sociabilités s'étendent hors-lignes lors d'événements rassembleurs tels que les concerts ou autres rassemblements festifs. Pour les *darknets*, et comme nous le verrons par la suite, la socialisation se fait et reste majoritairement en ligne. Internet ne sert pas seulement d'outil, de lien entre les individus pour un futur face-à-face éventuel, mais agit comme un cyberspace au sens propre, où « tout s'y fait » à l'intérieur.

25 Lacaze, Lionel. « L'interactionnisme symbolique de Blumer revisité », *Sociétés*, vol. 121, no. 3, 2013, pp. 41-52.

26 Le trollage est une technique consistant à empêcher le bon fonctionnement d'un forum de discussion sur Internet en parlant de sujets provocateurs qui n'ont rien à voir ou en éditant des centaines de messages à la suite pour stopper la discussion.

27 Paul Hadkinson, « Goth : Identity, Style and subculture ». 2002

« Parce que l'interaction par définition n'est pas une activité solitaire, une idée de la conduite humaine centrée sur cette idée ne se focalise pas sur des actes isolés d'individus mais sur le développement de l'action collective, sur la façon dont les gens agissent ensembles pour créer une activité qui devient quelque chose à quoi ils ont tous contribué » Lacaze (2013)

Recueillir des échanges dans un contexte exclusivement en ligne peut sembler être contraint à faire face à un manque de sincérité dans les propos. Perdre la communication non verbale peut ainsi apparaître comme un obstacle supplémentaire à une analyse qui s'étendrait par-delà les strictes paroles des enquêté-e-s. Or, les recherches effectuées dans le domaine des sociabilités numériques et des mondes en ligne (Boellstorff, 2013) ont démontré que les individus passaient une partie non négligeable de leur temps à créer et alimenter de nouvelles relations mais aussi à partager des idées, du savoir et plus généralement de la culture au sens étendu du terme. Les internautes crée-e-s des amitiés en lignes et montrent souvent beaucoup de complicité avec leurs homologues. L'immédiateté d'internet permet à ces derniers de passer d'un contenu à un autre comme ils peuvent passer d'une conversation à une autre de manière simultanée et sans pour autant perdre l'authenticité des interactions. Par exemple, l'anonymat offert par internet permet à celles et ceux qui seraient trop timides, d'engager des conversations de manière moins contraignante. Au delà de cet aspect le sens de l'anonymat permet une discussion plus ouverte sur des activités qui peuvent être considérées par les étrangers comme déviantes et soumises à certaines formes de sanctions morales. Du point de vue du chercheur, l'intérêt de l'ethnographie en ligne réside dans cet aspect émancipateur de l'absence de face-à-face. L'intérêt est que les enquêté-e-s se sentent aussi à l'aise que possible pour discuter de tous les domaines d'activité, expériences et perspectives (déviantes ou non) qui les intéressent. (Kleinknecht, 2003)

II) Définition et analyse d'une subculture en ligne.

En poursuivant nos recherches sur les modes d'organisation d'une subculture, son historique ainsi que son contexte d'émergence, nous sommes arrivés au point où la mise en place d'une typologie est devenue nécessaire pour poursuivre à bien notre travail. L'importance de formaliser et de comprendre les caractéristiques communes des subcultures vont nous permettre par la suite de mettre en perspective notre propre groupe d'enquête-s-es et de l'analyser à l'aune de cette dernière.

Nous nous sommes pour ce travail inspirés de la thèse du sociologue Kleinknecht sur laquelle ce dernier a travaillé à définir et à comprendre une subculture *hacker* au travers d'une ethnographie. Nous avons emprunté et traduit de ses écrits sa présentation des éléments caractéristiques des subcultures. La pertinence de ces éléments communs donnent selon nous une appréciation plus complète des éléments d'une culture communautaire. Sans y être strictement réduite pour autant, la lecture de ces derniers doit s'accomplir en envisageant chaque élément comme étant lié au suivant et s'assemblant pour former un tout interconnecté, ce qui entraîne -selon l'auteur- la formation d'une subculture (p.33). Voici les spécificités qu'il présente:

- (1) **L'Idéologie** - La façon dont un groupe voit et donne du sens au monde qui l'entoure. Cette vision du monde justifie l'existence du groupe, de ses valeurs ainsi que de ses croyances.
- (2) **Les routines** - Un ensemble commun de valeurs et d'usages qui sont transmis par les initiés aux nouveaux. Cet ensemble est propre à la subculture et diffère des interprétations extérieures.
- (3) **L'argot** - Des mots et un langage distinctif de la subculture et dont le sens, l'interprétation et la compréhension, peuvent différer pour des personnes extérieures au groupe.
- (4) **Les normes** - Règles de comportements et d'attentes de conduite au sein du groupe et présentes sous deux formes : formelles et informelles. Ces règles servent à la gouvernance et à l'organisation du groupe.
- (5) **Les artefacts** - Objets (matériels ou immatériels) dont le caractère symbolique peut renvoyer à un événement historique marquant du groupe ou un élément central de leur activité . Leur importance et leur signification est transmise par les initiés et agissent comme un élément d'identification pour les personnes appartenant au groupe.

(6) **L'identité** - Définitions des membres de la subculture tournant autour de la façon dont les individus dans le groupe se voient et comment ils pensent que les étrangers les voient.

Dans les chapitres suivants, les concepts **d'idéologie**, **d'argot** ainsi que de **normes** seront explorés plus en profondeur et appliqués directement dans l'analyse de la subculture *darknet*.

Le choix de prendre, dans cette partie, cette classification au détriment d'une autre – nous pensons notamment à celle de Dick Hebdige (1979) - est due au fait que la typologie de Kleinknecht se veut plus ciblée et mieux appropriée à notre enquête sur le *darknet* que ne l'est celle de Gelder. Sans pour autant être contradictoires, les différents points que ce dernier aborde s'appliquent davantage à un contexte « in real life » qu'un contexte strict de sociabilité numérique. Nous conseillons tout de même la lecture (ou la relecture) de son ouvrage « *Subculture, the Meaning of Style* » car il permet d'avoir une vision complémentaire de ce qu'implique la participation à des mouvements subculturels, notamment en terme de subversion et d'apposition à une culture vue comme dominante.

A) Mise en place de la méthodologie d'enquête : du recueil de données à l'analyse des pratiques et des représentations.

En sociologie, l'étude compréhensive d'une communauté en ligne impose d'opter pour un certain nombre de cadres et de choix méthodologiques. Qu'ils soient traditionnels, c'est-à-dire s'inscrivant dans la lignée de la discipline anthropologique ou s'en éloignant, ces derniers doivent se plier au contexte et à l'environnement sur lequel s'exercent les pratiques des communautés étudiées (Berry, 2012). Elles doivent donc se montrer pertinentes et justifiées. Dans notre cas, le recueil de données est un passage crucial sur lequel nous ne pouvons faire l'impasse et sur lequel nous nous efforcerons de poser notre problématique. D'une part, ce travail de recueil aura pour but de tester et d'ajuster nos questionnements mais surtout, ce corpus de données s'établira comme un support sur lequel baser notre analyse de terrain. Nous nous efforcerons donc dans cette partie, d'explicitier nos choix méthodologiques dans la perspective de soulever notre future problématique.

B) L'observation non participante et le recueil de données.

« *Lurk more, it's never enough* »

Dans le travail précédent de Master I, nous avons amorcé une démarche ethnographique qui visait à mieux connaître le terrain étudié. Comme d'autres avant nous, et par prudence, nous avons pris « une position d'observateur, de « *lurker* » (Berry, 2012) afin de recueillir un maximum d'informations et ce, sans prendre le risque de fragiliser notre position de chercheur due à une participation précipitée et maladroite.

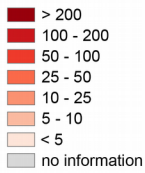
Ce travail de recherche s'inscrivant sur les deux années du cursus de master, nous pensons que la prudence avec laquelle nous avons abordé notre méthodologie d'enquête l'année précédente, pourra constituer un gain précieux cette année quant à la compréhension des modes d'interactions de notre groupe étudié. Comme pour l'analyse de certains phénomènes extrêmes ou déviants, nous pensons que cette étude préalable et à laquelle nous nous sommes attachés durant ces deux années était la seule viable pour aboutir à une étude rigoureuse et approfondie du phénomène des *darknets*. Ce sont donc des dizaines d'heures de lecture de *topics* tels que « Règles », « Guide du débutant » ou encore « Centralisation de liens utiles » pour tenter de comprendre les lignes de conduite et les informations importantes pour pouvoir mieux développer notre recherche. L'utilisation de méthodes de chiffrement des conversations ainsi que les règles de sécurité à adopter dans ces espaces numériques sont quelques exemples de démarches entreprises à la suite de ces lectures. Nous avons ainsi entrepris au gré de ces observations, de recueillir via des captures d'écran, toutes les informations utiles concernant la structure du site et les interactions entre ses membres. Celles-ci regroupent par exemple le visuel du site, les règles affichées, les différentes thématiques du site, les sanctions des modérateurs ainsi que les conflits entre les membres sur différents sujets. Cette utilisation de captures d'écran a été essentielle dans notre démarche car elle permet d'une part de centraliser et classer les matériaux en fonction de thématiques choisies et d'autre part de prendre le temps d'assimiler les règles du forum ; règles formelles tout d'abord, via la lecture des sections prévues à cet effet, et informelles ensuite via la relecture des conversations dans les *topics* du forum. Cette rigueur que nous nous sommes imposée dans cette recherche s'inscrit donc dans une lignée anthropologique : Explorer et tenter de comprendre le social, « à la manière d'un ethnographe qui autrefois arpenterait de lointaines contrées muni de son carnet de notes (...) » (Trémel, 2003, p. 167).

Nous attachons dans ce travail une attention toute particulière à l'observation du cadre numérique dans lequel se déroulent les interactions de cette communauté. S'attacher à ne pas délaissier le cadre d'un environnement virtuel pour se focaliser uniquement sur ce qui s'y déroule. Nous définissons ici par cadre, l'architecture du site, ses contours et limites mais aussi les droits inégalement répartis entre les utilisateurs. Ces points importants qui œuvrent entre autre à la définition des règles d'interactions des membres du forum. Cette démarche s'attache à décrire ce qu'induit l'environnement du site de l'utilisation qui en est faite. Qu'il soit « virtuel » ou « réel », nous pensons qu'un environnement ne peut être neutre et conditionne l'action des individus, d'où l'importance d'y attacher son regard. Ce « cadre » délimiteur que nous voulons analyser peut ainsi prédisposer les utilisateurs à un usage particulier. Ces prédispositions peuvent prendre plusieurs formes qui peuvent aller, de la prise de parole jusqu'à la construction d'une identité virtuelle plus au moins élargie en passant par l'élaboration d'une carrière au sein de leur communauté.

La première problématique à laquelle nous avons été confrontés durant ces deux mémoires de master était de ne pouvoir obtenir de données chiffrées quant aux caractéristiques de composition du réseau Tor. En effet au-delà de la répartition géographique des utilisateurs du réseau, aucune autres données pertinente n'étaient disponible pour tenter de classer ou d'objectiver les conditions et les pratiques ayant cours sur ce dernier. Ainsi, tenter d'élaborer et de présenter un échantillon représentatif des acteurs aurait été une manœuvre impossible à mener. Ce réseau étant conçu spécifiquement pour permettre une telle opacité, cette tentative de classement aurait été aussi imprécise qu'infructueuse. Malgré cela nous nous sommes efforcés de partager dans ce travail les données les données démographiques disponibles sur le réseau Tor.

The anonymous Internet

Daily Tor users per 100,000 Internet users



Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

 Oxford Internet Institute
University of Oxford

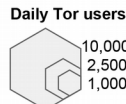
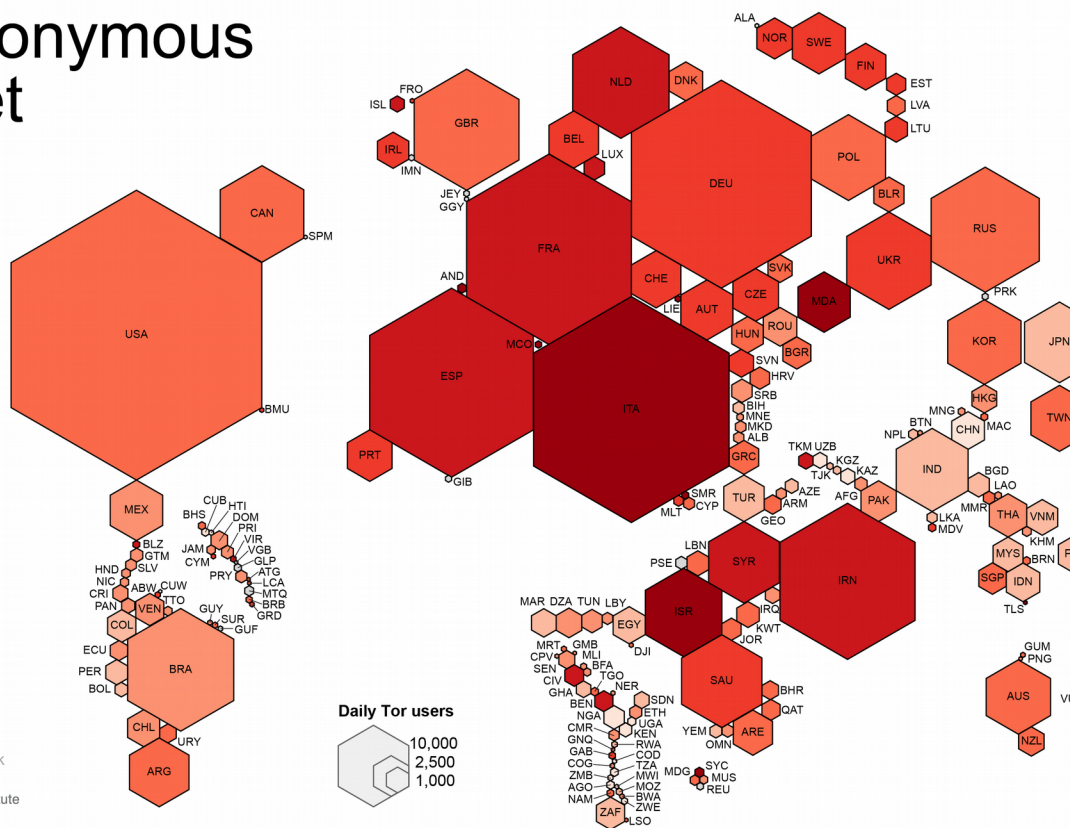


Illustration 1: Répartition mondiale des utilisateurs du darknet Tor pour 100 000 connexions entre 2012 et 2013

Répartition du nombre de connexions journalières de 2015 à 2018 pour les dix plus grand pays utilisateurs du réseau Tor.

Pays	Nombre d'utilisateurs
États-Unis	391771 (18.01 %)
Allemagne	295041 (13.56 %)
Russie	219275 (10.08 %)
Émirats arabes unis	148926 (6.85 %)

France	113040 (5.20 %)
Ukraine	78494 (3.61 %)
Royaume Unis	77219 (3.55 %)
Pays bas	53185 (2.44 %)
Italie	43918 (2.02 %)
Brésil	42841 (1.97 %)

Source : <https://metrics.torproject.org>

Malgré la prédominance des États-Unis en nombre de connexions journalières, la France se situe en cinquième position avec 113040 connexions par jour au réseau Tor et totalise 5.20% du total des connexions mondiales. Ajusté à la démographie de chaque pays, les Émirats arabes unis, avec une population de 9,5 millions d'habitants en 2018²⁸ passeraient en première position en pourcentage de leur population connectée au réseau Tor avec 1,5 % . Les États Unis eux, seraient à 0,12 % de leur population connectée au réseau Tor alors que la France, quant à elle aurait 0,16 % de sa population connectée tous les jours à Tor. Les données concernant l'âge, le genre ou encore la profession des utilisateurs du *darknet* Tor sont inexistantes et à moins d'une étude quantitative de très grande envergure, ces données seront difficilement disponibles un jour.

C) Ethnographie numérique: le cas du forum « DeepNetwork » sur le *darknet* Tor.

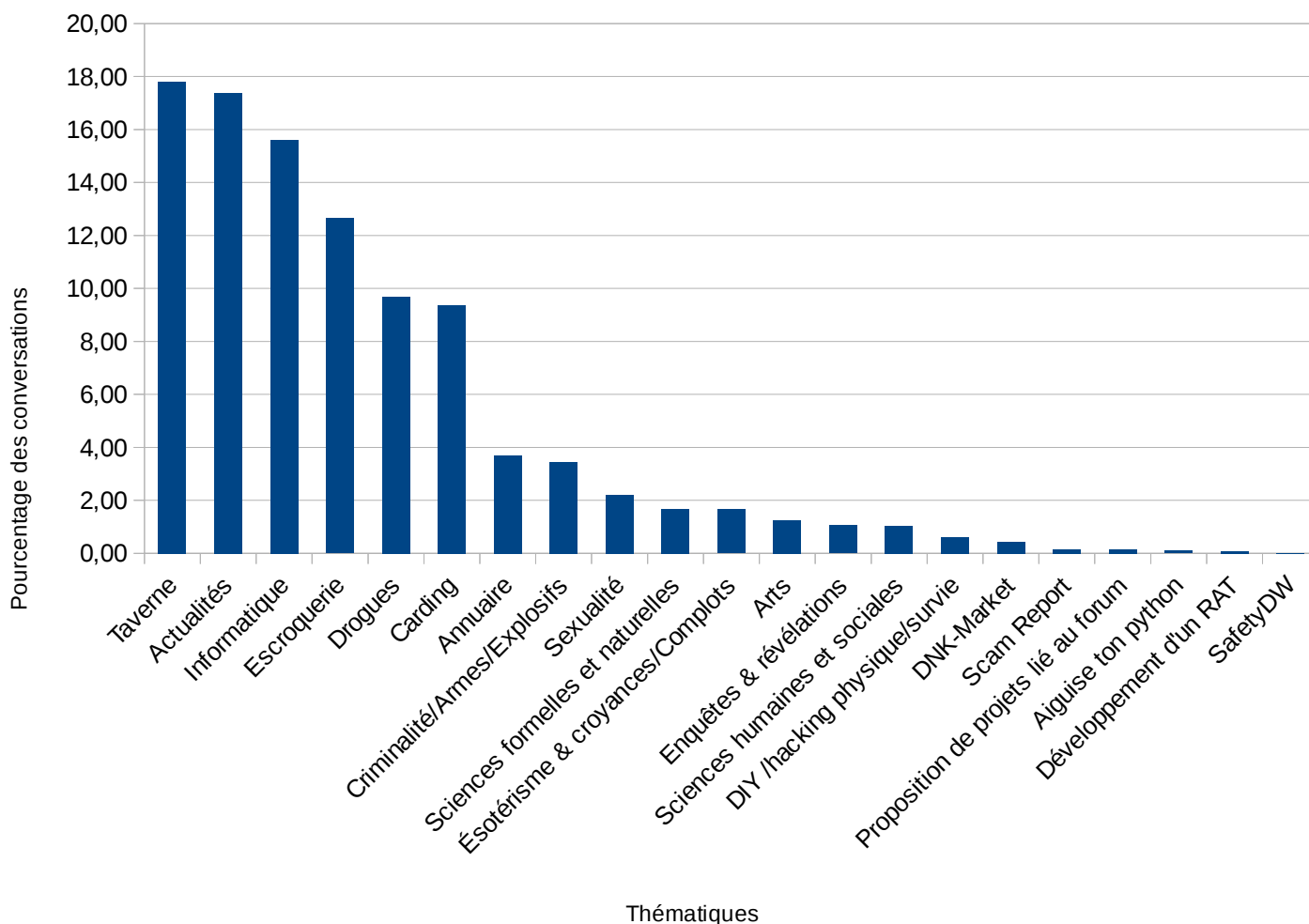
Comme dans nos travaux précédents, nous avons opté pour le choix d'une ethnographie en ligne se limitant aux captures d'écran. Nous avons ainsi pris soin de rassembler et classer par thématiques tout un ensemble de conversations se référant à des sujets aussi variés que possible. Ce choix méthodologique trouve sa source dans deux points majeurs liés à la fois au conditions objectives du terrain virtuel mais aussi, à un choix délibéré de rester dans un cadre entièrement

²⁸ Source : <https://www.populationdata.net>

numérique. L'importance de saisir le « quotidien » au sein d'un groupe d'enquêtés, et ce à travers leurs conversations journalières, représente pour nous l'assurance d'une certaine d'authenticité dans les échanges du groupe. L'objectif fondamental restant de restituer avec le plus justesse une routine de groupe, le choix de se saisir du terrain « as it is », c'est-à-dire de ne pas sortir du cadre numérique, devenait pour nous un choix aussi rationnel que justifié. Comme pour les recherches de Tom Boellstorff (2013) sur le jeu *Second Life* ou de Bonnie Nardi (2010) sur *World of Warcraft*, l'ethnographie numérique permet ainsi d'observer et d'analyser les phénomènes socioculturels qui peuvent émerger d'un espace interactif tel qu'internet. Nous appréhendons le terrain du *darknet* Tor et du forum « DeepNetwork » comme auto-suffisant et par lequel un ensemble d'individus, au sein d'une communauté, font émerger un ensemble de normes et pratiques sociales spécifiques à ce cyberspace.

Pour cadrer ce travail nous avons pris comme environnement d'enquête les différentes thématiques du forum dans lesquelles des internautes ouvraient des fils de conversations. Ces conversations pouvant s'étendre sur plusieurs dizaines de pages, ces dernières représentaient un terreau d'analyse extrêmement riche pour notre recherche :

Diagramme des thématiques du forum sur un total de 12261 conversations



- Dans un premier temps nous avons extrait les différentes thématiques présentes dans le forum pour ainsi en dégager les plus actives des plus secondaires. Cette observation nous permet de mieux comprendre quels sont les sujets les plus abordés entre les internautes et ainsi en extraire des pistes d'analyses futures. Nous avons pu constater que les thématiques contenant le plus de fils de conversations rassemblent des sujets gravitant majoritairement autour de l'informatique orienté *cracking* ainsi que de l'actualité.

- Nous avons donc dans un second temps focalisé notre regard sur ces fils de conversations, tant ceux publiés sous les thématiques vues précédemment que sur d'autres moins courantes et ce pour étudier certains mécanismes propres à des formes de collectifs. Que ce soit en réaction à des simples tutoriels ou à des demandes d'informations, les commentaires laissés permettent de comprendre certaines logiques, comme celles qui peuvent s'attacher au respect des normes du groupe ou à l'anonymisation par le vocabulaire utilisé, ou encore celles qui font écho à une forme de distinction entre les internautes, sur celui/celle dont le statut ou la mesure de son capital subculturel lui permettent de légitimer la pertinence de ses propos. Tout ce travail de recueil et de classification de données de terrain nous servira à faire émerger dans notre analyse, une étude de terrain aussi précise et pertinente que ce que peuvent permettre les contraintes de ce mémoire.

D) Les entretiens exploratoires comme moyen d'accéder aux discours et aux représentations des acteurs.

Au vu des contraintes et de la sensibilité du terrain étudié, il a été décidé en premier lieu, de ne faire appel qu'aux observations et à l'analyse conversationnelle et non aux entretiens individuels. En effet, au vu de la méfiance de certains utilisateurs de la communauté, le risque de se faire exclure du terrain a été tout le long de ce travail une réelle inquiétude et un enjeu méthodologique important. Malgré cela, et après avoir recueilli le contenu nécessaire à la réalisation des objectifs analytiques de ce travail (via les captures d'écran), il a été décidé d'entamer des entretiens avec certains utilisateurs du réseau. Ces entretiens avaient pour objectifs d'enrichir ce travail et de nous permettre à la fois d'affiner certaines analyses mais aussi d'ajouter la dimension subjective des enquêté-e-s via leurs expériences personnelles sur le *darknet* Tor.

Par respect de l’anonymat des interviewé-e-s, notre échantillonnage ne pourra renseigner que les informations qu’ils/elles ont bien voulu nous transmettre. Cet échantillon ne peut prétendre à la représentativité des utilisateurs de ce *darknet* mais agira comme un complément de données empiriques permettant de recueillir une variété des discours et de comptes rendus de pratiques. Ces conversations se sont déroulées dans un cadre **entièrement numérique** au travers d’une plateforme de discussion instantanée anonyme et cryptée se nommant « Cryptocat » et ont suivi une grille d’entretien construite préalablement autour de thématiques générales. Ces thématiques étaient au nombre de quatre et se divisaient comme suit : « Parcours et expériences dans le réseau » / « Perceptions des normes et des valeurs » / « Culture *darknet* » et enfin « Aspects politiques du réseau ». Dans la majorité des cas, ces thématiques ont été abordées dans cet ordre et se sont terminées sur des conversations ordinaires pour tenter de rompre avec l’aspect investigateur auquel je pouvais être renvoyé. Sauf pour un enquête (Sébastien) qu’une connaissance m’a conseillé via le réseau social Facebook, la prise de contact pour cet échantillon s’est déroulée via le forum « DeepNetwork » et par prise de contact directe via la messagerie du forum. Nous notons que pour dix demandes d’entretien, seulement trois internautes ont répondu positivement à la demande. Les autres se sont soldées par des échecs (quatre non réponses et trois refus).

Enquêté-e-s*	Age	Description
Bob	23 ans	Membre gradé du forum (Vénérable), se connecte à Tor quelques fois par mois. Majoritairement pour se tenir au courant des nouvelles et procéder à des achats.
Fred	34 ans	Membre gradé du forum (Antédiluvien), se dit cracker, se connecte sur Tor plusieurs fois par semaine pour contribuer à sa communauté et pour apprendre de nouvelles compétences. Habite dans le « Nord ».

Camille	Non divulgué	Étudiant-e , il/elle se connecte sur le réseau essentiellement pour acheter des stupéfiants. Ne contribue quasiment pas aux contenus.
Mathieu	« La vingtaine »	Membre Novice , se dit bidouilleur-se et curieux-se. Utilisateur-trice occasionnel-le du réseau, ne se connecte que pour faire des recherches précises.

*Pour plus de clarté les pseudonymes ont été remplacés par des prénoms anonymes.

III / La contestation au travers des règles et des pratiques.

A) Une communauté fondée sur une double prérogative : l'anonymat et la sécurité.

Comme nous l'avons vu dans les chapitres précédents, le *darknet* Tor fonde son existence sur l'anonymat qu'il procure à ses utilisateurs. En déviant leurs adresse IP dans un autre point du globe, l'architecture du réseau masque ainsi certaines informations (localisation, fournisseur d'accès etc.) intégrées à l'adresse et susceptibles de dé-anonymiser un utilisateur. C'est donc sans surprise que les internautes utilisant ce *darknet* mettent un point d'honneur à rester anonymes autant que possible.

Dans le cas de notre étude nous allons voir que cette double définition d'anonymat et de sécurité représente pour le groupe d'internaute du forum, un élément structurant de leur communauté.

Pour les internautes du « DeepNetwork », le choix de l'anonymat absolu impose une rigueur et un autocontrôle permanent sur les interactions qu'ils peuvent avoir sur le forum. Aucune information personnelle n'est divulguée et toute les pistes pouvant relier à leur identité (ville de résidence, métier etc) sont auto-contrôlées et signalées par les autres utilisateurs en cas de faux pas. Cette sévérité prend évidemment son sens au regard de l'ambition à la création du réseau Tor, à savoir l'anonymat de la navigation et des échanges. Détourner cette fonction fondamentale par les utilisateurs revient à annihiler la raison d'être de ce réseau mais aura surtout pour fonction de faire perdre ce qui représente pour les différentes communauté du *darknet* les fondations de leur mode de fonctionnement. Ce double horizon anonymat-sécurité prend une place centrale dans le modèle de construction de notre groupe étudié et sur lequel différentes pratiques viennent se construire en adéquation avec cette dernière. Par exemple, permettre au groupe l'expression de certaines formes de déviances ou de dissidences ne sont possible seulement si l'identité civile est masquée et protégée. Mais, au-delà de l'expression d'un mode de pensée et de pratiques libertaires permises par ce dispositif, l'apprentissage de cette dernière relève pour nous d'une forme **collective d'acquisition de compétences** au sein de la communauté. En effet, le choix de l'anonymat et de la sécurité des échanges, étant des règles contraignantes, leur application passe par un apprentissage

progressif sur lequel les « nouveaux entrants » dans le forum font leurs preuves pour gagner en crédibilité et alimenter leur capital subculturel (Sarah Thornton, 1995). Si ils l'estiment nécessaire, les anciens ou les plus compétents se chargeront publiquement de signaler les défauts ou les mauvaises manipulations aux novices. Cette configuration aura pour résultat de faire d'accroître les compétences de toute la communauté tout en alimentant le prestige de ceux qui signalent les « erreurs ». Ce modèle de fonctionnement scientifique de « la relecture par les pairs », est une logique qui a été acquise dès le début du mouvement *hackers* et perdue aujourd'hui dans toutes les communautés qui s'en revendique (Himanen, 2001). L'apprentissage par les novices des notions de sécurité et d'anonymat est une démarche que nous situons à la base du « parcours de l'internaute ²⁹ » du *deepweb* et avec laquelle ce dernier va construire un certain nombre de savoir-faire. Ces savoir-faire peuvent être variés et peuvent aller de l'apprentissage de la cryptographie à la maîtrise de son identité virtuelle par la retenue en passant par la maîtrise de sa « graphologie³⁰ » en ligne.

« L'anonymat, ANONYMAT, on demande pas le tel ou le Skype de personne, on ne donne pas son adresse, encore moins ses coordonnées bancaires, on désactive java-script, on va pas sur Facebook en même temps que sur le deepweb sur TOR. Il y a vous sur le clearweb et vous sur Deepweb, ils ne doivent être repliable en rien ! Vous faites pas des recherches de choses trouvées sur l'onion sur chrome par ce que ça va plus vite ! Ne faites n'importe quoi, réfléchissez avant d'agir. »

Extrait des « guides de débutants »

L'analyse des différents *topics* et conversations nous ont permis de mettre à jour les éléments constitutifs du capital subculturel des internautes. Par exemple la section « Présentation » du forum a été pour nous un excellent terrain d'observation pour mieux comprendre et analyser comment les internautes se présentent à la communauté quelles informations ceux-ci divulguent mais aussi quels types de compétences sont mobilisées dès leur entrée dans le groupe.

Pour rappel³¹ la section « présentation » est une page du forum principalement dédiée aux nouveaux membres et y regroupe les messages de celles et ceux souhaitant se présenter à la communauté.

Pour la majorité des membres, ces quelques lignes représentent leurs premières publications³² dans le forum et ainsi leurs premières participations au sein de la communauté. Elle permettent de « briser la glace » et font partie des règles de bonne conduite. Dès leurs premiers messages,

29 Expression empruntée à l'*hacktiviste* français Benjamin Bayard.

30 La graphologie est une science qui permet d'analyser et de reconnaître l'écriture d'une personne et en établir un profil psychologique en fonction de cette dernière. Il est aujourd'hui possible d'appliquer cette démarche à un corpus de texte en ligne pour établir l'identité d'une personne.

31 Cette section a été présentée dans notre précédent mémoire de Master I

32 Attesté par la mise en visibilité du nombre de messages postés en bas de la photo de profil des utilisateurs.

beaucoup de nouveaux entrants font part de leur désir de créer leur clef PGP³³ publique afin que d'autres membres puissent communiquer avec eux de manière sécurisée et anonyme via la messagerie du forum. Lorsque cette clef est créée, cette dernière est systématiquement épinglée par les membres eux-mêmes en pied de page de leurs messages. Ainsi le partage, à la vue des autres membres dépasse l'aspect pratique et se saisit d'une fonction sociale singulière dans le groupe qui est celle de signifier à tous une maîtrise minimum de la cryptographie.

La sécurité informatique dans sa vision élargie (protection des données personnelles, intégrité des machines, du réseau ou de son identité digitale) est un domaine de fort intérêt dans la communauté du « DeepNetwork ». Le *clearweb* étant vu comme « une passoire ³⁴», beaucoup d'internautes viennent dans ces lieux reclus pour en apprendre un peu plus sur les failles informatiques potentielles. Certains viennent simplement corriger certaines de leurs habitudes de navigation et c'est à chacun d'évaluer la mesure de son implication dans la diffusion d'informations.

L'exploitation de certaines failles de sécurité (informatiques ou non ³⁵) à des fins personnelles est un domaine lui aussi assez populaire dans le forum. Les membres y partagent informations et expériences et améliorent ainsi collectivement leurs compétences en *cracking* ou simplement satisfont leur curiosité. Même si les intérêts des membres peuvent être très divers et peuvent aller de la simple soif de connaissances pour les uns, jusqu'à la constitution d'activités criminelles pour d'autres, les membres de la communauté revendiquent à la majorité, et quel que soit l'objet de leur présence dans la communauté, la priorité donnée à l'anonymat et à la sécurité au sein du réseau.

En choisissant de subvertir les contraintes légales ou morales entourant certaines pratiques comme le *cracking*, le *scam*³⁶ ou le partage de documents sous *copyrights*, les membres font le choix d'adopter une démarche contestataire typiquement *cracker* « *black hats* » : les droits d'auteur ou tout autre tentative d'encadrement et de normalisation de contenus sont sans cesse contournés et décriés au profit d'un mode de pensée se rapprochant d'une éthique *hacker*³⁷ plus libertaire. Par la mise en avant de l'anonymat et la sécurité dans la communauté, les membres revendiquent le droit à la vie privée et au « caché » sur internet. Que les savoirs partagés servent des intérêts frauduleux ou non, les membres sont tous réunis pour compléter et enrichir des domaines d'informations dont la sécurité et les dispositifs d'anonymisation jouent un rôle central.

33 Technologie utilisant la cryptographie asymétrique.

34 Selon les propos d'un membre du forum pris dans un post.

35 Certaines failles peuvent être d'origine humaine et exploitable sous la forme de manipulation psychologique (social engineering).

36 Arnaques à la carte bancaire

37 HIMANEN, Pekka (2001), *L'Éthique hacker et l'esprit de l'ère de l'information de l'information*, Exils, Coll. Essais

B) L'élitisme technologique comme pratique structurante de la communauté.

Dans un article intitulé *Power/freedom on the darkweb: A digital ethnography of the Dark Web Social Network*, Robert Gehl décrit le mode de fonctionnement d'une communauté du *darknet* au travers d'une focale basée sur la tension que celle-ci exerce entre pouvoir et liberté. À l'image de la prohibition de la pédopornographie dans le *DeepNetwork*, les membres de la communauté étudiée par Gehl procèdent de façon similaire pour arbitrer entre liberté d'expression au sein de la communauté et règles de modération qui, par principe, vont à l'encontre de cette dernière. Cette tension entre pouvoir et liberté est décrite comme étant au cœur des modes de régulation de la communauté. En suivant ce double enjeu, l'auteur fait émerger certaines pratiques des membres dont une que nous voulons transposer à la communauté du *DeepNetwork*, celle de **l'élitisme technologique**. Cette forme d'élitisme agit comme un filtre de compétences qui exclut directement ou indirectement les membres les moins chevronnés en informatique. Nous voulons à travers la transposition de ce concept dans notre propre communauté, décrire le mode de déploiement de cette forme d'élitisme et expliquer en quoi celui-ci relève de **l'auto-préservation de la communauté**.

Comme nous l'avons vu plus haut dans ce mémoire, l'accès aux services cachés de Tor impose certains pré-requis qui amoindrissent les chances qu'un internaute « lambda » se retrouve impliqué dans une communauté du *darknet*. Cependant, le *DeepNetwork* reste relativement ouvert et contrairement à certains autres forums du réseau Tor, une personne peut, au bout de quelques minutes, se créer un profil et commencer des discussions. Toutefois, cette relative ouverture de la communauté est contrebalancée par une grande sévérité envers les manquements aux règlements et aux pratiques de la communauté. Les références péjoratives qui sont faites aux *noobs*³⁸ qui n'utilisent pas la fonction recherche et ne lisent pas le règlement sont monnaie courante. Atteste cette conversation prise sur le forum :

– *Membre 1* : « Bonjour vous savez ou est ce que je peux trouver de la MDMA ? »

– *Membre 2* : « Tu vas pas faire long feu ici si tu continues à poser des questions de merde comme ça ».

– *Admin* : « Pas de business sur le DN. 1 mois de ban. »

³⁸ *Noob* est l'abréviation péjorative de *newbie*, c'est-à-dire un débutant dans le domaine de l'informatique. Ce terme est également utilisé comme insulte dans les jeux vidéo pour un joueur considéré comme débutant.

La crédibilité d'un membre peut être atteinte si ce dernier réitère les mêmes erreurs de débutants. Pour comprendre cette sévérité envers les nouveaux membres et les efforts faits pour ne pas se décrédibiliser et passer pour un novice, il faut remonter à certains événements marquants du réseau Tor. En effet depuis l'affaire du site *The Silkroad* puis les révélations de Edward Snowden, le trafic sur le réseau Tor a significativement augmenté apportant des centaines de milliers de nouveaux membres sur tout le réseau. Cet afflux massif de *noobs* a été vu comme une menace pour la communauté du *DeepNetwork* qui s'est vue, en réponse, durcir drastiquement ses règles de modération. Même après l'accalmie et le départ de la majorité de ces badauds venus du *clearweb*, la communauté continua de souffrir de la médiatisation du *darknet* dans les grands médias, apportant encore son lot de curieux et d'adolescents à la recherche de sensationnel. Cette répulsion pour le *noob* par une partie des membres transparait dans certaines pratiques comme par exemple l'obligation de décrypter un message codé pour pouvoir lire un document partagé par un membre. Ce « patch anti-noob » qui reste malgré tout peu répandu, est révélateur d'une certaine véhémence d'une partie des membres envers les moins compétents.

L'attachement de la communauté aux règles d'anonymat impose aussi à ses membres une parfaite maîtrise de l'interaction. La divulgation d'informations pouvant retracer l'identité de la personne peut être perçue comme un signe d'amateurisme et d'un manque de rigueur par d'autres membres ou modérateurs. Dans ces cas, un rappel à l'ordre est souvent prodigué de manière plus ou moins courtoise selon la personne ainsi que le rang du « fautif ». Il en est de même pour les règles de sécurité où plusieurs membres n'acceptent de converser en privé qu'à condition d'utiliser des clefs de cryptographie. D'ailleurs la création et l'affichage de sa clef de cryptage relève de plusieurs aspects dans la dynamique du forum que nous voulons brièvement expliciter ici. Premièrement, elle permet au membre de se démarquer des *noobs* ne sachant pas utiliser ce que la communauté considère comme étant les b.a.-ba des outils du *darknet*. Ensuite, elle est pour la communauté une marque de confiance et de sécurité pour des personnes ayant des conversations pouvant leur porter préjudice. Et enfin, l'affichage et l'utilisation de la cryptographie de manière générale relève de l'affirmation de ce que sont les enjeux légitimes du *darknet* : la sécurité et l'anonymat. Toutes ces pratiques ayant cours sur le *DeepNetwork* et ayant pour modalité la maîtrise de l'outil informatique, sont pour nous au cœur de cet élitisme technologique. Une manière d'affirmer ses compétences et la maîtrise de son savoir par la contribution aux conversations du forum. Ainsi, aider d'autres membres, contribuer à un sujet ou encore créer des postes pour qu'ils soient épinglés en haut de page, servent à gagner en crédibilité auprès de la communauté par l'affichage de ses compétences.

Dans ce réseau social où le cadre interactionnel est 100 % numérique, l'affirmation de sa légitimité en tant que membre passe par la maîtrise d'un certain nombre de savoirs inhérents au *Darknet* et au web de manière générale (recherche d'informations, croisement des sources, maîtrise de certains outils etc.) Ces savoirs étant indissociables du canal par lequel ils sont transmis, la maîtrise de l'outil technologique devient un enjeu en soi. La véhémence parfois exprimée envers les mauvais novices passe par le fait que leur maîtrise incomplète des outils informatiques et de l'information peut être vue comme handicapante pour la communauté qui recherche une certaine efficacité informationnelle et interactionnelle. Ce qui peut expliquer -dans une certaine mesure- les sanctions systématiques liées à l'abus de fautes d'orthographe.

Paradoxalement à cette position peu valorisante, les novices ne sont pas dénués d'intérêts et concourent grandement à la dynamique de la communauté. En effet leur amateurisme dans certains domaines donne la possibilité à d'autres, plus expérimentés, d'afficher leurs compétences en répondant à leurs questions. En rentrant dans une relation d'entraide, des utilisateurs plus anciens ou plus expérimentés peuvent afficher leurs compétences, les améliorer et ainsi gagner en crédibilité. Ainsi, un novice ayant acquis de nouvelles compétences au travers de ces relations d'entraide et des tutoriels disponibles, pourra lui aussi aider d'autres novices et monter les échelons. D'ailleurs, un nombre conséquent de ces tutoriels sont écrits par des utilisateurs (hors modérateurs) et servent ainsi cette stratégie d'altruisme. La mise en avant du savoir par la contribution à la communauté est un processus de légitimation qui appuie cet élitisme technologique. Autrement dit, montrer que l'on maîtrise l'interaction anonyme, la pertinence des informations véhiculées et l'outil informatique de manière générale permet d'acquérir du crédit auprès des autres membres.

C) Normes sociales de la communauté.

« *Nous sommes une communauté très hétéroclite. Elle se compose d'escrocs, de marginaux, de voleurs, de menteurs, de fous, de dissidents...Pour réussir à unir toute cette grande famille sans qu'elle ne s'entre-tue (sens figuré) il est indispensable de garder quelques règles de bonne tenue. »*

C.1) Le statut du règlement intérieur

Comme pour toute communauté subculturelle locale ou *groupculture*, celle que nous étudions dans ce projet de mémoire possède un certain nombre de normes partagées entre ses membres. Elles se divisent en normes formelles et informelles et comme pour toutes règles sociales, leur évolution dans le temps est le fruit de résistances ainsi que de négociations collectives. Afin de familiariser les nouveaux entrants au modèle de fonctionnement du groupe et d'afficher leurs importances, le placement des règles fait l'objet d'un positionnement stratégique dans l'ergonomie du site. En effet, dès son arrivée sur ce dernier, et par le biais de la mise en page, l'utilisateur novice est invité à prendre connaissance d'un certain nombre de règles internes au groupe. Majoritairement créées pour ces nouveaux arrivants, ces dispositions sont des guides pour le nouvel utilisateur souhaitant s'intégrer à la communauté et naviguer sur les différentes sections du forum. En effet, chaque section thématique dispose de *posts* centralisant les informations relatives à leurs bons fonctionnements : on y trouve les questions fréquemment posées par les internautes, le vocabulaire spécifique utilisé ainsi que toutes autres informations permettant aux utilisateurs d'être autonomes dans leur apprentissage. L'assimilation des règles et des techniques par l'internaute novice se fait de manière séquentielle et suit l'organisation du site. Les informations considérées comme primordiales, généralistes et applicables à tout le *darknet* sont épinglées en page de garde du forum alors que les informations plus spécialisées sont quant à elles, à chercher dans des *topics* spécifiques et dans les liens hypertextes qui les composent. L'entête du forum comprend donc les liens renvoyant aux informations suivantes (liste non exhaustive) :

- Le règlement du forum.
- Le rang des utilisateurs.
- Les règles de bienséance et de publication.
- La sécurisation du navigateur Tor.

- L'utilisation de clef de chiffrement.
- Le vocabulaire utilisé dans le forum.
- Un « guide de survie » du *deep web* pour les débutants.

La présence de règlements internes aux forums est une pratique assez répandue sur le web en général. Cependant, l'importance qui y est accordée varie en fonction des sites et des communautés qui la compose. Si en effet la majorité des forums disposent d'un onglet explicitant les règles de fonctionnement, il n'est cependant pas aussi commun que ces dernières prennent autant de place et soient sujet à autant de rappels. Ces liens renvoyant aux règles de fonctionnement de la communauté étudiée sont au cœur des pratiques des utilisateurs. Chaque *post* rédigé par un internaute est amené à suivre ces règles, sinon son auteur s'expose à des sanctions de la part de la communauté. Par son caractère écrit et sa visibilité permanente durant la navigation sur le forum « DeepNetwork », ces textes se posent comme les principaux cadres de normalisation des pratiques. **Ce sont les règles formelles du groupe.** Elles se composent de l'interdiction de la pédopornographie, de la xénophobie, du commerce, de l'assistanat ainsi que des messages visant à polluer les fils de conversation.

Ce forum étant stocké sur un hébergement mutualisé, il est de votre responsabilité de respecter les règles établies par l'hébergeur : [\[lien\]](#)

Pornographie infantile

Si il est autorisé d'aborder le sujet, la diffusion de contenu pédopornographique (photos, vidéos, liens, etc...) est strictement interdite.

Xénophobie

La xénophobie (origines, croyances, etc...) n'est pas tolérée sur [\[lien\]](#)

Commerce

[\[lien\]](#) n'est pas un forum à visée lucrative ou mercantile. Il n'est pas permis d'effectuer des transactions, de se créer une forme de business, de faire de la publicité ou de la vente sauvage.

Assistanat

L'assistanat (à ne pas confondre avec l'entraide) n'est pas toléré. Nous entendons par assistanat le fait d'ouvrir un topic juste pour que les gens fassent quelque chose que l'auteur du topic aurait très bien pu faire tout seul sans prendre le temps des autres. Notre temps est précieux, ne nous le faite pas perdre.

Bonnes pratiques

Les messages polluants sont à éviter. Les spams, les up, les doublons et le langage SMS sont autant de choses à éviter.

Sachez qu'il n'y a pas de réelle règle de modération.

Les modos tireront à vue sur tout comportement suspect ou abusif, et priez pour que ce soit pas un admin qui s'occupe de votre cas. Si vous constatez un comportement contraire à ce règlement, cliquez sur le lien "Signaler", en bas à droite du message incriminé. Par contre, n'abusez pas de cette fonction, ne faites pas perdre de temps à l'équipe.

À tout hasard, voici un topic étendu sur les règles : [Règles étendues](#).

Règlement intérieur du forum

L'application de ces règles est gérée par les modérateurs qui sanctionnent les utilisateurs en cas de manquements à ce règlement et s'appliquent de la manière qui suit :

-Membre novice : Salut, je cherche un plan pour des XTC, entre 100 et 500 / semaine environ, obligatoirement avec envoi FR et express (...) je dois passer par FR et mon gars n'est plus là.

-Modérateur : Pas de business sur le forum. Un mois de bannissement.

Conversation extraite du forum

Le non respect de chacun des points du règlement vu plus haut fait l'objet de sanctions lourdes qui passent souvent -sans rappel à l'ordre préalable - par le bannissement temporaire ou définitif du membre fautif. Si la mise en application du respect des normes formelles s'applique via le bannissement par une autorité en place (modérateurs), les normes informelles -plus subtiles- s'exercent elles, par la sanction morale. Elles peuvent s'exercer par l'ensemble de la communauté et peuvent prendre la forme de brimades, rappels à l'ordre, d'humiliations et pouvant aller jusqu'à l'exclusion d'un membre du groupe. Les sanctions proférées à l'égard de certains utilisateurs qui ne respectent pas les règles s'exercent avec une violence assez palpable. Le degré de la sanction est souvent corrélé à la « gravité » de la maladresse / faute et il n'est pas rare de voir des formes d'humiliation des novices par les modérateurs.

Cette violence du modèle de régulation de la communauté traduit un fort désir de contrôle et de coercition des membres par le filtrage des moins disciplinés et des moins autonomes. En effet ceux qui, par leurs messages, traduisent un manque de maturité ou la non lecture du règlement du forum subissent systématiquement le quolibet des autres membres qui les rappellent à l'ordre de manière franche et sévère.

Nous développerons plus en détail, dans la partie qui suit, certains aspects de ces normes informelles notamment celles des normes langagières et des règles conversationnelles de la communauté.

C.2) Argot et sociolecte.

La formation d'une culture -ou dans notre cas d'une subculture- est nécessairement un processus linguistiquement médiatisé (Prus, 1997). Ce processus permet, par l'élaboration de mots ou d'expressions, de formuler une représentation du monde commune pour celles et ceux qui partagent cette même culture. Le langage permet à cette culture de se transmettre d'une personne à une autre et de créer des liens entre celles et ceux qui partagent un certain nombre de ces signifiants. Ainsi, tout groupe social se caractérisant par une proximité géographique, sociale, générationnelle ou culturelle tend à établir un sociolecte³⁹ le démarquant des autres groupes sociaux alentours. Bien que les membres d'une société puissent avoir un langage préexistant en commun (leur langue), en formant des groupes autour d'activités communes, ces derniers développent un vocabulaire spécifique qui ne peut souvent être compréhensible que par les membres de ce groupe (Mitchell, 1983, Letkemann, 1973, Prus, 1997, Shibutani, 1955). Cet argot peut relever d'une fonction pratique -le cas du jargon des métiers par exemple- mais peut aussi prendre une marque plus identitaire comme pour celui de l'argot des « cités » ou encore le langage « jeune » (Bulot, 1999). Le développement d'un argot spécifique est donc un élément constitutif d'une subculture et en devient une partie intégrante. La spécificité de cet argot peut prendre la forme de modifications d'accents, d'inventions de nouveaux mots ou encore de contractions de ces derniers jusqu'à l'utilisation d'acronymes. Toutes ces nouvelles formes linguistiques ont trait à partager au sein d'un environnement de proximité culturelle, un ensemble de vocabulaire qui fait « sens » dans une subculture.

Ainsi l'argot d'une subculture peut se développer en tant que le reflet des différentes expériences de ses membres, de leurs préoccupations, ou encore d'intérêts à réaliser des contenus de communication particulières. Comme la langue d'un groupe évolue pour formuler de nouvelles façons de conceptualiser les objets, la perspective de ce dernier change nécessairement pour correspondre à de nouvelles réalités linguistiques (Kleinknecht, 2003). Un même mot peut ainsi circuler d'une culture, ou d'une subculture, à une autre et prendre des sens différents à chaque passage.

La partie que nous entamons ici aura pour objectif d'examiner, au travers des conversations des membres de la communauté, comment celle-ci structure un langage et un argot spécifique à la

³⁹ En linguistique, un sociolecte est une sorte de dialecte, précisément la façon de parler d'un groupe social, d'une classe sociale, ou de toute catégorie se distinguant par une *culture intime*. Source : Wikipédia

subculture des *darknet* et comment au travers de ces usages différenciés du vocabulaire, se distinguent des pratiques différentes au sein de la même communauté.

C.3) Normes conversationnelles.

« Un forum est un espace où le moyen d'échange est l'écriture. Nous ne sommes pas des grammar-nazies, mais il est indispensable que vous fassiez un minimum d'efforts pour écrire proprement. Si vous n'êtes pas trop paranoïaques, ou particulièrement peu doué en orthographe, vous pouvez installer un correcteur(...) Bref, on ne vous demande pas d'accorder chaque verbe, de n'oublier aucun accent ou de bien mettre toutes les majuscules...mais de rester lisible, ceci pour le confort de tous. Le CAPLOCK est aussi à éviter (...) +1 n'est pas un propos pertinent, et la durée pour qu'un sujet soit « périmé » est relative. Il en va de même pour les « floodoirs » ... Tout ceci demande que vous réfléchissiez par vous-même pour ne pas faire n'importe quoi n'importe où.

Donc deux choses si vous doutez :

- Vous vous abstenez.
- Vous contactez un membre du staff pour demander.

Nous ne sommes pas des tortionnaires juste bons à faire sauter des comptes. Personne ne vous reprochera d'avoir demandé avant d'agir. »

Post rédigé par un membre et extrait des «règles de bonnes pratiques »

Comme pour la majorité des plateformes de discussion ou de contenu sur internet, l'écrit représente le moyen privilégié de communication entre les utilisateurs du réseau. Pour aider à la lisibilité et améliorer l'efficacité des échanges, un certain nombre de normes implicites se sont mises en place progressivement jusqu'à devenir ce qu'on appelle aujourd'hui la « netiquette ⁴⁰ » : Une sorte de « contrat social » ou de code de conduite du cyberspace que l'on pourrait brièvement résumer ici par ses grands principes : Clarté, Concision, Prudence, Respect, Courtoisie. Le plus souvent ces principes ne sont pas immuables et chaque espace d'échange dispose de règles plus ou moins permissives à leur sujet, en focalisant l'attention sur un point plus qu'un autre par exemple. Ces règles communément admises dans les forums du *clearweb* se retrouvent appliquées sur le *darknet* et chaque communauté gère cette norme informelle différemment.

40 Pour accéder au document officiel de la norme RFC1855 : <https://tools.ietf.org/html/rfc1855>

Le forum que nous étudions ici affiche une attention particulière quant aux trois premiers points précédemment abordés. La clarté des propos et des questions posées par les utilisateurs prend ainsi un rôle central dans la diffusion des informations et son application passe selon nos analyses, par l'apprentissage d'une norme dans la communauté étudiée. À l'inverse de certains forums du *clearweb* qui ont consenti à un certain laxisme au niveau de la rigueur langagière, les membres et modérateurs du « deepNetwork » ont quant à eux souvent recours aux sanctions à l'égard de membres dont l'orthographe ou la syntaxe peut nuire à la lisibilité du message.

« -Administrateur : - à l'école, on apprend surtout à écrire correctement. Et vu ton niveau, je peux dire sans me tromper que ton assiduité en classe laissait fortement à désirer .
-Membre novice : - j'ai le bac monsieur. j'ai (sik) 21 ans et toujours eu des soucis avec ça un peut d'indulgence est il possible.
-Administrateur : - Si tu fais un effort, c'est possible. Mais là, tu n'en fais aucun. Si tu n'as pas le respect de correctement écrire pour que tes interlocuteurs ne se crève pas les yeux en te lisant, je n'ai aucune raison d'être indulgent. »

Cette intransigeance sur l'écrit traduit selon nous la visée de la modération, celle de forger et faire perdurer une communauté d'individus auto-régulés et dans laquelle les interactions sont efficaces. L'humour n'est évidemment pas exclu du forum et les blagues sont très récurrentes dans les discussions mais le soin donné à l'écrit est lui toujours de rigueur. A l'inverse, il peut être détourné pour tourner en dérision certaines pratiques d'utilisateurs en le renvoyant aux *noobs* :

Membre : - « Mdr il a mi un pass anti n00b kro for XD »

Cette conception assez stricte de la forme des échanges n'est pas sans rappeler une certaine vision élitiste et exclusive du « code de conduite des *hackers* ⁴¹ » dont celle des *darknets* est héritière. Elle permet de jouer une double fonction de décrédibilisation et d'exclusion des novices fraîchement arrivés d'autres forums plus laxistes du *clearweb* et permet en même temps d'afficher son statut social pour ceux et celles qui maîtrisent l'écrit. De plus, un facteur historique interne à la communauté du « DeepNetwork » vient renforcer cette inflexibilité des règles du forum et notamment de l'écrit. En effet depuis l'affaire de « silkroad » ainsi que des révélations d'Edward Snowden, les *darknets* ont subi malgré eux, une médiatisation importante. Due à cette dernière, une arrivée massive de novices et de curieux a afflué sur les communautés déjà établies. Cet événement

41 « How to become a *hacker* », disponible dans le lien suivant : <http://www.catb.org/esr/faqs/hacker-howto.html#respect3>

a été vu comme un bouleversement pour la communauté et a eu pour conséquence de briser l'entre-soi déjà constitué. Cette arrivée massive de *noobs* ne maîtrisant pas les codes étaient reconnaissables au manque de rigueur accordée à l'orthographe et à la syntaxe mais aussi au règlement interne des communautés de manière générale. Ce bouleversement a ainsi eu pour conséquence de renforcer les sanctions au sein du forum pour accroître la régulation de la communauté et conserver une mainmise des « anciens » sur le forum.

C.4) Différenciation des argots en fonction des différentes pratiques.

Comme nous l'avons vu plus haut, le « deepNetwork » possède plusieurs *posts* destinés à transmettre aux novices les normes et les modes de conduites sur le forum. De fait, la maîtrise du vocabulaire représente une partie importante du processus d'apprentissage des novices et les aide à comprendre les conversations tout en alimentant leur capital subculturel.

Le *darknet* -comme toute subculture- dispose d'un argot spécifique à son fonctionnement, à sa diffusion et à la préservation de son identité. Il représente un ensemble de mots trouvant leurs sens à l'intérieur de ce cyberspace et marque les frontières avec l'environnement extérieur. Héritières de la subculture *hacker*, les communautés des *darknets* en emprunte certains de ses codes dont un « jargon file⁴² » spécifique à leur cyberspace. Chaque communauté adapte ce glossaire à sa langue d'usage et plusieurs mots -majoritairement des anglicismes- sont utilisés par toutes les communautés des *darknets*. Un nouvel internaute voulant s'intégrer à une communauté ou simplement chercher de l'information sur un *darknet* devra en apprendre le jargon sous peine de difficultés.

42 Le Jargon File est un glossaire spécialisé dans l'argot des programmeurs.

- **AV** = Anti-virus.
- **Binder** = prendre un trojan et le lier à un autre logiciel pour le cacher.
- **bio-hacker** = communauté réunissant scientifiques, université, simples curieux et passionnés, qu'ils soit compétents en génétique, biologie, neurologie, chimie ou géologie dans le but de créer un domaine de la génétique libre afin de faire opposition au monde du "copyright sur le vivant" qui est en train d'émerger
- **BT** = Backtrack (OS Linux spécialisé dans le pentesting et la sécurité)
- **BTC** = BitCoins => Monnaie pouvant être utilisée de façon anonyme sur le Deep Web.
- **Card sharing** = C'est le fait de permettre à plusieurs utilisateurs d'accéder aux chaînes de télévision payantes à partir d'une seule carte d'abonnement mise en partage.
- **Defacing** = fait de modifier par un acte de piratage la page d'accueil d'un site afin d'y afficher le message voulu par le pirate.
- **Dump** = Petite ou grosse database contenant des informations (Généralement en texte)
- **FUD** = indétectable par les antivirus actuels
- **IDE** = Integrated Development Environment >> Outils/Logiciel de développement de programme
- **NFC** = "Near Field Communication" qui veut dire "communication en champ proche" et qui est une technologie de communication sans-fil (comme le bluetooth) à courte portée ainsi qu'à haute fréquence. Cette technologie est utilisée le plus souvent pour les smartphones et les cartes bancaires (sans-fil).
- **No logs** = se dit principalement d'un VPN, cela veut dire que ce dernier ne garde pas vos identifiants de connexion (IP , etc)
- **Open-source** = ce dit d'un système dont le code source, le plan de création ou le principe de fonctionnement est accessible à tous. C'est le contraire du système propriétaire qui , lui , conserve précieusement son code source sous un copyright interdisant la copie, la modification ou l'utilisation détournée. C'est souvent la bête noire des hackers, des pirates et des partageurs en général. Il existe cependant des licences libres tels que la licence GPL.
- **OS** = "Operating system" ce qui signifie "système d'exploitation", comme windows XP, windows seven, mac OS X, Debian, Slackware, kali-linux, backtrack, openBSD, FreeBSD, arch-linux, TRISKELL, Irix, Solaris pour n'en citer que quelques uns.
- **Pass PTT** = clés générique ouvrant un bon nombre de hall d'immeuble par exemple, cela dépend du format.
- **Phreaking** = Le piratage téléphonique
- **RAT** = Un serveur RAT est utilisé pour avoir le contrôle d'un PC distant.
- **RFID** = Radio Frequency Identification système de code barre utilisé dans de nombreux cas, elle est parfois réencodable et c'était la base des cardeurs à une époque....
- **SE** = Social Engineering, ou en français "ingénierie sociale", ce qui signifie "toutes les méthodes de manipulation d'une personne".
- **Socks** = protocole réseau.
- **spread** = méthode de diffusion d'un trojan
- **SQL** = "Structured Query" Language qui veut dire "langage de requête structurée" est un langage informatique normalisé.
- **VPN** = Virtual Private Network (Réseau Privé Virtuel en FR) , vous attribue une autre IP & assure votre anonymat
- **VPS** = Virtual Private Server (Serveur virtuel privé) = serveur privé que l'on peut transformer en VPN, en serveur web, en relais pour tor, en pleins d'autres choses si vous êtes imaginatif.

Illustration 2: Exemple de Jargon file lié à la section informatique du forum

Comme nous l'avons vu sur le diagramme des thématiques (p30) , le forum que nous étudions dispose de plusieurs sections différenciées où plusieurs thèmes y sont abordés. Pour exemple, la section « carding » regroupe des sujets spécialisés dans le *cracking* de cartes bancaires alors que la section « informatique » traite elle de *hacking* et de programmation. Ainsi pour toutes les thématiques qui requièrent des spécifications techniques élevées, un vocabulaire distinct y est employé et est répertorié dans le glossaire du forum⁴³. Fait d'abréviations et d'anglicismes cet argot - à l'image d'un jargon de métier- permet aux membres de communiquer sur des éléments ayant un certain degré de technicité et avec un maximum d'efficacité. Dans le cas de notre étude, le glossaire est divisé en sous-parties traitant chacune une thématique.

Comme pour tous les argots, le vocabulaire spécifique des *hackers* leur permet de maintenir leur culture et aide ces derniers à identifier par la maîtrise ou non de l'argot, la place de chacun dans la communauté. La connaissance de ce vocabulaire constitue évidemment une étape importante de la carrière des internautes dans les communautés des *darknets* et aide à l'intégration d'un individu au

43 Voir annexes

groupe. Ainsi «ne pas connaître l'argot (ou l'utilisant de façon inappropriée) suffit à définir une personne comme étrangère ou banale (...) Toutes les cultures humaines utilisent l'argot de cette triple manière : en tant qu'outil de communication, d'inclusion et d'exclusion ». (Raymond, 2000, page 2).

Comme pour tout *groupculture* local, celui que nous étudions dans ce travail a su développer un vocabulaire spécifique adapté à sa langue de fonctionnement (le Français) et pouvant circuler entre les différentes communautés du *darknet* francophone.

Aussi variés que peuvent être les domaines de connaissances et d'activités recherchés par les nombreux internautes du *darknet*, la maîtrise de l'argot de ce cyberspace est un processus obligatoire au bon déroulement de la navigation. La compréhension, l'apprentissage et la restitution de ce langage propre à cette subculture sont pour nous autant de ressources culturelles nécessaires à la construction et à l'alimentation du **capital subculturel** (Thronton, 1995) des membres de cette subculture *darknet*.

Nécessaire à une bonne intégration, l'argot permet, par mimétisme langagier, de se faire une place parmi une communauté exclusive. Élément intrinsèque au capital subculturel, il permet -comme pour les savoirs et les techniques- d'afficher son statut et de se différencier des membres d'un autre groupe culturel.

D) L'expression identitaire à travers la dichotomie de l'espace.

Face à la multiplicité des formes d'expression que peut avoir une subculture (langage, idéologie, style vestimentaire etc), l'espace géographique représente pour nous un aspect important par lequel une subculture se regroupe et s'exprime. Elle permet aux communautés et aux groupes d'individus de se rencontrer et d'exprimer leur lien d'appartenance à une culture particulière à travers l'espace dans laquelle cette dernière se déploie. Ainsi, s'intéresser à la situation géographique dans laquelle une subculture s'exprime c'est examiner comment un espace construit, influence et reflète les attentes et l'idéologie d'un mouvement culturel. Ainsi, la formation et l'expression d'une subculture fait davantage référence à des espaces et à des territoires qu'à des propriétés ou des objets (Gelder, 2007). Ces territoires sont des lieux de réunions et de rencontres entre les individus d'une subculture et permettent la mise en commun et le partage des expériences individuelles. Les clubs, halls d'immeubles, caves sont autant d'éléments choisis par les acteurs d'une subculture et permettent d'inscrire et de faire perdurer l'identité de leur groupe à travers une

localisation spécifique. Les forêts et les espaces ruraux sont par exemple, depuis plusieurs années, le lieu de rencontres et d'expressions privilégiés des communautés « rave » à travers les *free parties*.⁴⁴

Comme pour tous ces espaces, les *darknets* représentent dans leur forme numérique, des lieux qui permettent la mise en œuvre et l'expression d'une appartenance à une culture marginale et dissidente. Comme pour l'opposition entre les « teufs » et les boîtes de nuit (vues comme « underground » pour l'une et *mainstream* pour l'autre), le *darknet* intègre cette même opposition et opère cette même dichotomie liée à des espaces différenciés que sont le *clearweb* et le *darknet*. Les internautes procèdent ainsi à une démarcation qui a pour fondement l'incompatibilité de ces espaces entre eux. Incompatibilité dans l'idéologie mais aussi dans les outils et services proposés par chaque cyberspace. Par exemple, et à moins de vouloir contourner une censure du réseau internet, aller sur Facebook en utilisant le navigateur Tor serait contradictoire tout autant que vouloir rester anonyme en utilisant le service de messagerie de Google :

« [...] on va pas sur Facebook en même temps que sur le deepweb sur TOR. Il y a vous sur le clearweb et vous sur Deepweb, ils ne doivent être repliable en rien ! Vous faites pas des recherches de choses trouvées sur l'onion sur chrome par ce que ça va plus vite ! »

Extrait des « guides de débutants »

Cette rhétorique qu'on retrouve communément chez les internautes du *darknet* établit une différenciation franche entre l'espace des *darknets* et le *Clearweb*. Ces deux univers opérant avec un mode de fonctionnement et des normes différentes et souvent incompatibles entre elles, agissent sur les individus et orientent les manières avec lesquelles ces personnes vont interagir dans chacun de ces espaces. Les normes de présentation, la manière d'aborder les sujets ainsi que les attendus en terme autodidaxie par exemple, se démarquent d'un espace à l'autre et ne sont légitimes que dans leur propre espace de prédilection. Par l'isolement numérique, les *darknets* permettent l'expression d'une liberté considérée comme muselée en dehors de ces lieux. La liberté de partager, de pirater, d'être déviant et de contester l'ordre et la morale établie, sont tout autant de facteurs qui permettent de différencier l'espace subculturel de l'espace *mainstream*. Ainsi cette différenciation sert aux

44 Concerts de musique électronique organisé de manière autonomes et sans l'accord des autorités.

communautés du *darknet* d'alimenter la construction d'une identité commune basée sur cette opposition binaire entre le "nous » et le « eux", "le souterrain » et « la surface" :

"Ici c'est le darknet » (Camille)

De cette opposition fondamentale s'ajoute un ensemble d'éléments et de points de ruptures entre les deux univers. Les logiciels utilisés, la logique de navigation et d'utilisation de l'espace ou encore la mise en scène de soi à travers l'anonymat sont autant de points de divergences qui séparent les deux univers et affirment l'identité de la subculture.

IV / Idéologie de la subculture *darknet* : Éthique *hacker* et esprit *cracker*.

Selon Prus (1997), une des caractéristiques majeures distinguant une subculture d'une communauté plus large est l'idéologie qui la traverse et qui la différencie d'une plus large communauté. L'idéologie se compose d'un ensemble de catégories de pensées ou de dispositions qui conditionnent le groupe à penser le monde d'un angle particulier et influence leurs actions au sein de ce dernier. Celles-ci peuvent être imposées via l'autorité d'une institution sociale, être le fruit d'une construction collective adaptée à un environnement nouveau ou être une réponse à l'idéologie d'une culture dominante vue comme arbitraire. Dans un contexte de proximité de groupe, les individus tissent des relations les uns avec les autres sur les bases de perspectives similaires tout en renforçant et en maintenant leurs points de vues particuliers (Kleinknecht, 2003). Ces individus peuvent être impliqués dans plusieurs groupes et adhérer à différentes idéologies. Par le biais de ces différentes interactions, ces derniers développent un certain nombre de points de vue à la fois similaires et dissemblables et s'engagent dans une négociation et une reformulation de la réalité en cours (Kleinknecht, 2003). L'idéologie peut être ainsi comprise comme la manière qu'a un groupe ou une communauté plus large "de voir le monde". Du point de vue de la recherche en sciences sociales, l'analyse de cette dernière est une ressource indispensable à une meilleure compréhension d'un groupe ou d'une subculture. Elle conditionne les comportements et représente une façon unique de percevoir l'environnement de ce dernier. Ainsi, l'analyse de l'idéologie d'une subculture permet, par les discours issus de cette dernière, d'en comprendre la visée et les actions. Nous tenterons, dans cette partie d'analyser l'idéologie du *darknet* à travers les principes de fonctionnement de son réseau, de ses règles issus du discours des acteurs et qui forment ainsi l'idéologie de cette *subculture*.

Principe n°1 : Le *darknet* est un espace de libertés.

« *Freedom is good* »

Dans le livre de Steven Levy « *hackers : Heroes of the computer revolution* » (1984) l'auteur identifie dans ce qu'il nomme « l'éthique *hacker* » et qui structure l'idéologie du mouvement à ses débuts. Celle-ci se compose d'un certain nombre de prérogatives que voici :

- L'accès aux ordinateurs, ou n'importe quelle autre ressource informationnelle permettant une meilleure compréhension du monde devrait être totale et illimitée.
- Toujours privilégier la pratique à la théorie.
- Toute information devrait être libre.
- Les *hackers* devraient se méfier de l'autorité et promouvoir la décentralisation.
- Les *hackers* doivent être jugés par leurs compétences non par des critères comme le diplôme, l'âge, la race ou le statut social.
- On peut créer la beauté et l'art via un ordinateur.
- Les ordinateurs peuvent changer votre vie de manière positive.

L'auteur suggère dans son travail, que les principes de cette « éthique *hacker* » restent constants dans le temps et subissent peu de changements. Cette affirmation appuyée par d'autres auteurs (Capron, Jamieson, McCaghy, 1999) font en effet ressortir un certain nombre de similitudes avec les principes vus par Levy. Ces travaux indiquent que, « bien qu'il puisse y avoir des différences entre les multiples "types" de *hackers* (par exemple, les « script kiddies⁴⁵ », les « *crackers* » etc), l'accumulation de connaissances, la liberté et le partage d'informations restent des règles unanimement partagées par toutes les communautés. » (p.337).

C'est donc sans surprise que nous retrouvons ces mêmes éléments dans notre étude et que nous développerons dans cette partie. Dans notre étude de cas, la mise en visibilité de ce principe de liberté se traduit sous plusieurs formes dont le partage d'expériences de *hacking*, de tutoriels ou d'entraide de manière générale constituent les éléments principaux. Le format du forum en ligne met à disposition de ces visiteurs, l'ensemble de l'historique conversationnel⁴⁶ ayant eu lieu entre ses membres, et ces derniers peuvent ainsi y accéder par la fonction de recherche disponible. A l'image d'un forum public dont les archives seraient disponibles à tous-tes, le forum en ligne se veut être le

45 Script kiddie est un terme péjoratif d'origine anglaise désignant les néophytes qui, dépourvus des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou programmes mis au point par d'autres. (Wikipédia)

46 Exit les conversations privées évidemment.

dispositif idéal à la diffusion d'informations. La permanence de ces dernières permet une accumulation et un archivage au fil du temps propre aux forums en ligne et qu'un dispositif de chat ne pourrait permettre. Il n'est donc pas surprenant de voir que le forum en ligne constitue sur le réseau Tor, comme sur le *clearweb*, le portail privilégié de partage et d'échange collaboratif de savoirs.

Sur les forums en ligne du *clearweb* où se retrouvent les différentes communautés de *hackers* pour discuter et partager leurs savoirs et savoir-faire, il est tout à fait commun de voir (ou plutôt de ne pas voir) que la question de la légalité est souvent évitée par ces utilisateurs. Lorsqu'un internaute demande de l'aide pour cracker un mot de passe, un réseau Wifi ou un protocole de sécurité par exemple, il ne mentionnera pas si l'intrusion est illégal ou non. Car si tel était le cas, ses chances de recevoir une réponse seront amoindries et l'internaute prendra même le risque d'être sanctionné par la modération. Il en va ainsi de sa responsabilité légale du modérateur de gérer son site dans la légalité. En intégrant des dispositifs d'anonymisation, la question légale autour du partage d'informations sur le réseau Tor se retrouve non pas contournée comme sur le *clearweb* mais au contraire affrontée et affichée. Les communautés des *darknets* se voulant libres au regard de la loi n'auront elles aucun problème à aborder la question de l'illégalité de certaines pratiques dans leur communauté ni à partager les informations nécessaires au passage à l'acte.

Ainsi, cette liberté d'information partagée par toutes les communautés de *hackers* se voit soustraite à un ensemble de contraintes légales annihilées par les capacités techniques offertes les *darknets*. Au-delà du règlement interne des communautés qui bannissent certains contenus (la pédopornographie et le commerce pour l'exemple du « DeepNetwork »), la majorité des informations restent libres d'accès et libres d'être partagées par leurs membres.

Cette liberté de partager du contenu sans contraintes peut même parfois entrer en contradiction avec les intérêts de certains *hackers* du réseau qui tirent bénéfice de certaines failles.

« -Membre : Amazon entre 500 et 800 dépôts de plaintes, ça a bien changé...je suis pour la suppression du topic car sinon dans un an on ne pourra plus faire.

-Modérateur : le forum a été crée dans le but de fournir un espace d'échange sans censure. Ce post ne sera pas supprimé. Inutile de demander »

Conversation extraite du forum

Dans cette réponse, nous voyons un exemple typique de conflit d'intérêts dans cette pratique du partage où l'intérêt de certains internautes passent après la liberté de circulation des savoirs. Cette

liberté de publication de contenus s'assimile dans notre cas d'étude, et selon les propos des utilisateurs de la communauté, à une forme plus globale formulée sous la forme de **liberté d'expression**. En effet, dans notre étude de cas, être libre de s'exprimer, c'est avoir aussi la liberté de partager tout type d'informations. Cette règle centrale, aux frontières poreuses, intègre pour la communauté que nous étudions, le concept d'expression en lui-même et le formule d'un angle libertaire. Ce n'est pas juste la liberté d'exprimer une opinion ou une appartenance sans peur de représailles mais c'est l'entièreté de l'acte d'expression qui est défendu. Celui-ci se veut sans censure et la seule limite étant le respect du code interne de la communauté. Au delà du règlement interne propre à chaque groupe, la liberté d'expression peu être totale et le respect de celle-ci, devient un élément « pilier » du groupe.

Ainsi, les seules limites à l'expression sont ce qu'interdit le règlement en vigueur propre à chaque communauté du *darknet*. Dans notre étude, le fait de juger ou de dénigrer une personne sur des caractéristiques relevant de la sphère privée (religion, genre, sexe, ethnie etc) est proscrit et peut aller jusqu'au bannissement. Ce règlement prône de manière générale, une tolérance assez large vis-à-vis de la déviance -plus affichée que sur le *clearweb* pour les raisons d'anonymat- et instaure une cohabitation mutuelle s'élaborant sur le respect des libertés de chacun.

Sur le *darknet*, la notion de liberté prend un sens qu'on qualifierait ici de libertaire. Défaite des contraintes légales inhérentes au web « conventionnel » mais régies par le règlement interne des communautés, cette dernière permet l'acte d'expression, dans un sens plus large que ce que nous avons l'habitude de voir au quotidien. Elle dépasse la frontière de la liberté d'opinion et englobe à la fois, la liberté de partage de contenu chère aux communautés *hackers* ainsi que la liberté d'expression de la déviance.

« -hacker à temps partiel, je vis dans le nord et je bosse dans l'informatique, je crois au pouvoir de la connaissance et au web libre. » (Fred)

Principe n°2 : L'assistanat est proscrit, soyez autodidacte.

« No problem should ever have to be solved twice »

Un des grands fondements de l'éthique *hacker* qui se transpose sur le *darknet* est celle de l'autonomie des utilisateurs quant à leur apprentissage. En effet, un grand nombre d'internautes considèrent que leur temps est une ressource précieuse qui ne devrait en aucun cas être gaspillée pour répondre à des problèmes déjà résolus auparavant.

« Pour se comporter comme un hacker, vous devez vous dire que le temps de réflexion des autres hackers est précieux - à tel point que c'est presque un devoir moral pour vous de partager des informations, de résoudre des problèmes et de partager ces solutions pour que d'autres hackers n'est pas à perpétuellement revenir dessus. » (Raymond, 2002)

Ce mode de fonctionnement axé sur l'économie de temps et l'efficacité collective appelle directement les utilisateurs à rechercher activement une solution ou une information avant de demander de l'aide à une communauté de *hacker*. En effet, l'usage des *hackers* étant de partager systématiquement les solutions et informations utiles à leur communauté, ils demandent en contrepartie à cette dernière de ne pas les solliciter inutilement. Sur le « DeepNetwork » par exemple, et comme nous l'avons vu précédemment, les posts destinés aux novices et à la recherche d'information sont extrêmement présents et sont placés de manière à être trouvés et lus facilement. Cet appel à l'autonomie par l'abondance « des liens utiles » suit une logique très présente dans notre communauté et qui est celle de la proscription de l'assistanat. Cette règle, suivie de manière stricte, est systématiquement sanctionnée en cas de manquement par utilisateurs et administrateurs confondus. Elle sert une double fonction dans la communauté : le filtrage des nouveaux membres et l'accroissement de l'efficacité du partage d'informations. Elle permet à la fois d'éviter l'encombrement des *topics* par des questions ou problèmes déjà abordés, tout en donnant un cadre interactionnel commun, permettant aux internautes d'interagir plus efficacement.

Membre : - « Bonjour, je me suis demandé aujourd'hui si il existait d'autres plantes pour remplacer le tabac à rouler (...) avez vous des trucs à me conseiller ? »

Admin : - « Bonjour, je lock pour assistanat. PS : si tu trouves ça injuste ou que tu ne comprends pas, je t'invite à en débattre ici (lien renvoyant vers une section abordant les règles de modérations)».

Conversation extraite du forum

Ainsi la coprésence entre abondance de règles pour guider les débutants et proscription de l'assistantat, est pour nous une logique de fonctionnement héritée de l'éthique *hacker* (Himanen, 2002). A l'image des communautés épistémiques (Morgan, Susan, 2011), ce mode de fonctionnement permet au groupe de progresser collectivement sur des sujets techniques en évitant de perdre du temps sur des questions triviales ou déjà traitées. L'application de cette règle impose donc aux internautes une certaine « maturité » et un certain nombre de compétences leur permettant par exemple d'utiliser avec justesse, différents moteurs de recherche, forums ou autre ressources numériques avant de demander de l'aide.

Bonjour à tous.

Comme vous l'avez peut-être remarqué ,depuis que je suis modo, je lock pas mal de sujet de façon un peu arbitraire (en me fiant uniquement à mon jugement).

Je ne suis pas quelqu'un de tyrannique, au contraire, je suis assez ouvert aux suggestion des autres, je me suis simplement fixé des règles de modérations qui sont les suivantes :

- mise à la corbeille de tout sujet incompréhensible ou dans une autre langue (ça c'est normal, c'est du bon sens)
- mise à la corbeille de tout sujet ne respectant pas les règles du forum (pédo & xéno, ça aussi c'est normal, on s'en fout)
- mise à la corbeille de tout sujet **qui est une demande d'aide explicite pour obtenir des info trouvable par sois-même** (c'est de ça que j'aimerais débattre)

exemple a écrit :
"kmen on hak facbok"

<corbeille direct + réponse méchante

exemple a écrit :
"bonjour, ou on achete des ccv svp merci"

<corbeille + réponse avec remontrance + éventuellement (rarement) un [lien](#)

exemple a écrit :
"Bonjour, je souhaiterais commencer dans le hacking, pouvez-vous me donner des liens ?"

<corbeille + réponse avec souvent un lien

exemple a écrit :
"Bonjour, je recherche activement un moyen de convertir de l'argent sur un compte paypal ou autre en BTC, sauriez-vous ou trouver ça? j'ai essayé virvow mais je trouve que c'est un peu une arnaque"

<corbeille + réponse en disant que c'est une question déjà posée + [lien](#)

Illustration 3: Exemple de conversation traitant des règles de modération

Dans une communauté sans sélection à l'entrée comme l'est le forum « DeepNetwork », faire perdurer cette règle de non assistanat impose à la modération d'agir de manière stricte et systématique. Les nouveaux membres voulant intégrer la communauté étant assez nombreux et les membres novices plus nombreux que les membres anciens, le risque de « débordement » reste très fréquent et la sanction en réponse, quasi systématique. Ces sanctions systématiques sont, sans surprise, une manière de préserver les normes du groupes par la mise au pas des membres novices et préserver ainsi une certaine cohésion. Par la suite, les membres novices qui auront acquis l'expérience nécessaire, rejoindront ou prendront la place des anciens et se chargeront de rappeler les règles aux novices.

Héritée de l'éthique scientifique, transposée à l'éthique *hacker* et enfin exacerbée sur le *darknet*, cette problématique d'autodidaxie et de l'efficacité de la transmission d'informations s'inscrit dans les principes structurant de la subculture *darknet*. Les différents sous-groupes appliquent ainsi cette règle avec plus ou moins de rigueur et font perdurer cette norme du *darknet* :

Mathieu : - *Olivier* est dur avec les noobs mais franchement je le comprends...t'imagines tu gère un forum et t'as tous les jours les mêmes questions de merde alors que la réponse est dispo dans les threads ? Il suffit de chercher 10 secondes. En plus y a des posts pour débutants partout dans le forum. Ils ont pas d'excuses pour pas respecter les règles.*

Moi : - *Peu être que sur le clear c'est plus flexible à ce niveau, ils ont peut être pris l'habitude de ça ?*

Mathieu :« - *Ben oui tu vois bien comment ça se passe sur ces forums des fois, c'est le bordel. C'est pour ça que certains se tirent*»

Moi:« -*C'est pour ça que t'es allé sur DeepNetwork toi? »*

Mathieu :« - *Ça a joué je pense, pour certains trucs c'est plus efficace, et puis ça file droit. Tu poses une question et dans la majorité des cas tu as une vraie réponse, pas un truc approximatif*»

**nom du modérateur anonymisé*

Principe n°3 : Le *darknet* peut se montrer impitoyable.

« *Anonymous can be a horrible, senseless, uncaring monster* »

Pour les internautes du forum, le *darknet* est vu comme un espace disposant de libertés quasi infinies mais qui peut parfois se montrer impitoyable envers celles et ceux qui n'en sont pas avertis. L'anonymat et la sécurité permis par le réseau a en effet attiré un certain nombre de pratiques illégales au sein du réseau Tor. Les spécificités techniques qui rendent difficiles l'identification et la régulation⁴⁷ de pratiques frauduleuses comme le commerce de stupéfiants par exemple, soumettent les acheteurs à un grand nombre d'arnaques et « d'exit scams »⁴⁸. Au delà de l'aspect purement commercial, les nouveaux utilisateurs sont invités à se munir de prudence quand ils décident de naviguer sur un *darknet*. Certains contenus liés à certaines formes de déviances peuvent se montrer choquantes pour des internautes non avertis et la recherche de ce type de contenus doit selon les utilisateurs confirmés se faire en connaissance de cause.

« *Comprendre avant d'agir : réfléchissez avant de poster, avant d'acheter, avant de regarder du CP ou de faire n'importe quoi (...) n'oubliez pas que si c'est trop beau pour y croire c'est que c'est trop beau pour être vrai et qu'il existe toujours plus horrible* »

Extrait du guide du débutant.

Grâce aux spécifications techniques du *darknet*, la poursuite en justice de pratiques illégales ou criminelles devient une tâche difficile pour les autorités (Buxton, Bingham, 2015). Les internautes sont en quelque sorte « livrés » à eux-mêmes et doivent redoubler de prudence si ils décident de s'adonner à des pratiques illégales sur le réseau. Cette prudence passe par un apprentissage des règles élémentaires de sécurité sur le réseau et qui implique une reconfiguration des pratiques de navigations habituelles. Comme l'explique un enquêté :

Fred : - « *les pièges sont nombreux sur le darknet, il faut être prudent* ».

Moi : « *c'est à dire ?* »

Fred : « *ben il faut faire gaffe quand tu télécharge quelque chose ou pire si tu achète quelque chose sur le deep. Y a des arnaques partout et faut bien vérifier que y a pas un virus dans ce que t'as téléchargé ou que tu ne file pas ton argent comme ça. Être sûr que ton vendeur est fiable quoi.* »

47 Un système de tiers de confiance est souvent utilisé pour sécuriser les transactions mais ne garanti jamais à 100 % la fiabilité du vendeur ou de l'acheteur.

48 L'exit scam est une pratique qui consiste pour un vendeur, de stopper son activité tout en continuant à encaisser les achats avant de disparaître de la place de marché. Un tiers de confiance remédie souvent a ce problème.

Moi : - « et comment tu fais pour ça ? »

Fred : « - déjà les virus c'est simple, tu déconnecte internet, tu scanne ton fichier, et tu l'ouvres. Si c'est clean tu peux te reconnecter. Si tu veux acheter sur le deep moi je conseille d'éviter les autoshops, c'est un piège à noobs et tu ne reverras jamais ton argent. Il faut tout le temps passer par des escrow ».

Étant un espace exclusivement régulé de manière locale via une modération propre à chaque communauté, un certain nombre d'utilisateurs peu scrupuleux du réseau Tor ouvrent des sites exclusivement portés sur l'arnaque d'utilisateurs novices. Ces sites appelés « *auto-shops* », contrairement aux *market places*, sont des sites particuliers qui ne disposent souvent pas de tiers de confiance (*escrow*) pour s'assurer de la bonne tenue des transactions entre acheteur et vendeur. Le plus souvent les *auto-shops* sont les sites d'achat de faux billets, de faux papiers ou encore de téléphones portables. Mais l'exemple le plus connu d'escroquerie qui suscitent souvent un certain fantasme à l'extérieur des *darknets* sont les services de tueurs à gages et autres « *redrooms* ⁴⁹ ». Ces services relevant plus de la légende urbaine que de réels services financiers, sont souvent démentis par les membres expérimentés du réseau et sont désignés comme étant des arnaques grotesques destinées aux journalistes peu méticuleux ou aux novices en recherche de sensationnel. Ainsi la reconfiguration des pratiques de navigation des débutants sur le réseau passe par une lecture méthodique des conversations des autres membres et du croisement d'informations quant à la fiabilité de certains services financiers. Les pratiques de téléchargement sur les *darknets* se voient aussi reconfigurées par les utilisateurs du réseau. En effet, ces espaces étant occupés par une multitude de *crackers*, le piratage et le *hacking* d'autres utilisateurs sont monnaie courante et passent souvent par l'infection volontaire de fichiers disponibles au téléchargement. Pour pallier ce problème, plusieurs utilisateurs, comme l'enquêté « Fred » plus haut, recommande fortement d'utiliser un système d'exploitation plus sécurisé sur leur machine (Linux) et de déconnecter cette dernière d'internet en cas d'ouverture de fichiers téléchargés.

Le *darknet* peut être ainsi analysé comme un espace libertaire très peu soumis aux contraintes légales appliquées au web conventionnel. Parfois désigné comme le « *wildwest* de l'internet »⁵⁰, il invite ses internautes à une utilisation consciente et avertie du contenu disponible. Ces préconisations se traduisent par une auto-régulation de ses pratiques de navigation ainsi que l'apprentissage et l'application des règles implicites du *darknet*.

49 Il s'agit d'un site web ou d'un service caché sur le Deep Web où les internautes ont la possibilité de voir et / ou de participer -contre rémunération- à une torture interactive ou un meurtre filmé en direct.

50 <https://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022>

Par le caractère élitiste que peut constituer ce genre de réseau (Gehl, 2016), l'amateurisme est souvent dénigré et les attendus en terme de compétences sont souvent élevés pour une majorité d'utilisateurs provenant du *clearweb*. Comme nous l'avons vu dans la partie sur le principe de proscription de l'assistantat, le dénigrement de la figure de l'amateur non averti est monnaie courante dans plusieurs communautés. Certains administrateurs n'hésitent pas à user de propos humiliants pour qualifier le manque de compétences de certains novices et les réactions peuvent être parfois violentes.

"-Administrateur : Tu vas pas faire long feu ici si tu continue a poser des questions de merde comme ça."

Cette démarche d'incivilité, corrélée au niveau de gravité estimé par les plus qualifiés ou les plus anciens, s'apparente pour nous à une forme dressage des conduites par les brimades. A l'image d'une forme de bizutage en ligne, cette pratique permet de faire appliquer les normes de la communauté tout en faisant accepter une certaine forme de violence routinière ayant cours dans plusieurs communautés anonymes sur internet.

Principe n°4 : Le *darknet* est politique.

« Les objets techniques définissent dans leur configuration une certaine partition du monde physique et social, attribuent des rôles à certains types d'acteurs - humains et non-humains - en excluent d'autres, autorisent certains modes de relation entre ces différents acteurs etc... de telle sorte qu'ils participent pleinement de la construction d'une culture, au sens anthropologique du terme » Madelaine Akrish

Dans les précédents chapitres nous avons montré l'importance que peut avoir l'utilisation d'outils cryptographiques dans ce réseau pour certains utilisateurs du *darknet*. Mais au-delà d'une utilisation utilitariste de ces outils, le discours des acteurs en font émerger une utilisation revendicative et politique de ces « objets » numériques. Pour certains auteurs, le *darknet* est indissociable d'un certain nombre d'objets techniques qui mettent en cohérence les bases idéologiques de ce cyberspace (Rennard, 2016) et qui ont trait selon eux à un **libertarisme politique et financier**. Revendiquer l'importance de la vie privée sur internet, la non traçabilité des échanges numériques et vouloir échapper à la surveillance de masse sont, selon nos analyses, un ensemble de revendications à la fois partagées par les utilisateurs des *darknets* mais aussi par des grands acteurs du monde *hackers* tels que l'EFF fondation aux États-Unis ou la « Quadrature du net » en France. L'aspect politique autour de l'utilisation des *darknets* et de ses outils est un élément auquel il est difficile d'échapper lorsque l'on se connecte sur ces réseaux. En effet les sites politiques sont nombreux et les appels à la dévalorisation des institutions étatiques et des GAFAM sont récurrents :

« Pour moi le Deepweb c'est internet sans l'État, sans les lois et tout ce qui va avec. Et c'est ça qui rend cet endroit unique. C'est plus eux qui fixe les règles... » (Bob)

L'arbitraire de la morale étatique est souvent mise en cause au profit d'un univers digitale auto-régulé par les internautes eux mêmes et hors de toute traçabilité. Ce désir d'autonomie et de repli autarcique amène les internautes les plus motivés à intégrer, dans leur usage des *darknets*, toujours plus d'outils pour mener à bien cette quête de la protection et de l'anonymat numérique. Les failles de sécurité et d'anonymat (qu'elles soient dans ou en dehors des *darknets*) ne cessent d'être investiguées et les solutions sont assez rapidement partagées à l'intérieur des communautés.

Pour beaucoup, les GAFAM⁵¹représentent une force pesante sur le fonctionnement d'internet et les *darknets* sont des réseaux où cet oligopole est absent (Smyrnaio, 2017). Ces utilisateurs s'opposent ainsi à la dérive de la massification d'usage d'internet par le fait qu'ils se sont sentis au fil des années, dépossédés du réseau par ces mêmes GAFAM. Ainsi, les outils proposés par ces géants du web (moteurs de recherche, messageries, système d'exploitation etc) sont dénigrés et remplacés par leur équivalent compatible avec « l'état d'esprit » (Rennard, 2016) de ces réseaux.

Les *darknets* et plus particulièrement le réseau Tor, est indissociable de sa capacité à avoir créé et alimenté depuis ses débuts, un marché noir parallèle en dehors du carcan des états et des multinationales. L'utilisation des cryptomonnaies sont en effet légion et en deviennent un élément indivisible de la subculture portée par ces espaces. L'intégralité des échanges marchands se font grâce aux cryptomonnaies et ne passent que très peu par les systèmes bancaires classiques :

« Les crypto c'est l'avenir. Plus besoin de banques ni d'états pour contrôler et surveiller ton argent. T'en fais ce que tu veux, il est à toi ! » (Camille)

En effet la technologie de la *blockchain*⁵² qui est au cœur du modèle de fonctionnement décentralisé des cryptomonnaies a très vite trouvé des adeptes et défenseurs au sein des *darknets* et a rapidement été utilisée pour accroître le commerce dans ces espaces. Ces monnaies alternatives, entrent en cohérence avec ce libéralisme politique et financier défendu par des grandes figures et pionniers du commerce sur le *darknet* tel que Ross Ulbricht. Créateur du site « the silkroad », ce dernier a été condamné à la prison à perpétuité après son arrestation en 2013. Il fait l'objet jusqu'aujourd'hui de multiples soutiens de la part des communautés du *darknet*. Considéré pour beaucoup comme un idéaliste tentant de réaliser un rêve libertaire sur internet, la lourdeur de sa condamnation est vue comme injuste et disproportionnée au regard des faits.

En effet, les conditions techniques des *darknets* permettent selon nous une application et le dévoilement d'un certain idéal politique, dépourvu de surveillance et régulé par les propres acteurs du réseau. La formation des communautés des *darknets* et de leur subculture peuvent être analysées comme une sorte de repli digitale, un isolement volontaire en réaction au contrôle toujours plus étendu d'internet par les gouvernements et les multinationales du web. Ainsi cette vision pessimiste du monde numérique telle qu'elle est pensée par les acteurs du réseau, amène à légitimer à la fois l'existence de ces espaces mais aussi de la subculture qu'ils portent.

51 Google, Amazon, Facebook, Apple, Microsoft

52 Technologie de stockage et de transmission d'informations sans organe de contrôle.

Par leurs pratiques et leurs discours, les acteurs de cette subculture font un usage politique d'outils techniques. Ils transposent une vision politique libertaire à un espace numérique libéré des contraintes légales.

V / Transgression et cybercriminalité.

A) Situer la cybercriminalité dans les *darknets*

Comme nous l'avons vu dans le mémoire précédent, la communauté étudiée impose son propre mode de fonctionnement et propose une remise en question de la normativité sociale vue comme étant arbitraire. A l'image des travaux entrepris sur la formation d'actes criminels (Sutherland, 1924), le processus d'interprétation des dispositions légales par les individus d'un groupe ou d'une subculture se voit modifié comme dans le cas de la subculture *darknet*. Par la remise en cause de la légitimité des normes de justice établies, ce processus d'invalidation des normes peut amener ces derniers à adopter une posture transgressive ou potentiellement illégale (Becker, Sutherland, Goffman). Même si l'objectif de ce travail n'est pas d'analyser la formation de réseau criminel au sein du réseau Tor, certains aspects des recherches entreprises par la sociologie de la criminalité peuvent nous apporter un point de vue éclairant sur la facette transgressive de ces subcultures. Dans les travaux d'Edwin Sutherland (1883-1950), l'auteur élabore une définition de la criminalité dont certains points peuvent nous intéresser . Cette théorie comporte neuf points et se divise comme suit :

- Le comportement criminel est appris, autrement dit, il n'est pas héréditaire ;
- Le comportement criminel est appris au contact d'autres personnes par un processus de communication.
- Il s'apprend surtout à l'intérieur d'un groupe restreint de relations personnelles, ce qui minimise l'influence de journaux ou du cinéma ;
- Lorsque la formation criminelle est apprise, elle comprend l'enseignement des techniques de commission de l'infraction et l'orientation des mobiles, des tendances impulsives, des raisonnements et des attitudes ;
- L'orientation de ces mobiles est tributaire de l'interprétation favorable ou défavorable des dispositions légales. Quand certains groupes sont respectueux des règles, d'autres ne cessent de les violer ;
- Un individu devient criminel **lorsque les interprétations défavorables au respect de la loi l'emportent sur les interprétations favorables**. C'est ce qui constitue le principe de l'association : on devient criminel parce que l'on s'associe à des modèles criminels sans avoir sous les yeux des

modèles contraires. Chaque individu apprend la culture de son milieu environnant et ce d'autant plus qu'il n'a pas de modèle de comparaison ;

- Ces associations sont différentielles parce qu'elles peuvent varier en fréquence, en durée, en intensité ;
- La formation criminelle met en jeu les mêmes mécanismes que tout autre formation ;
- Le comportement criminel est l'expression des mêmes besoins et des mêmes valeurs que le comportement non criminel.

Selon les points de cette définition, et par l'aspect communautaire et transgressif que peuvent prendre certains groupes présents sur le réseau Tor, le *darknet* présente selon nous, tout un ensemble de dispositions favorables à l'alimentation ou à la formation d'éventuels passages à l'acte illégale. L'évolution des internautes dans des communautés souvent exclusives et à la dissidence admise, peut amener les internautes à reconfigurer certains principes sociétaux tel que le bien-fondé des principes de légalité et de morale. A l'image des réseaux criminels « IRL⁵³ » où l'apprentissage de la posture et du comportement illégal passe par le contact et la communication avec d'autres membre du groupe (Sutherland, 1924), le *darknet*, de son côté, met en œuvre dans un environnement numérique, ces mêmes processus de partage, d'apprentissage et de reproduction d'actes déviants ou illégaux. Comme pour l'analyse de ces derniers par l'école de Chicago (Burgess, Shaw, Sutherland, Becker), la communauté étudiée dans ce mémoire amène à une remise en cause de la perception de la légalité et de morale vue comme arbitraire (Becker, 1963) . La reconfiguration de ces notions de justice et de légalité s'analyse au travers des théories de la criminalité comme un basculement interprétatif, de telle sorte que « lorsque les interprétations défavorables au respect de la loi l'emportent sur les interprétations favorables » (Sutherland, 1924), l'individu devient potentiellement criminel. Comme le précise l'auteur dans sa définition, la formation d'actes délinquants ou criminels s'élabore par transmission d'informations entre les membres d'un groupe ou d'un réseau. Un processus de formation qui, sur les *darknets*, s'établit majoritairement par le partage d'informations et d'expériences liées à des actes illégaux. Cette démarche informative entreprise par une subculture n'est pas sans rappeler les analyses de Richard Cloward et Lloyd Ohlin (1960) sur la formation d'une subculture criminelle, notamment dans sa démarche de formation de ses nouveaux membres : les anciens initient les nouveaux venus et leurs apportent techniques et conseils lors de passages à des actes illégaux.

53 Acronyme de « In real life », c'est-à-dire hors du monde numérique.

B) Une subculture basée sur la transgression.

Même si plusieurs points peuvent rapprocher la subculture *darknet* d'une subculture criminelle, celle-ci diffère des analyses par Cloward et Ohlin dans sa capacité à être centrée non pas sur l'acte criminel et la recherche de profit ou l'inscription dans une carrière criminelle mais sur **l'aspect transgressif en lui-même**. Ainsi, la transgression des considérations légales et morales permettent à des membres aux visées très différentes de partager un même espace sans que leurs intérêts respectifs ne soient en concurrence. Au contraire, chaque profil d'utilisateur (*cracker*, *hacker*, *cardeur*, activiste ou simple curieux) apporte à la communauté un ensemble d'informations relatives à leur intérêts et c'est l'ensemble du groupe qui peut profiter de cet élargissement des connaissances. Ainsi l'hétérogénéité des membres de certaines communautés comme celle que nous étudions, est due à cette abondance d'informations disponibles dont ces membres peuvent profiter librement et dont les seules contraintes sont les règles internes à chaque groupe.

Moi : - « *Est ce que tu peux me dire pourquoi tu vas sur le darknet ?* »

Bob : - « *La plupart du temps c'est pour trouver des choses que je ne trouve pas sur le clear. Ça peut être pour des tutos, du bidouillage ou juste pour discuter, partager.* »

Moi : - « *Ces choses ne sont pas possibles en dehors du darknet?* »

Bob : - « *Si c'est possible, mais c'est plus compliqué, le clear est trop surveillé maintenant, déjà tu ne peux plus rien faire sans être tracé, et en plus y a toujours quelqu'un pour venir te faire chier en te disant : ah ça c'est pas bien, ça c'est illégal etc. Ici au moins on ne vient pas faire son moralisateur sous prétexte qu'on se pense être dans le camps des gentils. Chacun se mêle de ses affaires quoi* ».

Le passage à des actes illégaux ne représente pas un objectif commun structurant des *darknets* mais c'est la liberté de partager et de consulter sans contraintes des informations qui elles, sont au cœur de la formation des communautés du réseau. C'est donc un ensemble d'individus qui cohabitent mutuellement sous une forme large de transgression des normes sociales. La cybercriminalité est évidemment présente sur le réseau et il est entendu que plusieurs individus peuvent s'associer dans ce but mais cet objectif ne représente pas selon nos analyses le principe unificateur de cette subculture. Malgré cette liberté prise au regard de la loi⁵⁴, les communautés du *darknet*, comme celle du « DeepNetwork », sont tout de même conscientes des implications judiciaires que peuvent prendre certaines de leurs pratiques. Car comme pour les posts définissant les règles et usages de la communauté, plusieurs informations sont à la disposition des utilisateurs pour comprendre les

54 La loi interdit la diffusion d'informations susceptibles d'inciter à commettre des actes illégaux.

conséquences légales de certaines pratiques comme le *cracking*, le commerce illégal ou simplement la navigation sur un *darknet*⁵⁵.

« *hackers, cardeurs, crackers, preux défenseurs de la liberté d'expression, whistleblowers ou escrocs cupides, votre art est informatique et vous déployez moult efforts pour vous rendre intraçables. Mais imaginons que vous fassiez suffisamment de bordel pour que la cybercim' s'intéresse à vous et vous tombe sur le coin de la mouille.* »

Tiré de l'entête d'un post recensant les textes de lois relatifs à la cybercriminalité.

Il n'est pas surprenant de s'apercevoir qu'une communauté basée sur le partage d'informations développe aussi en son sein l'initiative d'informer ses utilisateurs des conséquences légales de certaines pratiques sur le réseau. Les sections relatives au *cracking* étant populaires, cette démarche informative se situe pour nous, sur continuum d'enrichissement des connaissances des membres de la communauté. Du point de vue de la formation criminelle, ces informations peuvent être comprises comme faisant partie du processus d'apprentissage de la posture criminelle ou délinquante.

Par la récurrence des affaires judiciaires⁵⁶ concernant certaines activités du réseau, la cybercriminalité est un élément indissociable de l'univers des *darknets*. Pour autant, ces derniers n'en constituent pas l'unique élément structurant des communautés qui s'y trouvent. Par leurs capacités à anonymiser et à sécuriser les connexions de leurs internautes, ces réseaux abritent de fait un certain nombre d'activités illégales facilitées par ces dispositifs. Pour autant les logiques mises en œuvre dans des subcultures criminelles différent de celles des *darknets* dans leur rapports à la production d'informations. **Dans l'une, ces informations sont cruciales pour alimenter et faire perdurer l'activité criminelle, dans l'autre, elle ne sont qu'un élément informationnel parmi d'autres.** Dans les paragraphes précédents, nous avons vusque l'aspect transgressif par le libre partage d'informations étaient au cœur des pratiques structurantes du *darknet*. C'est davantage sur son aptitude à offrir un espace de libertés individuelles et informationnelles sans entraves que sur sa capacité à construire des carrières criminelles ou déviantes que le réseau se structure. Malgré les similitudes avec la formation criminelle, la subculture *darknet* doit être pensée sur une échelle et un positionnement différent de cette dernière. Les profils criminels sont bel et bien existants sur le

55 La navigation sur un *darknet* est légale.

56 Nous faisons référence ici au site « the silk road » mais encore plus récemment à la saisie du site français « la main noire » et l'arrestation de certains de ses membres.

réseau mais ne sont qu'un élément (difficilement mesurable au vu des contraintes de ce mémoire) parmi un ensemble de portraits (bidouilleurs, hacktivistes, curieux etc) qui se nourrissent et alimentent à leur tour le réseau en informations diverses. Ces typologies d'utilisateurs doivent être pensées comme des éléments profitant des aspects transgressifs qu'offrent les communautés de partage des *darknets* plus qu'elles n'en constituent, individuellement, l'élément structurant sa logique. Le *darknet* correspond ainsi davantage à une subculture basée sur la transgression au sens large qu'une subculture criminelle dans sa forme numérique.

V/ Conclusion.

Encore aujourd'hui, l'univers des darknets reste un sujet trop méconnu des sciences sociales. Le fait que ces réseaux soient relativement récents en font un sujet d'étude pluriel et ouvert aux recherches. Un atout majeur aujourd'hui en sociologie et dont on peut tirer un intérêt et un enrichissement intellectuel considérable.

Nous avons développé dans ce projet de recherche une problématique et des axes d'analyses qui nous ont permis d'aborder une partie de ce que ces vastes réseaux peuvent nous révéler. Nous avons tenté au travers de nos réflexions et analyses d'ouvrir ce sujet en répondant à plusieurs questions : Qu'est ce sont que ces réseaux ? Comment fonctionnent t-ils ? Mais surtout, comment les pratiques et les discours de ses internautes peuvent être le vecteur d'une idéologie propre à une subculture particulière : celle des *darknets* ?

Pour répondre à ces questions, nous avons dans un premier temps focalisé notre attention sur l'histoire du mouvement *hacker* auquel cette subculture se rattache. Cette mise en contexte nous a permis d'intégrer notre recherche dans un continuum historique auquel la mutation de notre société toujours plus digitalisée a joué un rôle prédominant dans l'évolution de ces mouvements *hackers*. Cette partie nous a permis de comprendre en quoi l'adhésion de certains internautes aux *darknets* depuis le début des années 2000 traduit en réalité la cristallisation d'une certaine angoisse sécuritaire et financière liée au contrôle croissant d'internet par certains acteurs comme l'État et les entreprises. Nous avons ensuite abordé l'aspect technique de ces réseaux pour permettre à nos lecteurs de dissiper certaines incompréhensions ou doutes quant au fonctionnement des ces réseau et aux termes utilisés pour les qualifier. Concernant ce dernier point, les appellations *deepweb*, *darkweb* ou *darknet-s* sont souvent confuses, s'entremêlent et rendent plus difficile l'appréhension de ces réseaux. Comme nos lecteurs l'ont peut être ainsi remarqué, nous avons choisi dans cette recherche de ne pas utiliser l'appellation *darkweb* et ce pour deux raisons principales. La première étant que cette appellation ne qualifie pas pour nous un espace numérique mais deux simultanément : les *darknets* et le *deepweb*. La deuxième raison de ce choix étant que nous avons volontairement voulu identifier et distinguer ces deux espaces au travers de la portée politique et idéologique qui les traversent : portée quasi inexistante pour le *deepweb* qui ne constitue que

l'ensemble du web inaccessible aux moteurs de recherches mais présente dans les *darknets* qui sont le fruit de l'isolement volontaire d'une partie du réseau internet par leurs créateurs.

Entreprendre l'analyse des *darknets* en délimitant notre ethnographie à une communauté en particulier nous a permis de border notre terrain et de se focaliser sur les phénomènes sociaux émergeant dans ce groupe. La focale interactionniste adoptée pour mettre à bien cette recherche nous a montré comment les individus se construisent au travers de leurs relations avec leurs environnement et comment ils alimentent à leur tour un système de valeurs construit collectivement. Au-delà des échanges commerciaux non régulés et du besoin de préserver son anonymat dans une communauté élitiste, c'est tout un phénomène culturel qui se joue dans ces espaces. Une subculture basée sur la transgression et qui se dote d'une idéologie propre, de systèmes normatifs et d'un argot spécifique à leurs membres. Au-delà des normes et valeurs partagées par les groupes à une échelle locale, ces groupes partagent un certain nombre de traits culturels communs à l'univers des *darknets*.

Liée au mouvement *hacker* dont on peut remonter la source aux pionniers du réseau Internet, la subculture des *darknets* en devient une de ces ramifications et développe en son sein un certain nombre de traits spécifiques à l'espace dont elle dépend. L'anonymat devient une force normative puissante et amène les internautes à repenser leurs interactions jusqu'à dans leur mise en scène de soi et questionnent pour nous chercheurs, l'importance du secret dans la formation des relations sociales. L'anonymat et le secret permettent ainsi aux individus *d'échapper au contrôle des autres et devient un facteur de différenciation entre les individus* (Simmel, 1991). Dans ces communautés, cette différenciation se déploie et se dirige autant vers l'intérieur du réseau, au travers d'une distinction élitiste véhiculée par certains membres que vers l'extérieur à travers une affirmation identitaire liée -entre autre- aux valeurs d'anonymats spécifiques aux *darknets*. Questionner la place de l'espace social⁵⁷ dans la formation des groupes subculturels a permis de mettre en avant l'importance identitaire que ces derniers constituent pour ces groupes. Même numériquement, les individus s'approprient l'espace, créent, adoptent et véhiculent des valeurs qui vont au-delà de leur communauté d'appartenance. L'élitisme, le libertarisme, la subversion de la morale et l'anonymat sont autant de traits caractéristiques de la communauté que nous avons étudié tout au long de ce travail de recherche et qui nous pensons, dépasse la frontière de leur espace numérique pour alimenter une subculture *darknet* transnationale.

57 Entendu comme des lieux délimités où se jouent des interactions entre individus.

L'ambition de ce travail de recherche était d'explorer et de comprendre un sujet vaste qui nous paraît trop peu étudié aujourd'hui. D'ouvrir ce sujet à la recherche et d'amener d'autres sociologues à investiguer et à analyser à leur tour ces espaces. Nous sommes conscients que des questions restent en suspend et que certaines parties de ce travail mériteraient un approfondissement et une étude parfois entièrement focalisée sur ces dernières. Toutefois, malgré les limites de ce travail et des possibilités analytiques, il en reste que nous pensons avoir proposé un début d'étude pertinent qui permet de penser plus largement l'appropriation de l'espace numérique par certaines franges de la population. Notre sujet permet de questionner la place et l'importance du numérique au sein des groupes considérés comme marginaux, extrêmes ou déviants et permet d'ouvrir à d'autres questionnements : Dans quelle mesure ces objets techniques modifient ou déplacent le secret vers des espaces digitaux et quelles sont les conséquences de ce déplacement ? Comment penser aujourd'hui la déviance, la délinquance ou la criminalité en intégrant le numérique dans sa globalité?

Bibliographie

- AKRICH. Madeleine. « Comment décrire les objets techniques ? » . Techniques et culture, Éditions de la Maison des sciences de l'homme 1987, pp.49-64
- ARBAUGH. J. Cyberdeviance. In C. H. McCaghy, T. A. Capron, & J. D. Jamieson (Eds.), 1999. Deviant behavior: Crime, conflict, and interest groups (Fifth ed.). (pp. 366~86). Toronto, ON: Allyn and Bacon.
- BERGMAN. Michael. *White Paper: The Deep Web: Surfacing Hidden Value*. Journal of Electronic Publishing. 2000 .
- BERRY. Vincent. Ethnographie sur Internet : rendre compte du « virtuel ». *Les Sciences de l'éducation - Pour l'Ère nouvelle*, vol. 45,(4). Consulté le 19 Juin 2017. URL : <https://www.cairn.info/revue-les-sciences-de-l-education-pour-l-ere-nouvelle-2012-4-page-35.htm>
- BEAUDOIN Valérie et Velkovska Julia. “Constitution d'un espace de communication sur Internet (forums, pages personnels, courrier électronique...)” *Réseaux*, volume 17, n°97, 1999. “ Internet, un nouveau mode de communication ? ” p. 121-177.
- BECKER. Howard, *Outsiders, Etudes de sociologie de la déviance* (trad. fr. J.-P. Briand, J.-M. Chapoulie), Paris, Métailié, 1985.
- BIDDLE Peter, ENGLAND Paul, PEJNADO Marcus et WILLMAN Bryan: *The Darknet and the Future of Content Distribution*. 2002
- BULOT . Thierry *Langue urbaine et identité*, L'Harmattan, 1999
- BUXTON. Julia et BINGHAM Tim. *The Rise and Challenge of Dark Net Drug Markets*, Swansea University, 2015 . Policy Brief.

- CARDON. Dominique. *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Paris, Seuil, La République des idées, 2015
- CASTELLS, Manuel. *La galaxie internet*. Paris : Fayard, 2001, 368 p.
- CLOWARD Richard A., OHLIN Lloyd E., 1960, *Delinquency and opportunity*, The Free Press.
- DAGIRAL. Éric, 2008, « Pirates, Hackers, Hacktivistes : déplacements et dilution de la frontière électronique », *Critique*, n°733-734, « Pirates ! », Ed. de Minuit, p. 480-495
- DAKOTA. Rudesil, CAVERLEE. James et SUI. Daniel, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*. In - Ohio State Public Law Working Paper No. 314 2015 .
- DURKHEIM. Emile, « Communauté et société selon Tönnies », *Sociologie* (En ligne), N°2, vol. 4 | 2013, mis en ligne le 25 septembre 2013, consulté le 23 Juillet 2017. URL : <http://sociologie.revues.org/1820>
- FLICHY. Patrice. *Le sacre de l'amateur. Sociologie des passions ordinaires à l'ère numérique*, Seuil, 2010, P66
- GEHL. Robert, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network", *New Media and Society*, Forthcoming. September 19, 2014.
- GELDER. Ken, *Subcultures. Cultural histories and social practice* . Routledge, New York, 2007.
- GENSOLLEN. Michel « Biens informationnels et communautés médiatisées » *Revue d'économie politique* n°113, 2004

- HIMANEN . Pekka, « L'Éthique hacker et l'esprit de l'ère de l'information de l'information » 2001
- JOLLIVET. Pascal « L'Éthique hacker et l'esprit de l'ère de l'information de Pekka Himanen », *Multitudes* 2002/1 (n° 8), p. 161-170.
- LASSE Ø. PAUL S. *Locating Hidden Servers*. IEEE Symposium on Security and Privacy. 2006
- LACAZE. Lionel, « L'interactionnisme symbolique de Blumer revisité », *Sociétés*, 2013/3 (n° 121), p. 41-52. DOI : 10.3917/soc.121.0041. URL : <https://www.cairn.info/revue-societes-2013-3-page-41.htm>
- MEYER. Morgan et MOLYNEUX-HODGSON Susan, « « Communautés épistémiques » : une notion utile pour théoriser les collectifs en sciences ? », *Terrains & travaux*, 2011/1 (n° 18), p. 141-154. URL : <https://www.cairn.info/revue-terrains-et-travaux-2011-1-page-141.htm>
- NARDIE. Bonnie. *My Life as a Night Elf Priest: An Anthropological Account of the World of Warcraft*. Ann Arbor, MI: University of Michigan Press. 2010 .
- PAPSDORF. Christian. *What is the Hidden Web? The development, characteristics and social significance of anonymous communication on the hidden web*. Chemnitzer Internet- und Techniksoziologie. 2016.
- PRUS. Robert. *Subcultural mosaics and intersubjective realities : An ethnographic research agenda for pragmatizing the social sciences*. Albany, New York: State University of New York Press. 1997.
- RAYMOND. Eric. *How to become a hacker*. 2001
- RENNARD. Jean-Philippe. *Darknet mythes et réalités*, Paris, Ellipses, 2016

- SIMMEL. George, *Secret et sociétés secrètes*, Circé, 1991.
- SMYRNAIOS. Nikos. « *Les GAFAM contre l'internet : Une économie politique du numérique* ». Poche. 2017
- SUTHERLAND. Edwin H. (1924) *Principles of Criminology*, Chicago: University of Chicago Press.
- TIERNEY. J. *Key Perspectives In Criminology*, McGraw-Hill, United Kingdom, 2009
- TRÉMEL. Laurent. La pratique du jeu vidéo : un objet d'études sociologiques ? In : Roustan M. (Dir.). *La pratique du jeu vidéo : réalité ou virtualité ?* Paris : L'Harmattan, 2003, pp. 157-169.
- WENGER. E, *Communities of Practice: Learning, Meaning, and Identity*, Cambridge University Press, 1998. Saint-Onge, H & Wallace, D, *Leveraging Communities of Practice*, Butterworth

Annexe 1 : « Les 10 règles à suivre sur le Deepweb »

Les 10 règles à suivre sur le DW:

pour ceux qui sont la juste avec tor + firefox simple: <http://www.youtube.com/watch?v=rwxV1YSPBoE> c'est pas grand chose mais ça améliorera déjà votre sécurité et votre anonymat

1) l'anonymat, ANONYMAT on demande pas le tel ou le skype de personne, on ne donne pas son adresse, encore moins ses coordonnées bancaires, on désactive son javascript, on va pas sur facebook en même temps que sur le DW sur TOR. Il y a vous sur le CW et vous sur le DW, ils ne doivent être fiables en rien! Vous faites pas des recherches de choses trouvées sur l'union sur chrome parce que ça va plus vite! Ne faites pas n'importe quoi, réfléchissez avant d'agir

2) Le choix de votre Deepidentité : prenez un pseudonyme (alors par pitié évitez les momodope, les kevinvendushit, les bossdu18 ou les wesh93200) dont vous réfléchissez longuement (plus de 1h avant de faire votre choix) et vous collez à votre pseudonyme. Ainsi, si je vous dit que isellpizza est le meilleur vendeur de CC du web, il n'a que cette identité (du moins pour les CC). Bien sûr vous pouvez vous faire votre premier compte, venir sur un forum comme celui-ci, posez un tas de questions débiles et ensuite quand vous vous sentez prêt, cette fois vous changez de pseudo et ne faites plus le noob, ou si vous voulez faire des choses pas associées à votre identité que vous êtes créé. Le choix est vaste et les possibilités sont multiples mais réfléchissez toujours avant d'agir.

3) La lecture: prenez le temps (souvent des heures) de lire ce qui a déjà été dit, vous trouvez déjà la 75% de ce que vous cherchez. Et oui il faut beaucoup de patience, rien n'arrive tout cuit dans le bec sans rien faire

4) l'anglais: est absolument obligatoire, si vous maîtrisez pas la langue de Shakespeare, vous n'aurez accès quasiment rien, mais si vous parlez en plus allemand et russe vous avez accès à 95% du DW. Donc si vous parlez QUE français, vous êtes à la bonne place, car il n'y a que un petit réseau français pour l'instant pas mal down depuis le début du mois. Alors faites un effort et investissez dans des cours d'anglais, c'est vraiment facile et c'est obligatoire pour une ouverture mondiale.

5) Devenir paranoïaque: quelque soit l'activité que vous décidez de commencer en venant ici, il ne faut pas imaginer que tout va tomber du ciel sans risque. Par exemple vous décidez de faire du carding physiquement alors vous recherchez des dumps+pin FR ou EUR du moins, après avoir filé 2 ou 3 bitcoin vous vous apercevez qu'il n'y a que des scammer qui proposent ce service (ou tout du moins 95%) et vous auriez été parano à vous dire que le monde vous en veut, vous seriez plus méfiant et seriez passer par escrow. Ne soyez pas fénéant, cherchez des infos sur le vendeur, regardez s'il est trustable ou non, les reviews qu'il a eues. Mais bon imaginons que vous avez de la chance et tombez sur de vrais dumps+pin plastic, alors il faut des vêtements spéciaux pour cette occasion, des lunettes pour masquer des caméras de sécurité omniprésentes et des téléphones portables et surtout ne le faites pas dans votre ville

Be parano, Be safe
Don't shit where you eat

6) comprendre avant d'agir: réfléchissez avant de poster, avant d'acheter, avant de regarder du CP ou de faire n'importe quoi. Achetez pas 10g de desomorphine parce que le vendeur vous dit que c'est safe et un trip sans danger, utilisez TOR pour vérifier ce qu'est la desomorphine et vous serez directement fixé sur la destination de ces 10g à leur arrivée chez vous. Vous voulez voir des snuff movies ou de la pédophilie pour vous faire des sensations fortes, faites attention que ce ne soit pas trop fort et que ensuite vous ne pourriez plus retirer ces images ou ces cri de votre tête. Le DW est rempli de choses que votre esprit ne peut concevoir et tant mieux pour vous, ne faites pas le dur ou le blasé, ce n'est pas rotten ou teeange.com. Comprenez bien la portée de la chose et ce que vous faites.

n'oubliez jamais que si c'est trop beau pour y croire c'est que c'est justement trop beau pour être vrai et qu'il existe toujours plus horrible.

7) Le respect: si vous voulez que l'on vous respecte, que l'on prenne au sérieux votre business, respectez les gens, ils y aura des trolls, des scammer qui viendront pourri vos posts, ce n'est pas grave, ignorez les ou répondez leur calmement. Ne demandez pas le respect, faites en preuve et vous serez respectés. Cela inclus un effort au niveau de l'orthographe ou de la traduction, vous êtes ni dans votre lycée, ni dans votre cité ou votre patelin de campagne. Il est possible et même conseillé de parler de tout ici (sauf du vrai vous) mais pas n'importe comment tout de même.

8) faites vous des amis, des connaissances, des relations tout en restant ANONYME ir: partagez votre savoir, ce que vous découvrez par vous-même, apprenez des autres.

9) N'oubliez jamais que ce qui est illégal reste illégal! La profusion de services illégaux, du hackage, au arnaque, montage financier, pari truqué, snuff movie, carding, vol, assassinat, pedo, chimie, drogue, arme sur le DW ne les rend pas légal.

10) vous ir! = même vie que avant (surtout ne pas s'acheter une ferrari en étant au chômage), mais par exemple partir en vacances et y dépenser de l'argent ou faire des cadeaux, mieux manger, allez au resto ou blanchir l'argent à travers de multiples sociétés écran. Mais vous débutez, soyez patient, commencez petit, arrangez les choses du début à la fin régler les problèmes puis augmenter votre rendement diversifier vous etc...

vous ici = un nouveau né qui viens de naître avec une nouvelle identité qui ne doit jamais, JAMAIS croiser votre vrai ir et qui va découvrir l'envers du décor et tout un nouveau monde dans lequel ce charmant bambin pourra s'épanouir ou alors si c'est un sale gamin irrespectueux et pénible sa vie dans ce nouveau monde se retrouvera affichée sur hardcandy.

Annexe 2 : Jargon file tiré de la section Escroquerie / Carding

- DOX = Rassemblement d'informations sur une personne
- Pass PTT = clés générique ouvrant un bon nombre de hall d'immeuble par exemple, cela dépend du format.
- FDP = Fiche De Paie
- Scam-exit = Le fait pour un personne de quitter définitivement son identité en scamant un bon nombre de gens.
- scam = arnaque. Ce vendeur fait des scams

- BAC = Boite A Colis (les boites marrons qui servent de relais aux facteurs).
- BAL = Boite aux lettres.
- Cardable = ce dit d'un site internet où il est facile d'utiliser une CC volée, car il n'y a pas beaucoup de sécurités telles que le VbV (verified by visa)
- CC = Carte de Crédit.
- CCV/VCC = carte de crédit virtuelle.
- CVV = cryptogramme visuel = Le code de sécurité (CVV2 ou CVC2) est un groupe de 3 ou 4 chiffres imprimés au dos de la carte de paiement à droite de l'emplacement réservé à la signature, mais il n'est pas encodé dans la bande magnétique contrairement au CVV1.
- DAB = Distributeur Automatique de Billets
- DROP = Boite au lettre servant à récupérer des colis ou des lettres, souvent à un faux nom ou utilisé à l'insu de l'utilisateur

Résumé

L'univers des *darknets* reste encore aujourd'hui un sujet principalement connu pour ses activités illégales ainsi que ses capacités de contournement de la censure. En effet, les articles relatant ses trafics à l'intérieur de ces espaces sont légion et les études universitaires qui abordent ce sujet gravitent majoritairement autour d'un point de vue légal ou technique. Pourtant, cet espace numérique dispose en son sein d'un grand nombre de communautés actives véhiculant des normes, des argots, ainsi qu'une idéologie propre aux *darknets*. Hérité de la subculture *hacker* à laquelle ils empruntent certains traits caractéristiques, les communautés des *darknets* développent une représentation du monde particulière que les sciences sociales abordent difficilement.

L'objectif de cette étude est de tenter de comprendre comment ces espaces reclus sont organisés et régis de manière étonnamment exigeante. Ce travail a aussi pour but de d'appréhender les communautés du « *darknet* » par leur capacité à être le vecteur d'une forme de production et d'alimentation d'une subculture propre à ce réseau entièrement anonyme.

En d'autres termes : quelle production culturelle s'exprime dans ces espaces élitistes?

Pour répondre à cette question, une immersion dans une communauté du *darknet TOR* aura été nécessaire pour comprendre les enjeux véhiculés dans ce réseau. Une ethnographie virtuelle au travers d'analyses de captures d'écran ainsi que d'entretiens avec les internautes de la communauté du « DeepNetwork » aura permis d'extraire ce qui semble constituer une expression identitaire propre à la subculture des *darknets*. Basée sur la transgression des normes sociales et du partage d'informations libres et sans censures, cette subculture se structure autour de plusieurs axes majeurs dont l'anonymat et la sécurité en constituent les piliers principaux. Opposées au *clearweb* considéré comme l'espace de la surveillance de masse et de la marchandisation des données personnelles, les communautés des *darknets* développent en leur sein des règles de fonctionnement peu soumises aux représentations légales et éthiques applicables au web conventionnel.

Les communautés des *darknets* expriment une vision politique libertaire dans un espace numérique libéré des contraintes légales. Autrement dit, ces réseaux véhiculent des pratiques et des discours renvoyant à un usage politique d'outils techniques.