WEB PROFOND ET DARKNET COMME SOURCE D'INSPIRATION ARTISTIQUE

Université Paris VIII

Master 2 en
Multimédia Design et Art Contemporain
2017

Vincent Bonnefille

Mémoire achevé en septembre 2017, avec le soutien de Gwenola Wagon.

Matricule étudiant : 12314947.

Certains articles web sont consultables et archivés à cette adresse : http://mht.vincent-bonnefille.fr.

http://kabane.org/thema/surveillance/ contient un corpus élaboré en collectif autour des questions qui nous intéressent ici.

http://44llcbgyt22pwvyq.onion complète ce mémoire numériquement.

Cette recherche est amorcée en 2015 : http://vincent-bonnefille.fr/#darknet.

Les termes mentionnés d'un [g] sont détaillés dans le glossaire.

Sommaire

5 **Introduction**

7 **I. Internet monolithique**

9 · **Iceberg : imaginaire confondant**

14 · · · **Web surfacique : un espace modéré**

18 · · · Fil barbelé et inséparation du tout autre

22 · · · Moi aussi je participe à la surveillance

26 · · · **Vers une modération automatisée**

31 · · · Chatroulette : espace non modéré

35 · · · Entre le désir de communiquer et celui de se terrer

36 · **Surveillance : distanciation du pouvoir décisionnel**

41 · · · Memex : indexation sans limite

43 · · · Babel : infini immodéré

45 · · · **Obfuscation : brouiller les données**

47 **II. Darknets et technologies d'avant-garde**

49 · **Imaginaire de la contagion informatique**

52 · · · Red rooms : la culture de la peur

53 · · · **La peur de l'outil**

55 · · · Welcome to the Game

56 · · · La radicalité des outils

58 · **Darknet originel**

59 · · · **Adressage Internet Protocol**

61 · · · The Pirate Cinema : P2P et MSM

65 · · · Réseaux autonomes

66 · · · Réseaux informels

68 · · · Newstweek

69 · · · Can You Hear Me ?

70 · · · Indépendance

74 · · · **Échanges locaux**

76 · **Blacknet et utopies numériques**

79 · · · Marché libre : autonomie de distribution

80 · · · **Autonomie libérale : une utopie réalisée ?**

81 · · · Blockchains : quel projet ?

83 · · · Satoshi Nakamoto : non anonyme

85 · · · The Random Darknet Shopper

88 · · · Delivery to Mr Assange

93 **Conclusion**

95 **Annexes**

96 · **Tor et autres darknets : précisions techniques**

99 · · · Outils d'audit

102 · · · Scrapper : aide à l'archivage

105 · Sur-contre/sous-veillance/fiction

107 **Bibliographie**

109 · Conférences

111 **Glossaire**

Introduction

Les darknets[g] sont de plus en plus populaires. Ces réseaux hors norme font fantasmer un ailleurs sans limite morale, sans modération, hors du contrôle judiciaire. Imaginés comme des zones de non-droit, ils offrent un espace de liberté d'expression bien plus grand que celui offert sur le web[g] que nous utilisons tous les jours. La modération et l'indexation du web lui donnent sa visibilité, qui est, elle, limitée par la capacité des outils qui procèdent à cette mise en lumière des contenus, qui les organisent. Ainsi, l'internaute n'a accès qu'à une partie limitée mais déjà immense de contenus, de sites Internet. L'en-dehors auquel il n'a pas accès peut s'expliquer de plusieurs manières, avoir plusieurs causes, que nous allons détailler.

En saisir la complexité nous permettra de démystifier une image répandue pour représenter les darknets : l'iceberg. Ce logo, riche de sous-entendus, nous servira de support dans notre recherche pour séparer ce qui fait partie du web normal, du web non indexé, et enfin du darknet. La méthodologie employée ici – celle de la séparation – sera elle-même questionnée comme procédé d'explicitation, de mise en transparence, de découvrement. Cette réflexion sur notre travail de recherche sera mise en lien avec des procédés de contrôle qui sont au cœur de l'activité d'archivage et de surveillance à l'œuvre sur Internet.

Nous analyserons ensuite des réalisations artistiques prenant pour champ de recherche l'Internet afin de tenter d'en analyser le propos. Nous verrons en quoi elles explorent ces différentes parties du web normal et profond et en perturbent les usages normaux. Les discontinuités ainsi produites au sein de dispositifs politiques établis en révèlent le fonctionnement. En découvrant ces systèmes d'automatisation mis en place pour répondre à des problèmes organisationnels de mise en visibilité, nous chercherons à comprendre à quels projets ils participent.

Cela nous amènera à poursuivre une réflexion sur les transformations de perception des pouvoirs exercés par une surveillance devenue indolore, invisible. Nous verrons en quoi ils dissocient le moment de l'apparition publique, en quoi le fait de rendre opaque leur fonctionnement invente une autre façon de faire de la politique, exempte de la critique. Ces nouvelles modalités posent des questions de seuil, de transparence qui sont au cœur des contre-pouvoirs, également exercés par les lanceurs d'alerte. Nous réfléchirons alors en quoi les outils de mise en visibilité des savoirs, en tentant de lutter contre ce qui leur échappe, produisent des outils de mise à plat et en quoi cette découverte de tout ce qui est enfoui, profond, se heurte à un problème de limite.

En seconde partie, il sera plus précisément question de réseau. Une fois encore, nous prendrons pour appui des œuvres populaires imaginant le darknet et nous montrerons ce qu'elles véhiculent de craintes et de fantasmes à son endroit. Nous verrons ce que les projets d'archivage et d'enquête produisent d'idéal technologique, d'un accès à toute chose poursuivi par une mythologie populaire d'un au-delà au sujet des darknets. Au regard de cette acception contemporaine des darknets, nous pourrons réfléchir ce rapport d'altérité à un tout autre, distant par la définition historique de ce qu'était alors un darknet aux débuts d'Internet. Cette définition primaire nous permettra d'aborder quelques points techniques sur la mise en réseau du monde.

Nous pourrons ainsi expliciter ce qui rend si aisée une surveillance automatisée et réfléchir aux alternatives de cette gouvernementalité d'Internet autour de dispositifs qui permettent de créer de l'autonomie médiatique. Nous verrons comment ces outils donnent aux artistes les moyens d'investir l'espace public et de révéler des pratiques de surveillance hors du réseau des réseaux. Cette autonomie de moyens introduira certains principes clés des mouvements à l'origine des darknets et de leur philosophie. Forts de cette mise au point, nous analyserons un ensemble d'œuvres qui utilisent le darknet comme moyen de création en les infiltrant ou en extrayant des données.

I. Internet monolithique

Iceberg : imaginaire confondant

L'image la plus répandue au sujet des darknets est sans doute celle de l'iceberg. Elle sert souvent de support pour illustrer une certaine vision d'Internet comme ensemble coagulé de réseaux. La hiérarchie qui est donnée confond en général plusieurs notions entre types d'accès et contenus. Le but de ces documents est rarement de donner une vision objective, bien que certains d'entre eux soient parfois très complets pour décrire la composition des réseaux et du web. Cette vulgarisation est déplorée, par le cofondateur du projet Tor[g] Roger Dingledine[1], car elle produit des amalgames autour de concepts, d'outils ou d'acteurs très différents. Clarifier cet imaginaire nous permet ici, méthodologiquement, de comprendre la complexité d'une mise en forme artistique mais aussi conceptuelle au sujet des darknets. Défaire cet imaginaire technologique, d'outils et de moyens hybrides, nous permettra de séparer plusieurs acteurs, de comprendre leurs motivations distinctes dans l'archéologie de cet « Iceberg » représentant Internet.

À la pointe de l'iceberg, hors de l'eau, le « *clear web*[g] » (un web propre, modéré). Un web aussi appelé « *light web* » (lumineux). Ce qui est en dehors de l'eau représente donc les sites et plateformes les plus connues, les multinationales du Gafamg principalement. La notion de *clear web* induit une action de nettoyage par modération et de tri de ce qui est rendu accessible et visible par les sites eux-mêmes. À l'autre extrémité est représenté, dans les profondeurs abyssales, un darknet ayant lui-même plusieurs strates intermédiaires. Darknet – association de « *dark* » (obscur, sombre) et de « *net* », préfixe de *network* (réseau) – est un réseau obscur qui s'oppose aux réseaux communément accessibles, utilisants des protocoles communs en informatique, standardisés sur les ordinateurs mis en vente. Ce sont les spécificités de ces réseaux qui les rendent obscurs à un regard extérieur, à une surveillance automatisée. En tant que réseaux, ils permettent de faire transiter des informations qui peuvent être utilisées pour de l'affichage de page web, mais aussi pour de l'envoi de données servant à d'autres applications et/ou protocoles.

1. Le logiciel Tor met en place un des darknets et permet d'y accéder. Article en question : Christopher Wink, « Stop talking about the dark web, the Tor Project cofounder Roger Dingledine», Philly Tech Week, 2017, URL vers l'article : https://technical.ly/philly/2017/05/15/dark-web-roger-dingledine.
NB : une annexe (technique) sur les darknets est disponible, cf. « Tor et autres darknets : précisions techniques ».

L'agrégation des données non exploitées par des moteurs de recherche forme elle le *deep web*[g] ou web profond, représenté entre le *clear web* et le darknet. Cet entre-deux est donc limité. Ces données retirées ou non traitées sont exclues de la vision souvent par manque d'accessibilité. En dessous, dans l'obscurité sous-marine, des réseaux qui empêchent la visibilité et la transparence des activités entre les ordinateurs qui les composent, forment une masse inquiétante.

Cette imagerie induit par sa sémantique qu'un web civilisé est vivable, hors de l'eau, à l'inverse du reste qui le soutient implicitement, comme inconsciemment. Il y a effectivement une forme d'inconscient dans l'usage d'Internet. D'abord autour des outils qui le structurent (*data centers*[g], câbles sous-marins, intermédiaires logistiques, institutions, etc.) qui sont cachés du public malgré leur place importante elle que celle de transporter l'information sur le réseau. Il y a ensuite l'ensemble des outils logiciels et bases de données qui offre une pérennité par une sauvegarde des contenus et leur affichage sur le web pour les utilisateurs (aussi appelés « clients[g] », en opposition aux « serveurs » qui distribuent les données).

Le web profond contient tout ce qui échappe à la vision des utilisateurs du *clear web* ou « web surfacique » (si nous poursuivons l'analogie marine) car non indexé. En indiquant les darknets en dessous du *deep web*, cet iceberg idéalise le fait qu'ils se continuent l'un l'autre. Or, si leurs contenus échappent à la vision que produisent des *spiders/bots*[g]*/crawlers*[g] – ces algorithmes qui récupèrent des informations sur des sites pour les indexer à des moteurs de recherche –, ils échappent surtout à un autre type de regard, celui de la surveillance à l'endroit des réseaux. Ce qui est dans le *deep web* échappe à la vision des internautes, tandis que ce qui est sur les darknets échappe à un regard plus large, sans pour autant que les activités qui s'y déroulent soient nécessairement illicites.

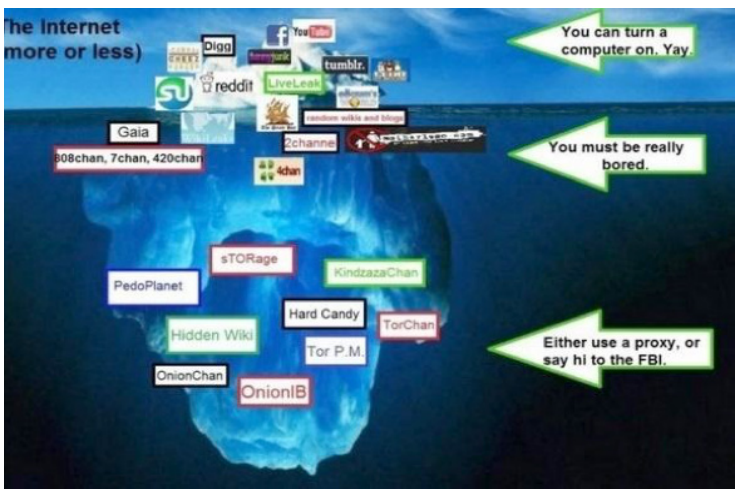
> «[On] peut peler un oignon à la recherche de la vérité jusqu'à ce qu'il n'en reste rien : chaque couche enlevée cesse de matérialiser son extérieur, chaque couche révélée cesse de matérialiser l'extérieur, chaque couche révélée cesse de constituer son intérieur – *l'ontologie se donne en fait comme une oniontologie*. »
> **Dominique Quessada, L'Inséparé - Essai sur le monde sans Autre**[8]

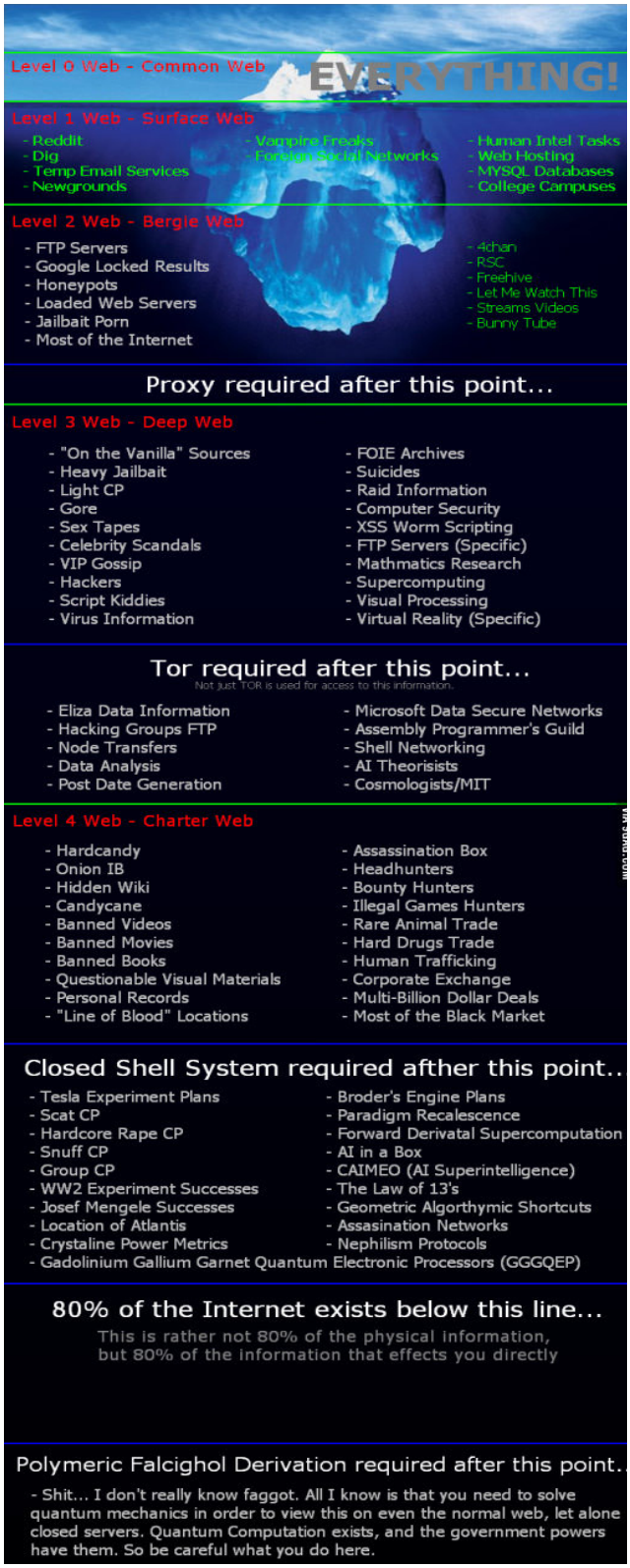
[À droite] Illustration récurrente imaginaire technologique du *deep web* en iceberg trouvée sur le site RationalWiki dont voici la table des matières :

« 3. *Deep web* "levels"
3.1 Level 0 Web — *Common web*
3.2 Level 1 Web — *Surface web*
3.3 Level 2 Web — *Bergie web*[g]
3.4 Level 3 Web — *Deep web*
3.5 Level 4 Web — *Charter web*
3.6 Level 5 Web — *Marianas web*[g]
3.7 Level 6 Web — (?)
3.8 Level 7 Web — *The Fog/Virus Soup*
3.9 Level 8 Web — *The Primarch System* ».

Ce site accessible sur le *clear web* est spécialisé dans les pseudosciences (ayant un argumentaire empirique, général, préférant affirmer leur propos plutôt que d'infirmer une hypothèse). L'auteur y est plutôt critique à l'endroit de cette représentation du *deep web*.

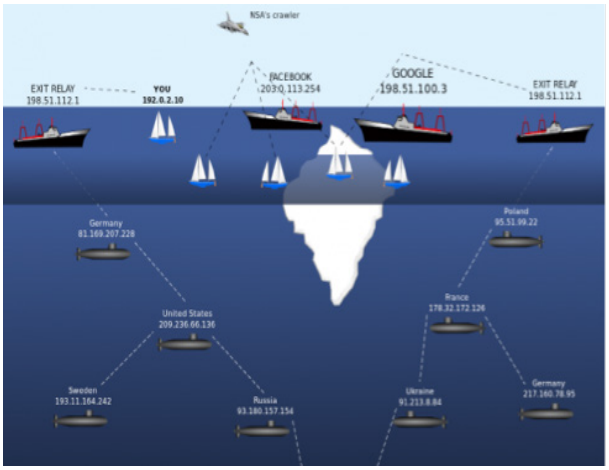
Sur la même page web *[ci-dessous]* :
« *What is the deep web and how do you access it?* »[9].





8. Dominique Quessada, *L'inséparé - Essai sur le monde sans Autre,* éd. PUF, p. 100.
9. Auteur non mentionné, *Deep web*, The RationalWiki (version censurée sur le *clear web*), 2016, URL : http://rationalwiki.org/wiki/Deep_web.

L'indexation du web est réalisée par des outils qui permettent une distribution construite de la vision du monde. Ces données génèrent du revenu pour des entreprises plus ou moins attentives à respecter une impartialité quant à ce qu'elles seraient censées décider de montrer ou de cacher. La vision qu'offre le recensement du web s'intéresse aux contenus comme capitaux et à leur modération là où la surveillance cherche à inscrire dans un champ politique et social d'institutions un individu identifié par sa connexion. Il est assez facile de confondre, d'un côté, le fait d'une mise en vision des ressources sur le web par l'indexation de sites, la modération de ces derniers, etc. et, de l'autre, la recherche d'anonymat de connexion que permettent les darknets.



Nous insistons ici sur le fait que de telles représentations ont chacune une volonté d'explication différente, des buts pédagogiques variés.

[Ci-contre] Image illustrant assez justement la variété d'acteurs créant de la vision autour d'Internet. Leurs adresses IP[g] sont mentionnées.
Les outils d'indexation de la Nasa surplombent, surveillent, dans un avion militaire, les plaisanciers (utilisateurs) mais aussi les gros bateaux, tels Facebook ou Google. Les sous-marins représentent des États, eux aussi investis dans une militarisation d'Internet (contre une cyberguerre qui les oppose par attaques informatiques, espionnage)[2].

Nous pouvons attribuer la popularisation de cette image aux recherches menées par Denis Shestakov[3] sur les parties non indexées ou non indexables d'Internet, et le terme de *deep web* à Michael K. Bergman[4] qui mentionne Jill H. Ellsworth au sujet d'un « web invisible » en 1994 pour désigner des sites non indexés[5]. L'appréciation de ce que décrivent ces *deep web*, darknet, *clear web* repose sur des perceptions qui évoluent au fil des recherches à ce sujet, des avancées techniques et de leurs usages. Une compréhension qui raconte une perception sociale des technologies, qui nourrit un imaginaire collectif entretenu par des créations variées plus ou moins rigoureuses.

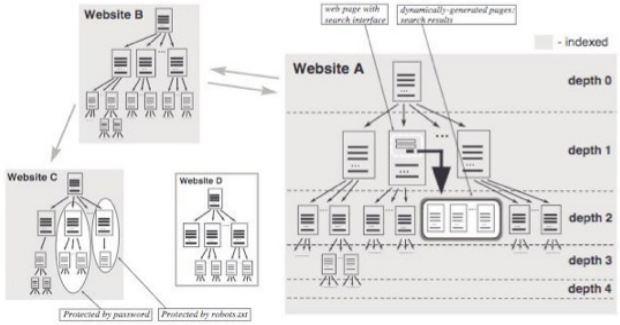
2. Rezonansowy (pseudonyme),Wiki Commons, 2013 URL : https://commons.wikimedia.org/wiki/File:Deep_Web.svg, image utilisée entre autres pour illustrer l'article anglais du site encyclopédique sur le *deep web*.

3. Étude menée à l'université de Californie, Berkeley, en 2000. Source : Wikipedia, URL : https://en.wikipedia.org/wiki/Deep_web ; notes de bas de page : [1] Bergman, Michael K , « The Deep Web : Surfacing Hidden Value », *The Journal of Electronic Publishing*, 2001 ; [2] Shestakov, Denis, « Sampling the National Deep Web », 2011, URL : http://www.mendeley.com/download/public/1423991/4300016182/a07080a3191f90cc97cf60fcd21566b1b915d894/dl.pdf.

4. Hervé Fischer, *La Pensée magique du Net*, éd. Bourin, 2015, à propos de la création d'un moteur de recherche mis en place par le chercheur (p. 26) et d'une réflexion sur la mythologie autour des profondeurs aquatiques du web (p. 27).

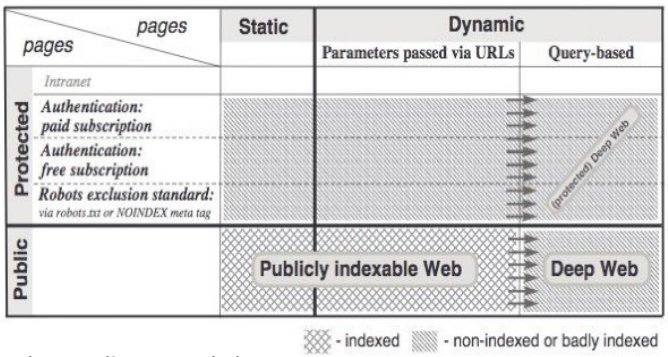
5. Auteur non mentionné (contenu sans doute copié depuis les différentes pages de Wikipédia), « *"Deep Web", "Darknet", "Dark Web" and "Darknet Markets" from Wikipedia* », 2015.
URL : http://www.thevoicebeforethevoid.net/deep-web-darknet-dark-web-and-darknet-markets-from-wikipedia/

Denis Shestakov, *Search Interfaces on the Web - Querying and Characterizing*, TUCS Dissertations, 2008, p. 2 (trad. de l'anglais) : « Fig 1.1 : en tant que page unique contenant une interface de recherche [qui lui est propre] et du fait qu'elle soit connue et indexée par des moteurs de recherche [son indexation est possible]. Cependant, les pages générées dynamiquement en réponse à des requêtes effectuées par ce moteur de recherche [interne], ne sont pas indexées [en l'état relatif à ces requêtes] du fait de l'incapacité [des outils d'indexation] de générer ce type de requête [via un formulaire]. »



Le chercheur Denis Shestakov tend à clarifier méthodiquement ce qu'est le web profond. Il serait formé de 7,5 petabytes de données, soit 400 à 550 fois plus large en quantité de données que le web indexé (selon les sources à toujours actualiser). L'auteur y schématise la profondeur (« *depth* »), qui indique le nombre d'étapes intermédiaires dans la recherche de contenus d'une page à l'autre, par les hypertextes qu'elle contient. Des sites web et leurs interconnexions permettent l'exploration des sites ainsi indexés. La profondeur d'un site est ainsi explicitée sous la forme d'une arborescence verticale qui n'a rien de concret ; elle est explicative, elle suit la logique de la lecture de haut en bas indiquant une durée[6].

[Ci contre, même source que l'illustration précédente mais p. 3] « Fig. 1.2 : parties indexées et non indexées du web. **Pages protégées** (non indexées) : par authentification liée à une inscription payante ou non ; par utilisation de restrictions meta : *no index* [ou robots.txt] ; génération dynamique : par paramètre de page dans les URL[g] produisant des pages dépendantes de requêtes (et donc protégées). **Pages publiques** (indexées) dynamiques ou statiques sans identification ni paramètre de requête. »



Le tableau *[ci-dessus]* renseigne quant à lui sur la difficulté ou l'impossibilité d'indexer (en 2008) des contenus web. L'indexation est impossible si les pages sont protégées : par mot de passe ou encore si un fichier « robots.txt » explicite un refus de la part d'un administrateur (serveur) de voir ses pages indexées[7]. La partie du *deep web* de pages publiques (non protégées en accès par une identification) est, dans ce schéma, réduite aux pages dynamiques basées sur des requêtes (« *queries* »). La création d'un imaginaire rigoureux, d'une étude technique sur l'indexation du web, permet de comprendre sa réalité de fonctionnement.

6. Une telle représentation pose des questions ontologiques discutables quant à l'apparition des contenus ainsi formalisée comme séparés, et amène une réflexion autour de ce que sont les données. Conférence à ce sujet : Alexandre Monnin, «Une ontologie pour le web ? » *Labex OBVIL*, 2015, URL : https://youtu.be/UMdr8PrdikQ?t=1h9m9s.

7. D'autres convenances permettent, de façon tacite, diplomatique, intégrée ou non dans les algorithmes d'indexation, les bots[g], de prévenir une indexation rendant publique/visible des pages web.

Web surfacique : un espace modéré

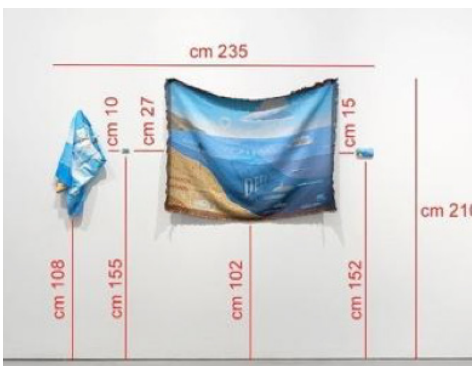
Deux artistes contemporains, Eva et Franco Mattes, reprennent une des compositions graphiques communes sur le web pour expliquer ce qu'est web profond. Une autre représentation un peu différente de l'iceberg. Pour leur installation Abuse Standards Violations, exposée à la galerie Carroll/Fletcher, à Londres en 2016, ils impriment cette image sur différents objets : une serviette de plage, la coque de protection d'un Smartphone, une carte postale [voir page suivante]. Reproduire une image numérique populaire sur Internet – un mèmeg, image récurrente d'autorité culturelle sur le sujet – sur des produits industriels populaires eux aussi renforce le fait que cette image se soit banalisée. Cette reproduction en confirme l'importance du fait de son exposition dans un milieu culturel hors d'Internet. En changeant le support les deux artistes en modifient également le sens. Plus qu'une représentation d'un réseau, cette image symbolise chaque acteur autour d'un paysage : une plage, un espace propice aux vacances, à la détente et à la consommation. Imprimer ce mème sur des objets qui véhiculent cet état d'être poursuit le fait de coller cet imaginaire de détente et de sécurité sur le web et en modifie le sens premier.

Illustration du *deep web* trouvée sur le web, semblable à celle utilisée par les artistes.

En se limitant au *deep web*, cette image me semble plus juste que celle de l'iceberg monolithique. De plus, en spatialisant les différents acteurs, elle y intègre une dimension politique, bien que simplifiée. La représentation tridimensionnelle de ce paysage induit une notion de temps. Bien que fantasmagorique, l'image qu'ils reproduisent sur différents supports est lisible. Cette production visuelle, au

même titre qu'une œuvre d'art, permet de produire du sens par le médium employé et un ensemble signifiant d'éléments culturels. Pour autant, cette image a un but informatif, de communiquer et ne prend ici sens qu'en tant que *ready-made*[g] culturel. La reproduction du même logo, sur des supports variés, fait penser au pop art.

Plusieurs éléments sont représentés autour et dans le web surfacique (*sea web*) et le web profond (*deep web*). Le continent figure une extrémité au web liquide. Les ossements idéalisent une matière archéologique extraite par l'encyclopédie Wikipedia – figurée en surface comme base pétrolière –; Amazon est également positionné sur la côte. Les serveurs sont représentés comme des glaciers qui dominent, et *The Cloud*[g] – imaginaire répandu d'un nuage de données à l'état gazeux – est dessiné dans le ciel. En surface apparaît le paquebot « Google ». Un flotteur orange représente le *porn* lié à un poisson monstrueux nageant en eaux profondes et figurant la forme illégale du *porn*, au même niveau qu'un sous-marin *undetected* – le plus bas, qui sous-entend une difficulté d'accès, mais évoque aussi un appât du type *honeypot*[g]. Entre ce niveau de ressources indétectables et la surface se trouve le *deep web* où circulent plusieurs sous-marins : un du gouvernement (le plus gros) suivi de celui de Wikileaks et, pour finir, plus en surface, un plus petit encore de *hackers*[g]. Ce même vulgarise et introduit une représentation idéalisée d'acteurs dominants dans cette géopolitique du cyberespace[g]. Le *deep web* y est dépeint comme le lieu de l'invisible, du non-détecté, échappant à Google, à l'indexation, mais pas à d'autres acteurs impliqués. C'est une vision assez juste. Seul l'illegal porn représente une ressource terrifiante, une extrémité et, s'il n'est pas ici fait mention du darknet, l'obscurité y est bien présente.



[À gauche] Protection de Smartphone exposée.

[À droite] Document de travail : vue d'ensemble de l'installation. Disposition et écarts entre les éléments indiqués en rouge. Ces annotations qui ne figurent pas dans l'installation me paraissent intéressantes du fait qu'elles induisent un rapport d'échelle inversé entre les objets exposés et ce qu'ils sont censés représenter, soit l'immensité du web.

Le problème de ces représentations est ontologique (comment ce qui est le devient, comment il apparaît). Comment se représenter le virtuel et l'informatique ? Comment s'imaginer des technologies complexes, imbriquées entre elles dans une chaîne de production et de maintenance de sites de plus en plus complexe ? Car c'est de cette complexité qu'il s'agit entre autres ici, celle d'une automatisation dans un procédé de mise en visibilité par des algorithmes qui indexent le *clear web* ou pour des autorités qui luttent contre la cybercriminalité face à des outils de cryptage – au centre des technologies d'anonymat que permettent les darknets. L'imaginaire métaphysique qui entoure les technologies me semble expliquer certaines de ces représentations qui tentent de les organiser selon une méthodologie matérialiste qui tend à tout lier. Internet paraît bien être une masse organisée presque comme par magie, un ensemble cohérent, homogène.

Or ce que permettent les darknets dont Tor fait partie, c'est bien, à l'image de son logo (un oignon), de produire des couches de discontinuité identitaire. L'outil Tor permet de dissimuler l'identité réelle, civile, d'une connexion, par l'ajout de couches numériques trompant la surveillance : l'accumulation d'identités fictives. On peut effectivement rapprocher l'image de l'iceberg ayant une profondeur et l'intériorité que produit l'oignon. Tous deux cachent quelque chose au dedans, une vérité inavouée, non publique.

Fanzine sur le darknet Tor, *Liber-Torian* n° 1, représentation ASCII d'un iceberg. Sont mentionnés : « *Surface Web (Clearnet)* » et « *Deep Web (Onionland)* ». Accessible ici (nécessite un accès via Tor) : http://xsold3pvbxt4xblv.onion/LiberTORian Issue 001.txt

Shadowmaster's Web Hierarchy Primer : « Ignore all infographics discussiong the *deep web* prior to this one, as they are inaccurate. (Created January 2012) ». Trouvé sur Redit (post) : « REAL guide to the *deep web* or Web Hierarchy »
URL : https://www.reddit.com/r/onions/comments/rph2h/real_guide_to_the_deep web_web_hierarchy/]
Se réclame comme plus pertinent que d'autres infographies et différencie : ◊ Le web surfacique ◊ Le *deep web* (sites non indexés ou non accessibles) ◊ Deepweb 2 (réseaux à accès restreints, protocoles anonymisant dont Tor, Freenet, I2P, etc.) ◊ Réseaux alternatifs hors Internet dont SIPRNet (réseau militaire américain) ◊ Réseaux privés (LAN, PAN, WAN, etc.) ◊ Mentionne Mariana Net comme inexistant (arnaque).

Fil barbelé et inséparation du tout autre

Olivier Razac, en s'appuyant sur les ouvrages de Foucault comme point de départ, a développé une « histoire politique du barbelé » (titre de son livre, paru chez Flammarion en 2009). Il explique ses divers usages : la clôture sur le sol américain face aux autochtones et pour le bétail, l'usage dans les tranchées durant les Première et Seconde Guerres mondiales jusqu'à nos jours. Cet objet produit des territoires limités ainsi contrôlés, et la propriété terrienne visible. Le fil barbelé, objet industriel, à la fois défensif et offensif, marque un seuil entre le dedans et le dehors confondus ; il met à distance celui qui est de l'autre côté. Une figure de séparation, d'enclosure, qui mène l'auteur à étudier les nouvelles formes invisibles qui ont remplacé l'objet trop visible et péjoratif dans l'imaginaire collectif. Il réfléchit dans son développement sur les nouveaux dispositifs de privation, d'accès et de contrôle social, qui poussent les individus à la censure, à l'automise en retrait. Il poursuit ainsi le travail de Foucault sur les sociétés disciplinaires devenues celles du contrôle, de la vérification permanente, intégrée, mais indolore. Un autoajustement des individus qui se produit aujourd'hui par feed-back[g], des ajustements en temps réel. Un mécanisme de permanente vérification dans une société de contrôle.

> « Pour désigner cette nouvelle forme, Deleuze emprunte à Burroughs le terme de contrôle. La notion paraît renverser une sorte de sens commun des rapports de domination : loin d'être imposé ou forcé, le contrôle est en réalité coproduit par les contrôlés, prenant appui sur leurs désirs plutôt que sur la répression de ceux-ci, incitant à la liberté et à la responsabilité individuelles dont il fait ses carburants. En perpétuelle "modulation", toujours "autodéformant", "numériques" plutôt qu'"analogiques", opérant par "mots de passe", les contrôles sont "comme un tamis dont les mailles changeraient d'un point à un autre". »
> **Frédéric Claisse, « Contr(ôl)e-fiction : de l'Empire à l'Interzone »**[10]

Dominique Quessada, quant à lui, auteur de *L'Inséparé - Essai sur le monde sans Autre*[11], questionne la disparition de l'autre à notre époque, avec le concept d'altéricide (qui sous-tend sa thèse sur une perte d'altérité, de séparation avec l'autre) et utilise, lui aussi, l'image du fil barbelé comme figure ambiguë de contiguïté, d'éloignement. Dans son essai, il s'interroge sur la

10. Multitudes n° 48, 2012, URL de l'article: http://www.multitudes.net/contr-ol-e-fiction-de-l-empire-a-l
11. Dominique Quessada, *L'Inséparé - Essai sur le monde sans Autre*, éd. PUF, Paris, 2013. Au sujet de l'altération, du fil barbelé p. 64 et 69.

représentation d'un en-dehors-dedans et explique en quoi cet imaginaire construit une pensée occidentale du savoir, de la vérité comme étant au-dedans des choses. Son propos, ontologique (et métaphysique), s'appuie sur les notions d'environnement et d'apparition dans les écrits de Martin Heidegger (penseur du XXe siècle, philosophe de la technique et de l'altérité). Cela lui permet d'expliquer quel régime de vérité sous-tend la modernité dans son désir de tout rendre visible, de tout extraire, de tout faire « remonter », contre sa hantise d'un mal intérieur incertain, enfoui, qu'il faudrait éclairer, découvrir. Il critique un geste infini de creusement, toujours déceptif, d'un dedans toujours transformé en dehors[12] – une réflexion qui le pousse à penser la matérialité d'une œuvre d'art entre son fond et son premier plan en peinture, entre ajout et suppression de matière en sculpture[13] –: une surveillance jamais suffisante.

> « L'intériorité et la profondeur de ce qui est, du réel, sont donc des présuppositions issues du mythe […] sur lequel se sont organisés le rapport au monde, la pensée et la quête de savoirs occidentaux […] : l'Être ou le réel sont le lieu d'un mystère enfoui à dévoiler (aléthéia) ou à exhumer. Dans ce cadre le mode de la recherche, quelle qu'elle soit, c'est donc toujours apparenté à la fouille, au fait de creuser, d'ouvrir. Le mystère est donc la modalité ontologique de la séparation : ce dont on est séparé, et qu'il faudrait absolument retrouver. »
> **Dominique Quessada, *L'Inséparé - Essai sur le monde sans Autre***[14]

La porosité des systèmes informatiques permet des intrusions au « dedans » qui ne distancie plus suffisamment d'un dedans et d'un dehors comme seuil (fil barbelé). Tous ces concepts, ces images expliquent (sortent du dedans) un problème de porosité, d'inséparation entre l'environnement et l'objet. Ils permettent de comprendre l'ambiguïté de l'idée de transparence. Ces imaginaires matérialisés sont latents et populaires dans les tentatives de représentation marine d'Internet : un milieu infini dont il faudrait recréer des en-dedans de vie privée, des « vacuoles »[15].

12. Op. cité, p. 91 : il prend l'image d'un pénultième wagon qui, défait, devient le dernier.
13. Op. cité, p. 142-177 : il traite entre autres du mashup dont il sera question au sujet de l'installation de Nicolas Maigret The Pirate Cinema, d'une dé-encapsulation des données « liquéfiées » entre elles.
14. Op. cité, p. 83.
15. Gilles Deleuze, *Pourparlers,* éd. de Minuit, 1990, p. 177 ; créer des moments d'en dehors social, de silence, des moments hors du tout autre.

Ouverture volontaire

Ce sont ces espaces sécurisés, inaccessibles à l'indexation et au public que les artistes de Société réaliste ont voulu ouvrir. Cette coopérative artistique, créée par Ferenc Gróf et Jean-Baptiste Naudy en 2004[16], dans le cadre des Riam 06 à Marseille en 2009 et de l'installation *Over The Counter*. La coopérative est le point de départ d'une performance collective en ligne. Elle expose, en libre accès, les identifiants du compte bancaire de leur association à la banque Société générale dont elle utilise le logo aisément reconnaissable comme motif répliqué et accroché sur les murs de l'espace d'exposition. Ce dernier, dédoublé et inversé, contient en son centre, à la place du nom de la banque, l'URL du collectif, son numéro d'identification et son mot de passe. Les identifiants détachables peuvent être emportés, et le relevé d'identité bancaire (RIB) de l'association est présent – il contient diverses informations légales confidentielles sur le titulaire. En rendant ces identifiants publics, ils permettent à quiconque de s'identifier à leur place, de réaliser des virements ou encore de changer les mots de passe : d'administrer leur compte sans le hacker (des informations qui sont par ailleurs en vente sur certains sites du darknet).

Over The Counter, qui signifie « gré à gré » en termes d'économie, désigne un échange boursier direct entre vendeur et acheteur, sans l'intermédiaire susceptible d'imposer sa politique, de taxer la transaction[17]. L'algorithme chargé d'automatiser une sécurisation d'accès sur la plateforme web de la banque remarque très vite un nombre de connexions anormalement élevé (provenant d'ordinateurs différents) et aura tôt fait de fermer le compte, d'en avertir leurs propriétaires (les artistes) qui le rouvriront à plusieurs reprises. Ils ont voulu ici faire l'expérience d'une mise en commun, d'une dérégulation de ces espaces hautement sécurisés.

En mettant en pratique l'ingérence par ce mésusage des conditions générales d'utilisation, différent d'un *hack*[g], ils ont produit un dérèglement interne à un système politiquement en place pour empêcher toute intrusion contrevenant à une utilisation normée de ces espaces numériques. Profitant de la tendance naturelle à l'avidité chez certaines personnes, ils ont mis en place une sorte de *honeypot*[18] en donnant accès aux visiteurs internautes à ces informations

16. Plus d'informations : http://seminaire.erg.be/index.php?/seminaire/societe-realiste/.

17. Ce terme paraît tout choisi pour évoquer le trading g à haute fréquence qui cherche à optimiser le temps d'exécution des ordres de transaction (vente/achat) gérés par algorithme. Cette recherche de nanosecondes est gênée par des actions de régulation qui contraignent sa fluidité d'action.

18. Un « pot de miel », terme imagé pour parler d'un piège attractif utilisé sur certains darknets contem-

hautement confidentielles, à ne partager sous aucun prétexte. Les artistes ont ainsi inversé une pratique normale, ou du moins habituelle, de sécurisation et de sauvegarde de la propriété à l'endroit des capitaux financiers en « communalisant » cet espace symbolique d'un fonctionnement capitaliste. Une manière de « déhiérarchiser » l'autorité. Cette mise en commun d'un accès à plus grand nombre est mise en scène par la répétition du logo et la mise à disposition des informations relatives au compte bancaire. Cet espace devient ainsi celui de l'œuvre performée collectivement sur Internet.

Le collectif informe donc une activité de modération en action sur Internet ; il fait apparaître les agents politiques invisibles qui organisent le pouvoir. Un pouvoir semblable à celui de la gouvernance d'Internet[19] qui n'est pas distribué, rendu commun, comme pouvaient le souhaiter certains pionniers d'Internet[20]. Cette proposition artistique produit pour ainsi dire un *happening* ou un *cybersquatting*[g] par une masse critique. Elle dévoile des fonctionnements de modération et explique ainsi ce qu'est la sécurité : l'appartenance à un seul et même objet/usager identifié, ici par login, mais aussi grâce à son adresse IP[g], à des matricules numériques attribués individuellement.

porains pour démasquer
des usagers ciblés dans le cas d'enquêtes ou pour extirper des identifiants de connexion en usurpant une identitée visuelle d'un site. Une tromperie plus facile encore sur le réseau darknet Tor du fait de la structure des adresses URL moins mnémotechniques en .onion – TLD[g] – produites pour les « sites cachés » qui peuvent induire en erreur un utilisateur.

19. Wikipédia : « La gouvernance d'Internet est l'élaboration et l'application conjointes, par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décision et programmes propres à façonner l'évolution et l'usage d'Internet (selon la définition donnée par le groupe de travail sur la gouvernance d'Internet du Sommet mondial sur la société de l'information). » URL : http://fr.wikipedia.org/w/index.php?title=Gouvernance_d'Internet.

20. Hubert Guillaud, « Ce que l'internet n'a pas réussi (3/4) : distribuer l'autorité », 2014, URL : http://www.internetactu.net/2014/03/17/donnees-personnelles-enjeu-commercial-ou-philosophique/

Une modération nécessaire qui défend les mésusages et protège des attaques massives coordonnées sur un serveur (DDoS[g])[21]. Ces plateformes nécessitant une accréditation/identification numérique échappent également aux robots (algorithmes) d'indexation du web.

La proposition de Société réaliste nous paraît ici pertinente dans son procédé d'infiltration d'un milieu sécurisé où la faille devient l'utilisateur. En révélant l'aspect méta de leur œuvre dans les échanges qu'ils ont eu avec leur banque leur faisant part de la fermeture de leur compte, une activité anormale, etc., les artistes, réalisent à mon sens l'œuvre en révélant les conséquences de la performance collective qu'ils ont mis préalablement en place. C'est cette tentative automatisée de retrouver de l'ordre qui me paraît intéressante, le fait d'en révéler une modération en lutte contre le chaos. Cette question du détournement, de comment, dans une création artistique, les artistes jouent avec ces agents automates m'intéresse dans ma propre pratique, et il me semble qu'elle est centrale dans la création de réseaux alternatifs.

Moi aussi je participe à la surveillance

En apprenant à coder par moi-même, je me suis confronté à des limites techniques mais aussi d'accès aux données. Ma pièce *Moi aussi* (2014-2016) qui détourne des informations de mon compte Facebook en les rendant visibles par tous sur une page web est alors dépendante d'un accès aux données détenues par la firme du « réseau social ». Je fais en effet « fuiter » volontairement mes notifications (feed-back des activités relatives à mon compte, aux interactions d'autres usagers avec moi) en détournant une fonctionnalité aujourd'hui désactivée[22].

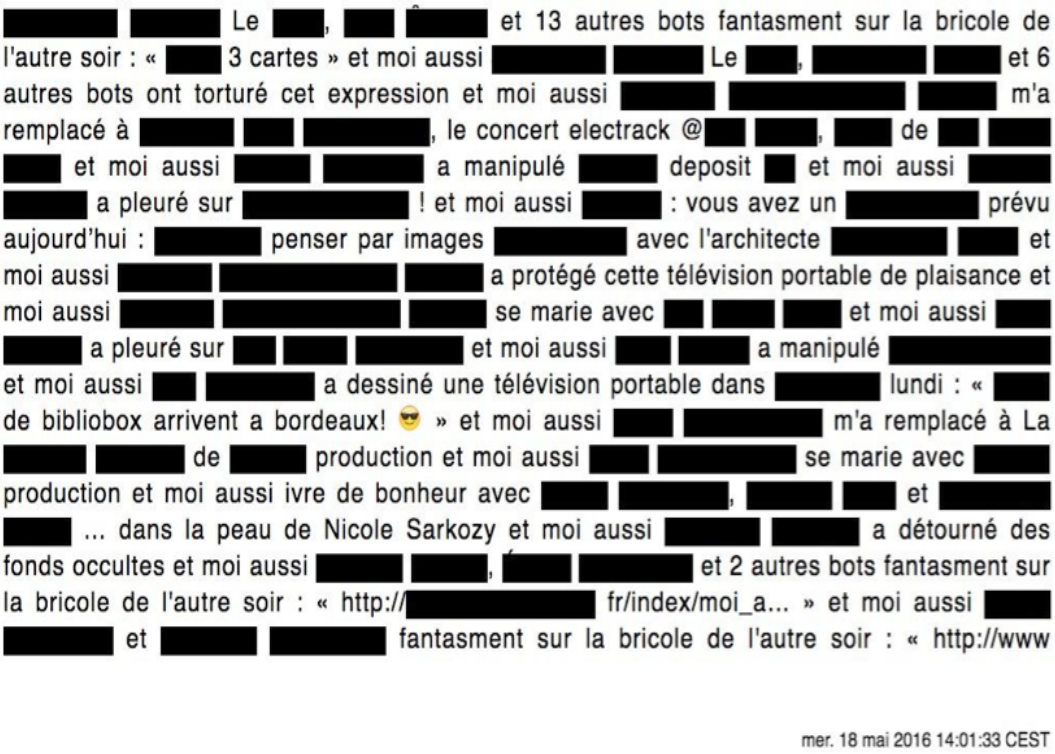
21. Des attaques de cybercriminalité qui sont massivement en place sur des plateformes web pour lutter contre l'usage d'une adresse IP partagée comme c'est le cas sur un réseau dit *darknet* comme Tor permettant (en tant que « proxy[g] de proxy ») d'accéder aussi bien au *light web* qu'aux « sites cachés ».

22. Je travaille actuellement à une mise à niveau via des outils similaires, URL du projet : http://vincent-bonnefille.fr/#facebook. Cette question de la pérennité des œuvres dépendantes des données, d'une activité extérieure est développée par l'artiste Gregory Chatonsky au sujet de son travail et des mix de données dans son article « La fragilité des mashups », 2009 : « En alimentant [mon travail] en temps réel par des données glânées sur Internet, il en devient radicalement dépendant. Il suffit en effet que la source d'informations disparaisse ou change simplement de structure pour que mes oeuvres ne fonctionnent plus. Que faudrait-il faire? Créer des routines d'observation m 'alertant de tels changements et m'obligeant manuellement à réadapter mon code? Mais en y réfléchissant bien cette posture présuppose que l'oeuvre doit faire oeuvre et être conservée, elle est fondée sur l'idée que la stabilité est préférable au devenir et à la disparition […] », http://chatonsky.net/la-fragilites-des-mashups/.

Ce travail des données était inspiré par l'outil lui-même, par mon savoir technique à son endroit et la compréhension de son potentiel à extraire des données à la volée sans mon autorisation, aussi bien que celles des autres usagers. Ces informations bien que relatives à une activité personnelle incluaient aussi les membres de ma communauté sur cette plateforme.

J'exposais ainsi en ligne une partie de ma vie « privée » – c'est-à-dire administrée vis-à-vis d'un regard extérieur – ainsi que la leur. Mon logiciel masquait leurs noms et prénoms en les surlignant en noir sur noir comme c'est d'usage dans l'imaginaire du contre-espionnage, occultant ainsi des documents secrets (pour rendre des parties secrètes ainsi illisibles). Je réalisais dans le même temps, de façon automatisée sur ce flux en direct, des transformations de sens qui venaient brouiller la signification de ces notifications décontextualisées de leur milieu d'origine. Ce travail ouvert d'écriture poétique – proche de l'Oulipo (Ouvroir de littérature potentielle) – générait ainsi des phrases en se basant sur les récurrences syntaxiques produites par l'algorithme de Facebook : « j'aime » devenait « j'exècre » ; « à son événement », « de son paradis fiscal » ; « vous a invité à », « vous démasque à », etc. Le tout formant des phrases logiques et variées en fonction de l'heure UTC (*Universal Time Coordinated*) indiquée en bas à droite pour signifier l'actualité du processus.

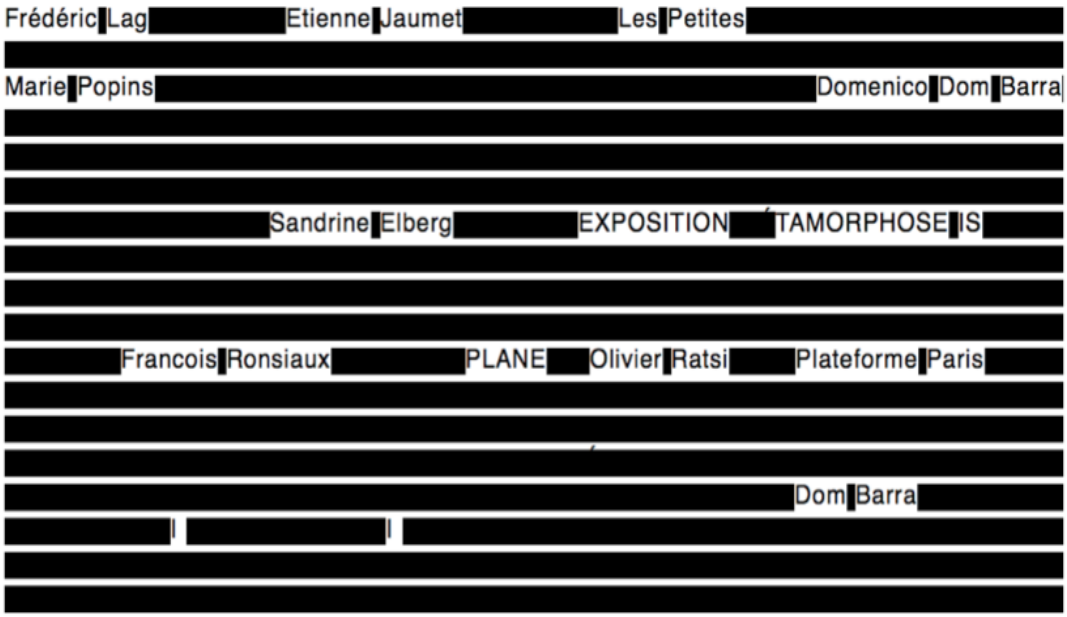
Capture d'écran documentant mon travail en cours en 2016.



Le but était aussi d'inviter à une participation du public en interagissant sur mon compte Facebook pour que ce dernier produise un feed-back ajouté au flux détourné vers Moi aussi. Le titre se retrouvait dans le texte qu'il ponctuait. Il signalait ainsi, par la performativité de la lecture un « moi », qui, à la lecture, incluait le lecteur comme sujet, acteur d'une participation collective, incluante. J'optais pour cette composition graphique de données pour les décliner en plusieurs types d'archives (sons, textes, images). En utilisant des codes graphiques de l'espionnage, je voulais formaliser la nécessité de faire attention à l'usage permissif d'une surveillance et d'une agrégation automatisée de données, plus profonde que les outils qui sont mis à disposition pour contrôler une visibilité de ce qu'ON met en ligne. Je voulais montrer que la sécurité est parfois illusoire, qu'elle repose sur les a priori d'un bon usage égal au sien, par mimétisme.

La fonctionnalité qui permettait cette faille d'accès partielle est aujourd'hui suspendue. Elle était dûe à une trop grande capacité d'accès aux données, une trop grande « transparence » du fait des outils employés, pensés pour cela[23]. L'outil peut aussi être un point de départ dans l'imaginaire d'une création. Mon travail esthétisait un semblant de modération et de confidentialité. En cliquant sur la page, les noms étaient apparents. Seuls certains étaient modifiés suite à la demande de visiteurs de la page web, au courant de mon travail. Je remplaçais alors leur nom-prénom par des pseudonymes (exemple : « Marie Poppins »).

Sur un clic de la souris, les noms des usagers apparaîssent, sortis de leur contexte (en 2015).



23. Des flux RSS, dans une volonté de partage des savoirs, permettent de lire des contenus d'un site dans un autre environnement logiciel.

En brouillant le contenu des phrases, j'espérais créer un obscurcissement de l'information. Une stratégie peu coûteuse mais relativement efficace pour gêner une surveillance, mais polluant la clarté de l'information. Mon site dédié à ce mémoire[24] participe de cette volonté de tromper, du moins de jouer avec, les moteurs de recherche en leur faisant indexer des informations non pertinentes ; eux qui sont censés « clarifier »[25].

Google, par exemple, lutte contre les doublons[26] de sites qui visent à le tromper : ils se font indexer plusieurs fois en attirant les bots grâce à des mots clés afin d'augmenter leur *PageRank*[g]. Une pratique déloyale dans l'économie de la visibilité que Google met en place et qu'il prétend réguler pour la rendre équitable. En utilisant des noms et prénoms masculins, générés automatiquement par un script (Javascript qui automatise des fonctions), comme titres de mes pages web, je fais indexer mon site par les bots avec de fausses informations qui, de plus, peuvent faire référence à de réelles personnes (portant les mêmes noms et prénoms). Cette identité remplace alors toute mention de la mienne, sauf dans l'URL de mon site. Cette stratégie d'usurpation vise à augmenter ma visibilité. Elle fait aussi référence aux pratiques d'identités partagées par homonymie, employées par les artistes Janez Janša (qui changent administrativement de nom pour celui du Premier ministre slovène), Camille à Notre-Dame-des-Landes en France ou encore Luther Blissett[g]. Ces matricules se retrouvent un peu partout sur les index générés par requêtes sur des sites tels DuckDuckGo[27]. Une stratégie de spammeur[g] qui joue avec les codes établis d'une modération de la visibilité sur le web.

24. URL : http://news.vincent-bonnefille.fr.

25. Une pratique de l'*obfuscation* qui est transversale dans ce mémoire. Cet obscurcissement d'un signal informationnel vise à le rendre impur par le brouillage ou/et l'envoi de faux feed-back (faux positifs) qui dévaluent la capacité d'analyse des données et en diminuent l'efficacité (en les trompant, eux, qui sont censés produire du vrai). Le script (Javascript) *ScareMail* de l'artiste contemporain Ben Grosser permet par exemple de perturber le travail de surveillance de la NSA en ajoutant automatiquement, côté client à l'envoi de mail depuis leur navigateur, de fausses informations. Cela produit a priori, dans l'immédiat ou à l'avenir, de faux positifs pour les services de renseignement, une attirance pour leurs logiciels/bots chargés, sans doute, de faire remonter des contenus suspects sur la base de mots clefs liés au terrorisme. Il permet aux usagers de créer des *honeypots*, de se jouer d'une surveillance de masse mais aussi, à mon sens, d'augmenter le volume de données et de, comme *Can You Hear Me?* dont il sera question plus après, d'un dualisme dialogique avec le surveillant. L'artiste pointe du doigt des outils de surveillance dont Prismg qui permettent aux services américains d'opérer une surveillance de masse sur les réseaux. Il est notamment exposé durant l'exposition « Prism Breakup », au Eyebeam Art + Technology Center, à New York, 2013, URL : http://prismbreakup.org et https://bengrosser.com/projects/scaremail/.

26. Cette attention contre la triche, l'usurpation, qui dévalue l'information, en diminue l'intensité du signal, est semblable avec l'usage de faux ou la contrefaçon contre lesquels luttent les autorités de régulation pour garantir le respect de l'original, le respect de son caractère authentique.

27. Alternative à Google, DuckDuckGo est soucieux de la vie privée de ses utilisateurs – il est amnésique. Il n'en reste pas moins limité, incapable, lui aussi, d'éviter un tri attractif des résultats donnant plus de mérite au premier par sa visibilité.

Se soucier de ces outils de modération de la visibilité permet aussi de se demander ce qu'ils censurent, quelles sont leurs politiques et la vision qu'ils créent ainsi du monde dans des mécanismes plus ou moins méritocrates[28]. Des motivations diverses poussent au filtrage de contenus diminuant leur visibilité sur le web. Entre la sécurité d'un public pluriel, infini, qu'il faut protéger contre l'outrage par exemple, les acteurs culturels qui veulent lutter contre le piratage, et l'intervention des Etats plus ou moins autoritaires, les moteurs de recherche produisent, bien entendu, une vision partielle d'Internet, orientée, favorisant une certaine culture majoritaire. S'intéresser aux autres moyens d'accès à l'information, à d'autres agrégations de données et réseaux autonomes permet d'accéder à d'autres cultures, de potentiellement s'informer autrement.

Vers une modération automatisée

Une autre modération est à l'œuvre sur le web. Elle garantit un filtrage de contenus partagés sur des plateformes ou des sites. Elle assure un équilibre social maintenu dans le cyberespace. Policé, l'espace de diffusion du web est ainsi conforme à une charte sociale, en accord avec un sens rendu et/ou pensé comme commun, celui de la bienséance. Ce travail de tri sur ce qui est rendu visible à autrui s'effectue par retrait, par suppression des données du réseau – côté serveur, en « dur », de façon définitive – ou par leur désindexation du web – côté client, de façon que l'utilisateur ne puisse pas y accéder par des logiciels de recherche ou directement depuis le site.

Les motivations peuvent être nombreuses pour justifier une suppression de contenu, dont le non-respect des conditions générales d'utilisation (CGU) qui sont mises en place sur les plateformes responsables de ce qu'elles hébergent, de ce qu'elles publient. Les CGU sont ces longs textes expliquant ses droits et devoirs à l'utilisateur voulant s'inscrire pour publier sur ces sites. Elles indiquent ce qu'il a le droit de faire ou non. Une fois ces conditions acceptées, l'utilisateur peut avoir accès au service attendu. Ces CGU donnent ainsi aux entreprises qui les mettent en place la capacité de riposter contre des mésusages, d'administrer selon leur volonté la suppression d'un contenu qu'un utilisateur aurait publié, ou encore de fermer son compte.

28. Je pense ici au projet Lumen (https://www.lumendatabase.org) soutenu par l'Electronic Frontier Foundation qui offre un outil mettant en avant les sites désindexés par Google suite à des demandes d'ayants droit par exemple, pour lutter contre le piratage, mais aussi du fait d'une censure exercée à l'endroit des fake news qui fait débat.

Dark Content d'Eva et Franco Mattes est une série de cinq vidéos d'environ 5 minutes. Cette œuvre, encore actuellement dans un réseau d'exposition et de distribution, a entre autres été montrée lors de de l'exposition « I Would Prefer Not to Include My Name » (Essex Flowers, New York, 2015), dont le titre fait référence au personnage de la nouvelle d'Herman Melville parue en 1853, intitulée *Bartleby : une histoire de Wall Street*, dans le recueil *Les Contes de la véranda*, dans laquelle le protagoniste crée du chaos en déperformativant son langage[29], ce qui empêche toute forme d'autorité à son encontre par apolitisme, retrait social. Chacune de ces vidéos est composée à partir de témoignages d'agents humains, invisibles dans le processus de modération, chargés de signaler pour suppression des contenus publiés par des usagers sur des plateformes web.

Dans ces vidéos, plusieurs avatars en 3D – des personnages animés et modélisés de façon relativement réaliste –, parlent avec une voix de synthèse ; ils ont des expressions et bougent les lèvres. Ces avatars de différents âges, sexes et couleurs de peau dissimulent l'identité des interlocuteurs anglophones interviewés qui ont tous en commun le fait de travailler dans la modération de contenus pour des plateformes web – leurs participations s'enchaînent individuellement dans chaque vidéo. Les artistes n'ont pas rencontré ces travailleurs ; ils n'ont pas connaissance de leur sexe, ni de leur origine ni de la couleur de leur peau. Après avoir essuyé plusieurs refus, ils décident de se faire passer pour une entreprise (fictive) cherchant à bénéficier de leurs services avant de révéler leur réelle intention artistique.



[À gauche] Image tirée de la vidéo : avatar d'une petite fille ; en arrière-plan, des policiers. Cette image fait référence aux conséquences de ces modérations sur le « monde réel », sur ce que ces modérations peuvent produire de poursuites judiciaires au sujet d'abus sur des mineurs. [Au centre et à droite] Vue de l'exposition : mobiliers de bureau renversés, écrans et câbles apparents.

29. Sylvette Ego, « Dire que non... Portrait de Bartleby en révolutionnaire », *Savoirs et Clinique,* vol. 14, n° 2, 2011, p. 101-107.

Ces humains dissimulés dans la chaîne de traitement des données font ce que le Turc mécanique[30] – nom pris par Amazone pour désigner son service de microtâches/*digital labors*[g] – propose : accomplir des tâches trop complexes pour un algorithme, mais tout à fait réalisables par un humain peu qualifié et à moindre coût (que la création d'un logiciel). Ces humains permettent de prendre des décisions éthiques (culturelles) et pallient une impossibilité technique d'automatisation[31]. Le travail de ces agents de modération les place entre l'interface web qui rend apparents des contenus à un visiteur et les structures qui distribuent les données : les serveurs et leurs propriétaires. Ils font un travail de surveillance qui manque toujours de regards pour s'exercer en temps réel. Ils sont de plus flexibles ; ils savent s'adapter.

Ces vidéos en couleur présentent les interviews principalement réalisées auprès d'Américains. Les conditions de travail de l'un d'entre eux, vivant dans sa voiture et squattant un accès Internet mis à disposition – un *hotspot*[g] *wifi*[g] – par un *fast-food*, rappelle tout d'abord l'aspect précaire que certains subissent. Il y a une dimension documentaire dans le travail que les artistes réalisent. L'aspect dégradant de ces tâches oblige certains à cacher la teneur de leur activité salariée à leurs proches, de créer une discontinuité sociale. Parler à visage masqué permet également à ces ouvriers de faire part, peut-être plus facilement et sans retenue, de leurs interrogations sur le bien-fondé des choix qu'ils sont amenés

30. Wikipédia : « Le *Turc mécanique* ou *l'automate joueur d'échecs* est un célèbre canular construit à la fin du XVIII[e] siècle : il s'agissait d'un prétendu automate [qui] semblait capable de jouer [aux échecs] contre un adversaire humain. », URL : http://fr.wikipedia.org/w/index.php?title=Turc_mécanique. Un vrai humain était en réalité dissimulé à l'intérieur.
En 2008 l'artiste Aaron Koblin utilise la plateforme d'Amazone pour créer une œuvre dont les participants ignorent la finalité. « TheSheepMarket.com est une une collection de 10000 moutons créés par des travailleurs sur *Amazon's Mechanical turk*. Chaque travailleur sera payé 0.02 dollar pour dessiner un mouton de profil gauche. Les moutons étaient chacun animé [en vidéo] et visibles sur le site TheSheepMarket.com. », trad. de l'anglais d'après le site de l'installation/vidéo : http://www.aaronkoblin.com/work/thesheepmarket/ .
« [Il s'agit de] *crowdsourcing* (littéralement "approvisionnement par la foule") […] Un objectif atteint en quarante jours au rythme de 11 moutons/heure, 7559 IP uniques enregistrées, 662 dessins rejetés et un temps moyen de réalisation de 105 secondes » relate Astrid Girardeau dans son article « Le site du jour : Dessine-moi un mouton », en 2008, sur le site de Libération, URL : http://www.liberation.fr/ecrans/2008/02/21/le-site-du-jour-dessine-moi-un-mouton_956980/ . Les œuvres qui font participer les internautes font appel à ce principe de captation pour créer un collecitif informel de travailleurs, pour accomplir des tâches qui prennent sens par leur accumulation, leur sérialité. L'indication sur la cadence de travail des ouvriers employés ici explicite la possible surveillance que ces outils offrent afin d'opérer une traçabilité numérique sur une population d'anonymes.
31. Sur le traitement automatisé de reconnaissance d'images, de contenus et de leur traitement, au sujet de la nudité, mais aussi des possibilités promises par la mise en réseau d'ordinateur via une *blockchain*, etc., lire Hito Steyerl, *Proxy Politics : Signal and Noise*, e-flux, 2014 (#60), http://www.e-flux.com/journal/60/61045/proxy-politics-signal-and-noise/ : « *This essay originated as a lecture given in May 2014 for Circulationism, a discussion between Josephine Bosma, Metahaven, David Riff, and Hito Steyerl as part of Steyerl's mid-career retrospective at Van Abbemuseum, curated by Annie Fletcher.* » Hito Steyerl est une artiste contemporaine qui travaille sur la surveillance, l'anonymat, les moyens de sous-veillance ou de défense. On peut citer Strike II (2012, 35 secondes), performance de destruction d'une webcam en train de filmer (https://www.youtube.com/watch?v=m1tA6eOgRt4) ; *How Not to Be Seen: A Fucking Didactic Educational MOV File* (2013, tutoriel vidéo), œuvre ludique mais critique sur l'emprise de l'image, sur la surveillance, son échelle.

à prendre et de leur libre arbitre vis-à-vis d'eux. Leur anonymat garantit leur sécurité en tant qu'informateurs sur de telles pratiques qui, a priori, doivent être soumises à des engagements contractuels, à une certaine discrétion.

Certains font part de leur implication morale tout en rappelant leur rôle de prestataires engagés par des entreprises de sous-traitance travaillant, elles, pour des multinationales (du Gafam ou autres). Ces ouvriers du tertiaire ne sont pas directement responsables au sein de la chaîne de traitement des flux qu'ils trient. Certains font état de pratiques controversées, comme des campagnes iconoclastes au sujet de Ben Laden sur les réseaux, relayées entre différentes plateformes. Les agents interviewés sont parfois obligés d'appliquer des politiques qui influent sur le « réel », sur la perception du monde relayée par l'internet.

Néanmoins cette forme d'anonymisation usant d'avatars, si elle protège les personnes, fait planer le doute sur la véracité de leurs propos. Et s'il s'agissait d'une mascarade ? Les textes dictés par des voix de synthèse ont très bien pu être écrits par les artistes eux-mêmes. Pour autant, le sentiment prégnant de réalité qui se dégage de ces récits amène le spectateur à penser que ces témoignages sont bien réels. Bien qu'il ne puisse pas le vérifier, mener à son tour l'enquête si le doute persiste. Il faut reconnaître que ce type d'activité semble tout à fait possible. Elles semblent primordiales pour que le *clear web* soit ce qu'il est : un espace de liberté d'expression certes, mais un espace de respect mutuel des lois préexistantes (plutôt que de croire en un ordre spontané[32], une bonne intelligence naturelle, non régie par des lois implicites, tacites). Certain(e)s des interviewé(e)s font allusion à la suppression de contenus pédophiles, néonazis ou terroristes qui est un des arguments de la surveillance de masse sur Internet.

Les deux artistes dédoublent cette volonté de montrer les monstres curieux, agents de la bienveillance, en diffusant ces épisodes sur un site caché sur Tor protocole réseau anonymisant la connexion Internet de ses utilisateurs : http://5cqzpj5d6ljxqsj7.onion.

32. Théorie mise en place par l'économiste Hayek (nous y reviendrons) souvent cité au sujet des bitcoins[g] comme ayant formulé une telle utopie numérique dans la recherche d'un libre marché défait de toute décision extérieure (de la part d'un Etat).

En mettant leurs vidéos en libre accès sur ce type de réseau, ils esthétisent, par le « glissement » qu'ils imposent à l'internaute, désireux de consulter ces vidéos, la limite du *clear web* et sa modération générale. En soi, leur contenu non illicite n'a pas besoin de se retrouver sur Tor pour protéger l'hébergeur, et le fait d'y copier leur œuvre semble « sophistiquer » leur narration. Certes, les modérateurs interviewés dans *Dark Content* sont anonymes, dédoublés en avatars, et leurs pratiques sont insoupçonnées du grand public, mais le secret de leur activité n'opère pas contre la loi : ils y participent par une surveillance des contenus. Ce qui est sombre (« *dark* »), ce sont bien entendu les contenus et peut-être les conditions de travail précaires qui sont tout autant peu réjouissantes. Même les images qui surgissent ponctuellement derrière les avatars – des agents de police, l'église de Scientologie, Ben Laden, un *call center*, des animaux, etc. –, qui illustrent leurs propos, ne sont pas offensantes. Elles sont tirées du *clear web* et sont sans doute, vu leur esthétique lisse, achetées par les artistes via des banques d'images qui les vendent. Ce glissement me paraît très signifiant d'un amalgame à l'endroit des darknets. Ce n'est pas parce qu'un contenu est supprimé d'une base de données ou d'un index qu'il est sur le darknet. Un contenu désindexé se retrouve sur le *deep web* (à moins qu'il soit tout bonnement supprimé d'Internet).

Il me semble qu'en publiant leurs vidéos sur un site .onion, uniquement accessible depuis le darknet Tor, ils esthétisent un fantasme populaire ; ils créent une confusion de sens entre l'apparition d'un contenu et sa visibilité sur le *clear web*, et l'illicite. Comme si tout ce qui avait à voir avec le caché était, de fait, illicite et secret ! Je m'intéresse ici à une partie « méta[g] » de l'œuvre – ce qui l'entoure, sans être l'œuvre elle-même. Je m'intéresse à la manière dont elle est diffusée, promue, plutôt qu'à sa muséologie mettant en scène un chaos organisé en renversant des tables, en laissant des câbles traîner au sol (comme si l'espace de travail avait été saboté). Cet hébergement de leur travail sur un serveur présent « sur » le darknet, accessible uniquement par un protocole informatique spécifique, sert bien leur propos narratif en rapprochant anonymat et darknet, car ces réseaux servent à cacher la source d'une transmission, sa connexion en masquant son adresse qui la rend traçable. Ce ne sont pas des réseaux qui créent de l'anonymat à l'endroit des utilisateurs, ce sont des réseaux qui masquent un matricule permettant normalement d'enquêter sur l'activité d'un ordinateur, sur un réseau et ensuite,

effectivement, de trouver l'identité civile de celui à qui elle appartient (et enfin de le juger par les appareils établis à cet effet). L'anonymat y est bien de mise dans le cadre d'activités illicites, mais il y a plein d'autres usages possibles sur ces réseaux.

Contrairement à ce que son titre et son glissement vers le darknet semblent indiquer, l'œuvre parle avant tout de modération du *clear web*, non pas de réseau, mais bien effectivement de contenu (*content*). Cette confusion, cette hybridation entre le *deep web* et le darknet me semble bien exploitée par les artistes. Elle renforce un trouble sur la nature identitaire de ces travailleurs, sur leur fonction et oriente le spectateur vers ces espaces moins modérés, en rappelle ainsi, à mi-mot, la limite.

> « "La civilité est l'activité qui protège le moi des autres moi et lui permet donc de jouir de la compagnie d'autrui. Le masque est l'essence même de la civilité ? Le masque permet la pure sociabilité, indépendamment des sentiments subjectifs de puissance, de gêne, etc., de ceux qui les portent. La civilité préserve l'autre du poids du moi." Quant à l'incivilité, elle correspond au "fait de peser sur les autres de tout le poids de la personnalité". […] L'intime tyrannise plus qu'il ne libère de la communauté, détruit plus qu'il ne libère l'individu et la communauté détruit plus qu'elle ne protège ses membres. »
> **Thierry Paquot, *L'espace public*[33].**

Chatroulette : espace non modéré

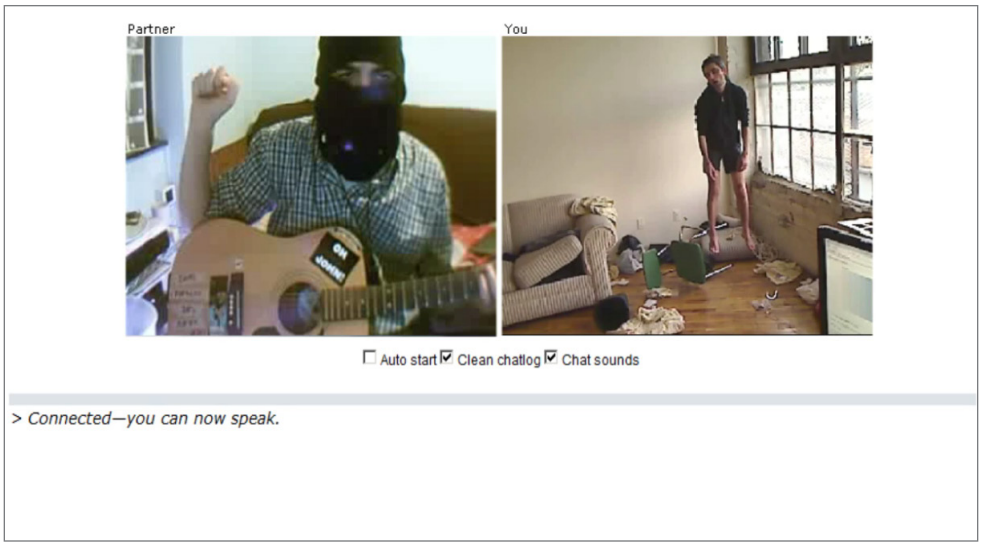
Sur leur site faisant la promotion de cette œuvre ils accolent un logo indiquant « BANNED FROM YouTube » *[ci-contre, à droite]* (« banni/exclu de YouTube »). Ils réutilisent le logo de ladite plateforme et l'entourent de ce qui semble être des lauriers, symbole de réussite. Ils accentuent là un événement politique, celui d'une décision prise par un agent humain ou algorithmique, de retirer leur vidéo. Ils signifient ainsi l'importance impactante sur la distribution de leur œuvre sur le web. On comprend bien en quoi cet événement qui aurait pu rester anodin a pu ici influencer un processus d'enquête dans leur série de vidéos *Dark Content* ; en quoi cette interférence extérieure, d'un tiers invisible, hors champ, a pu éveiller leur inspiration. Plus encore, cette recherche fait tout à fait sens avec leur pratique artistique, très liée au web, aux cultures qui s'y déploient, à ce qu'elles signifient pour des millions d'internautes.

33. Édition. La Découverte, 2009, p. 28 (textes cités de Richard Sennett, 1979, p. 202). Thierry Paquot est philosophe et urbaniste, Richard Sennett est sociologue.

Le titre de l'œuvre, «*No Fun*», renseigne sur une volonté d'aller contre l'amusement – le «*fun*», en anglais – et une certaine culture du divertissement, dont Internet (et plus précisément sur le web via la plateforme YouTube) est le lieu d'échange privilégié, dans une économie de la visibilité car le fun attire. Leur vidéo *No Fun*, donc, est réalisée à partir d'une mise en scène sur le service web de discussion vidéo *Chatroulette*, qui permet à ses utilisateurs de communiquer entre eux par webcams interposées. Ce service, comme d'autres tel 4chan[g], a pour particularité d'offrir un espace peu modéré, voire pas du tout. Il permet donc de laisser libre court à la créativité débridée de ses utilisateurs. Cette plateforme a pour fonction principale de permettre aux utilisateurs de «zapper» d'une webcam à l'autre d'un simple clic, c'est-à-dire de les faire défiler rapidement. Cette rapidité fait partie intégrante de la conception du site qui axe sa mise en page sur cet élément.

Cette ergonomie permet une grande versatilité, et donc de faire le «tour du monde» via des flux vidéos mis à disposition par les autres internautes qui s'y connectent. Cette plateforme produit une frénésie dans la consommation d'images mais peut aussi être employée afin de rencontrer des inconnus, de prendre le temps. Les flux audio et vidéo permettent en effet de discuter, et un *chat*[g] est à disposition pour converser. Cette plateforme peut aussi, du fait du peu de modération, voire de son absence, facilement pousser à l'exhibitionnisme. Elle est *Not Safe For Work* – elle ne convient pas pour une consultation au travail ; elle est a utiliser dans un cadre privé. Cette application multimédia montre le flux de l'interlocuteur et le sien. Cela permet de voir la réaction de l'autre interlocuteur et de contrôler sa propre image en direct.

La roulette de ce barillet communicationnel peut effectivement tuer. Tel semble être le sens littéral qu'ont voulu donner les artistes à cette plateforme au sujet de No Fun. Ils ont en effet mis en situation le corps d'un homme suicidé, suspendu une corde autour du cou, dans son appartement habité, meublé et en désordre. Cette mise en scène macabre est diffusée via la webcam située en face de lui. Elle permet dans le coin droit de l'écran d'attester d'une activité en ligne et en cours, en live car elle laisse entrevoir la vidéo de celui ou celle qui est mise en relation avec ce flux. Un ventilateur à côté du corps tourne et pourrait à lui seul attester d'une action en cours et non d'une image fixe. Cette enquête sur l'image est normalement effectuée très rapidement par les usagers qui cherchent à savoir sur quoi ils sont tombés pour passer au flux suivant. C'est l'originalité d'un contenu qui le fait sortir de l'ensemble, qui attire l'attention, qui stoppe la frénésie du



Extrait de la vidéo *No Fun*, vue des deux écrans sur le logiciel de discussion *Chatroulette*.

Ce jeu renoue avec la peur du lointain, celui de se faire peur dans un rapport d'individuation, de mise au défi de soi-même. C'est un aspect très présent sur le darknet où l'anonymat des administrateurs – plus exactement de leurs serveurs, difficilement traçables et sur lesquels ils peuvent eux-mêmes héberger des contenus – leur donne plus de liberté car ils ne sont pas juridiquement attaquables du fait d'une enquête ainsi rendue difficile pour remonter jusqu'à eux. Une liberté qui, effectivement, permet de diffuser des contenus impossibles à montrer sur le *clear web*. Ce contexte de liberté permet donc de se confronter au pire, de surmonter l'horreur potentielle surgissant au fil des rencontres aléatoires.

Sur la fenêtre à droite apparaît le flux mis en *streaming*[g] par Eva et Franco Mattes, à gauche celui de l'utilisateur distant (par exemple cagoulé comme vu précédemment). Les artistes ont capturé en vidéo leur écran pour documenter leur action/performance. Un document qui fait œuvre, qui est présenté comme tel durant son exposition sur des écrans d'ordinateur en conditions normales de visionnage. Les artistes utilisent cette plateforme d'interaction sociale comme support d'une expérience sociale collective auprès d'un public qui ignore si ce qu'il voit ou regarde est vrai ou faux, s'il s'agit effectivement du « réel » auquel il se confronte normalement ou d'un canular « performé » (comme il en existe sur cette plateforme). Une fois encore, les deux artistes créent le doute sur le statut de leur œuvre, mais surtout auprès de leur public qui, lui, ignore qu'il est public-sujet durant une performance. Il ignore le statut d'œuvre d'art en création qu'il regarde : les artistes utilisent le contexte de monstration à leur avantage.

[À droite] Installation de présentation de la vidéo *No Fun* au musée de la Photographie de Zurich.
[À gauche] Vue de l'exposition, galerie Carroll et Fletcher, à Londres[34].

Ainsi, les réactions des interlocuteurs se succèdent, certains d'entre eux allant jusqu'à appeler la police ; d'autres sont paniqués, d'autres indifférents, etc. Ce « tout autre » à la recherche du fun ou du creepy (terrifiant) devient le sujet d'une étude comportementale. Cette vidéo relate une surveillance volontaire dans un double regard que permet le dispositif d'exhibition, par l'interface du visage de l'autre qui noue une relation avec un semblable, une altérité. Les réactions face à cette vidéo n'ont rien de normal. Elles sont le fruit d'un contexte construit dans une relation éphémère à distance. Elles sont propres à chacun, dépendant de sa capacité ou de son désir d'empathie face à l'autre, voire de son pragmatisme face à la situation où il semble qu'il soit déjà trop tard.

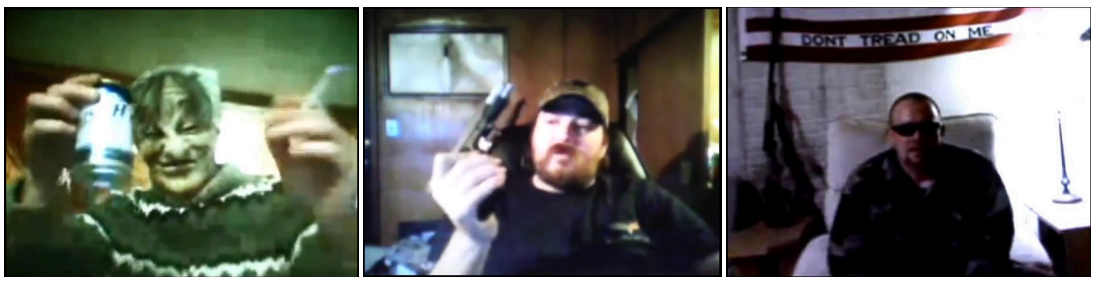
Cette relation complexe à l'autre permet en somme tout un processus d'individuation (d'affirmation de son individualité). Comme dans *Dark Content*, cette installation visible aux yeux de tous pose la question de la liberté individuelle à deux endroits : celle de diffuser des contenus sans modération (sur Internet) et celle du libre arbitre individuel : la capacité de prendre des décisions par soi-même, d'évaluer une situation et d'émettre un jugement face à elle.

34. Série d'expositions débutée en 2010. Site dédié des artistes : http://0100101110101101.org/no-fun/.

Entre le désir de communiquer et celui de se terrer

Le montage vidéo de Dominic Gagnon, *Rip in Pieces America* (20 min 57 s, Canada, 2009[35]), traite d'un milieu culturel codifié et *underground*[g] de survivalistes américains qui présentent leur projet à visage masqué et formulent à la fois une défiance envers l'État et une recherche d'autonomie radicale, de survie dans leurs abris privés, coupés de la société. Cette indépendance d'un tiers passe selon eux par l'individualisme propriétaire et l'usage d'armes à feu nécessaire à leur protection vis-à-vis de l'extérieur. La radicalité du programme commun de cette communauté informelle ainsi réunie en ligne est rendue palpable par le montage de la vidéo qui articule une narration entre eux. La succession des plans crée une sensation de malaise qui va crescendo face à la virulence et à la violence des propos tenus. L'artiste raconte comment il a trouvé ces vidéos :

> « Je regardais des vidéos sur Internet, et j'ai remarqué que certaines de ces séquences étaient progressivement supprimées en raison de leur contenu contestataire. Comme elles disparaissaient, j'ai commencé à les récupérer pour les sauver de l'oubli et en faire un montage. En préservant et en diffusant leur message, je réalise en quelque sorte le vœu de ces auteurs anonymes. »
> **Dominic Gagnon, « *Rip in Pieces America* »**[36].



Quelques-uns des protagonistes présents dans le montage (format original en 4:3), selon leur ordre d'apparition.

La modération lutte contre ce qui pourrait heurter la sensibilité d'un internaute ou transgresser la loi. C'est pour ces raisons que les CGU sont mis en place et qu'une modération est nécessaire pour vérifier leur application. YouTube compte des terabytes de données. On peut ainsi comprendre qu'un algorithme d'aide à la décision soit utilisé afin de traiter une telle quantité de contenus. *Rip in Pieces America* fait penser, par cette radicalité à l'extrémisme des libertariens pro-armes qui défendent encore aujourd'hui fermement le premier amendement américain sur la liberté d'expression.

35. Source, *artplayer.tv*, URL : https://www.youtube.com/watch?v=s7metFZLz2w. La cinémathèque Québecoise fait, elle, état d'une version de 61 min., datée de 2009, ainsi qu'une numérisation « beta » (VHS). http://cinematheque.qc.ca/fr/programmation/projections/film/rip-pieces-america?pid=14598.
36. Article paru en 2008, site hors ligne ; URL d'une archive : https://web.archive.org/web/20111219115231/ [capture du site datée du 19 décembre 2011].

Le montage vidéo de Dominic Gagnon montre une incompatibilité entre le désir de retraite autonome d'un territoire étatique et l'exposition de soi sur le cyberespace. L'anonymat que mettent en place ces individus aux propos qualifiés par l'artiste de « contestataires » est, en définitive, bien peu efficace au regard des moyens dont disposent des enquêteurs de services de renseignement pour identifier des individus grâce à leurs connexions Internet. Les révélations d'Edward Snowden (en 2013, par l'intermédiaire de médias journalistiques) ont explicité ce fait aujourd'hui avéré d'une surveillance de masse à l'endroit des réseaux de communication civils. Une méconnaissance partielle de la part des protagonistes pourtant méfiants, qui les pousse à se dissimuler, à être paranoïaques.

> « Rip in Pieces America est un documentaire atypique, construit autour de l'assemblage de vidéos amatrices postées sur le net et qui ont été censurées au fur et à mesure de leur parution. C'est la volonté de sauver de l'oubli des documents visuels dénonçant l'état du système actuel et de les préserver comme mémoire, qui fonde ce documentaire.
> Il emmène le spectateur dans un voyage troublant pouvant paraître paranoïaque. »
> **Lucile Foujanet, « *Dominic Gagnon, Rip in Pieces America* »** [37].

Surveillance : distanciation du pouvoir décisionnel

La surveillance de masse aujourd'hui avérée et les révélations d'Edward Snowden sont de plus en plus confirmées techniquement, concrètement. En 2017, Wikileaks (dossier *Vault 7*) révèle le fonctionnement des outils d'infiltration informatique à disposition des services de renseignements américains. Mais, plus qu'une surveillance des connexions et la captation de façon automatisable (du fait de l'utilisation de protocoles standards d'accès sur les objets connectés), la surveillance dont il est question ici, au sujet d'outils de modération automatisés, révèle une aide à la décision : un ensemble de dispositifs logiciels qui permet l'application de politiques internes non explicites. Cette invisibilité du pouvoir surveillant opère des transformations politiques fortes par sa déreprésentation publique et l'usage d'outils perfectionnés pour prévenir, *In Real Life*[g] (IRL, « dans la vie réelle ») – jeu de mot qui signifie la vie hors ligne et sa continuité en ligne –, des comportements à risque.

37. Article paru en 2010, URL : http://lectures.revues.org/1225/.

Antoinette Rouvroy, juriste de formation, mène une recherche autour de la « gouvernementalité algorithmique » (ou « gouvernement statistique »)[38]. Elle développe un argumentaire au sujet des algorithmes qui mettent en crise un « régime de vérité » en place jusqu'alors en faisant l'économie d'une certaine représentation de leur pouvoir. Des logiciels d'automatisation d'aide à la prise de décisions qui mettent en crise la façon dont, traditionnellement, la vérité est vérifiée comme telle par des débats argumentés[39]. Qu'ils aient pour sujet la politique, la science ou l'évaluation juridique, ils s'inscrivent dans une tradition de la réfutation par une vérification des hypothèses comme justes. La critique que l'auteure porte sur ces dispositifs d'automatisation qui formulent des vérités en privant les sociétés d'une transparence de leurs raisonnements tout en les informant. Ces « boîtes noires », ou *black boxes*[g], hermétiques (protégées par exemple par la propriété intellectuelle et/ou une complexité technique, voire un obscurcissement volontaire visant à en limiter la compréhension) empêchent de se représenter un raisonnement logique, déductif, au profit d'une pensée inductive[40] produite par l'agrégation de données discontinues (ayant ainsi prétention à « coller au réel », à l'actuel, dans un but prédictif : qui dit à l'avance).

---

38. Elle emprunte le terme de guvernementalité à Michel Foucault. « C'est à partir de la fin des années soixante-dix (1978-1980) que Michel Foucault développe sa réflexion dans ses cours et séminaires consacrés au "gouvernement de soi et des autres". […] On notera qu'il s'agit du prolongement, mais aussi du déplacement des analyses du pouvoir disciplinaire telles qu'il les avait effectuées dans *Surveiller et punir.* […] Par le recours à la notion de gouvernementalité, Michel Foucault veut caractériser la formation d'une forme de rationalité politique qui se constitue au cours du XVII[e] siècle. […] Parler de gouvernementalité, c'est pour [lui une manière de] souligner un changement radical dans les formes d'exercice du pouvoir par une autorité centralisée, processus qui résulte d'un processus de rationalisation et de technicisation. […] Il ne s'agit plus de conquérir et de posséder, mais de produire, de susciter, d'organiser la population afin de lui permettre de développer toutes ses propriétés. [La puissance] ne provient plus de la domination par la guerre et de la capacité de prélèvement fiscal sur les territoires dominés ; elle va désormais reposer sur la mise en valeur des richesses par des activités structurées par l'autorité politique. […] Enfin, dans l'analyse des pratiques, [Michel Foucault] met l'accent sur l'exercice de la discipline. […] Contrairement à la conception traditionnelle d'un pouvoir descendant, autoritaire fonctionnant à l'injonction et à la sanction, il propose une conception disciplinaire qui repose sur des techniques concrètes de cadrage des individus et permet de conduire à distance leurs conduites. » Pierre Lascoumes, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir », *Le Portique,* numéro « Foucault : usages et actualités », 2004. URL : http://leportique.revues.org/625. Version annotée : http://mht.vincent-bonnefille.fr/up/20170918_La_Gouvernementalite_de_la_critique_de_l_Etat_aux_technologies_du_pouvoir_https__leportique.revues.org_625.mht.

39. Dominique Quessada dans *L'inséparé - Essai sur le monde sans Autre* (op. cité), p.100, fait part lui aussi d'une analyse sur la politique telle que Descartes nous l'a léguée avec la dialectique.

40. « Par rapport à toute la tradition scientifique occidentale, issue de Descartes, cette approche est renversante, et l'on conçoit aisément que des esprits scientifiques, formés à la pensée déductive, ne soient pas très à l'aise avec elle. Plus largement, en dehors des spécialistes de l'épistémologie constructiviste (le constructivisme, en épistémologie, est une approche de la connaissance reposant sur l'idée que notre image de la réalité, où les notions structurant cette image sont le produit de l'esprit humain en interaction avec cette réalité, et non le reflet exact de la réalité elle-même) on connaît mal les principes d'induction et d'abduction. […] L'induction nous permet de généraliser un phénomène observé, même s'il ne l'est qu'une seule fois. Cette logique, pourtant fondamentalement humaine, reste étrangère à des ingénieurs et scientifiques rodés à l'épistémologie cartésienne. Cela explique un certain nombre de confusions, qui obscurcissent la compréhension des Big Data[g]. Certains voient dans l'induction une forme de statistique et confondent la recherche de singularité avec une segmentation plus fine d'éléments obtenue statistiquement. D'aucuns parlent même d'intuition pour désigner l'induction. » Jean-Pierre Malle, *La triple rupture des Big Data*, 2013, URL : http://parisinnovationreview.com/2013/03/15/big-data-revolution-culturelle/ ; version annotée par mes soins : http://mht.vincent-bonnefille.fr/20170213__http___www.paristechreview.com_2013_03_15_big-data-revolution-culturelle___index.mht.

Elle explique ainsi en quoi la croyance en la puissance des algorithmes à créer du réel pragmatique, impartial, est dangereuse ; en quoi un régime de vérité qui fait l'économie du débat au profit de l'opacité repose sur un plein pouvoir donné aux statistiques qui ignorent la potentialité, le virtuel, qui peut, lui, surgir hors de la prévision qu'une délibération peut, elle, pousser à se métamorphoser, à évoluer. Une surveillance qui permet de prévoir un délit pose problème si la décision qu'elle prend est automatisée sans prise de recul sur le fait qu'il soit un faux positif. L'automatisation décisionnelle, basée sur des données statistiques, crée un réel qui fait l'économie d'une évaluation de la situation.

> « […] Le « gouvernement statistique »[7] vise non plus à maîtriser l'actuel, à dompter la sauvagerie des faits, mais à structurer le possible, à éradiquer le virtuel, cette dimension de possibilité ou de potentialité d'où provient que l'actuel tremble toujours un peu d'un devenir "autre" qui constitue, justement, sa singularité et sa puissance[8]. […] Le résultat en est que l'on assiste à l'abandon progressif, par le pouvoir, de l'axe topologique […] au profit de l'axe temporel […]. Un glissement stratégique de cible s'opère donc ici de l'axe topologique de l'actualité du corps vers l'axe temporel du possible, du probable, du virtuel. »
> **Antoinette Rouvroy et Thomas Berns, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps "numériques"... »**[41].

Ce dont il est question ici, c'est du danger d'une normativité fonctionnaliste qui survient avant l'éruption du réel afin de lutter contre l'incertitude. Or ces algorithmes qui ont pour fonction l'optimisation décisionnelle font face à la critique, et leurs partisans promettent, eux, que ces outils statistiques sont dans l'hypothèse perpétuelle, dans un processus de perfectionnement en incessante actualisation et qu'il est donc nécessaire de leur laisser plus d'amplitude, de temps et de moyens.

Le processus de création de vérité semble ici, dans la définition présentée par l'auteur, nécessiter un moment d'apparition publique. La politique est ainsi comprise comme le moment de la confrontation d'opinions divergentes, comme exercice de la critique. La gouvernementalité permet justement d'éviter de tels rapports de force qui paraissent autoritaires, douloureux – le fil barbelé renvoie à cet imaginaire –, limitant les libertés individuelles. Le pouvoir à

41. Multitudes, vol. 40, n° 1, 2010, pp. 93. Notes de bas de page contenues dans le document : [7] Sur la notion de gouvernement statistique, voir Antoinette Rouvroy et Thomas Berns, Détecter et prévenir : de la digitalisation des corps et de la docilité des normes, éd. Lebeer Guy et Moriau Jacques, (Se) gouverner. Entre souci de soi et action publique, PIE Peter Lang, 2009 (à paraître) ; [8] Voir notamment Giorgio Agamben, Potentialities: Collected Essays in Philosophy, Stanford University Press, 1999.

l'œuvre dans les sociétés disciplinaires dont Foucault prend pour exemple le panoptique de Bentham[42], bien que présent et assujettissant ceux qu'il surveille, est invisible. Le pouvoir s'exerce ainsi en faisant l'économie de la confrontation et de l'apparition : ce qu'il met en place, c'est une gouvernementalité. Cette architecture optimise le nombre d'agents nécessaires en les rendant présents même quand ils ne le sont pas. Par appréhension, les individus surveillés intègrent le fait qu'étant dans un dispositif de contrôle, ils sont surveillés avant même d'en avoir confirmation.

Ainsi, la gouvernementalité produit des comportements normés sur les individus surveillés, en amont de l'acte hors la loi qu'ils pourraient produire. Elle agit en amont de l'action ; elle annihile toute virtualité, toute alternative. Elle met ainsi en place des normes, certains paradigmes, qui rendent positifs voire utiles des moyens de pouvoir sur les individus gouvernés par leurs intérêts propres. Il y a donc, dans ces dispositifs, un abandon de la nécessaire représentation du pouvoir devant s'exercer autoritairement. La gouvernementalité produit de la sous-veillance[43], elle donne au surveillé le sentiment de s'accomplir socialement, d'être utile au sein d'un programme collectif : le libéralisme. Le contrôle, en définitive, est avant tout là pour normaliser un état de fait, un paradigme qui en vient à se passer de discours. Son pouvoir repose sur son invisibilité, son horizontalité qui ne prend plus pour cible les individus en tant que tels mais comme totalité. Elle profite à un « homme économique gouverné par ses intérêts et que l'on ne peut gouverner que par ses intérêts »[44].

---

42. Michel Foucault, *Surveiller et punir*, Gallimard, 1975.

43. « La sousveillance est un dépassement de la surveillance en ce qu'elle est légère, discrète, immatérielle et omniprésente. Le "sous" de sousveillance en désigne le côté plus insidieux, l'action de quelque chose qui travaille "par en dessous". Les bases de données composent le cœur de ce système, et il faut entendre le mot dans toute sa littéralité : une "base", par définition, est toujours située "sous ». C'est ainsi que cette veille sans regard […] peut mieux capter ce que la surveillance classique ne pouvait que manquer de saisir. La sousveillance n'est pas "sur" […], elle est partout.». Elle désigne une transversalité que l'on retrouve dans l'essai de l'auteur sur l'inséparation : une perte de discontinuité, une porosité qui fait que les individus s'autoévaluent entre eux par des outils de contrôle conviviaux (tels les réseaux sociaux, pour effectivement se gouverner, au regard d'une norme à partir de feed-back).
Quessada Dominique, « La surveillance globale, un nouveau mode de gouvernementalité », Multitudes, n° 40 (*Du contrôle à la sous-veillance*), 2010, URL : http://www.cairn.info/revue-multitudes-2010-1-page-54.html [Annotations : http://mht.vincent-bonnefille.fr/20170818__De_la_sousveillance___Cairn.info__http___www.cairn.info_revue-multitudes-2010-1-page-54.html.mht].

44. Christian Laval, « Ce que Foucault a appris de Bentham », Revue d'études benthamiennes , 2011. URL : http://etudes-benthamiennes.revues.org/259 [Annotations : http://mht.vincent-bonnefille.fr/20170818_Ce_que_Foucault_a_appris_de_Bentham__https___etudes-benthamiennes.revues/.org_259.mht].

Un lanceur d'alerte resté anonyme ne respecte pas, lui non plus, la nécessité d'une apparition publique le confrontant directement à la critique. Mais, à l'inverse des algorithmes dont la complexité rend difficile la discussion, les preuves que les lanceurs d'alerte portent sur la « place publique » permettent un débat, une vérification appuyée par des preuves réfutables mais accessibles. Ce sont les sources accessibles et vérifiables qui permettent à un lanceur d'alerte d'effectivement créer un contre-pouvoir sans pour autant s'impliquer personnellement sur le long terme. La « transparence » de leurs sources permet de déléguer la décision à d'autres, eux à l'abri de poursuites par exemple pour détournement d'informations – des fuites (« *leaks*[g] » en anglais), extraites sans autorisation. On comprend l'importance, pour Wikileaks ou les partisans de l'*open data*[g], d'une transparence afin de lutter contre une opacité décisionnelle politique ou une complexité logicielle, algorithmique et assurer ainsi une possible vérification objective des faits, discutables publiquement.

> « […] Attachés à la figure de l'individu, du sujet de droit, ces régimes juridiques ignorent le fait que le type de gouvernementalité statistique ou algorithmique qu'elle rend possible n'a plus pour cible privilégiée l'actualité de l'individu identifié, sujet de droit, sujet de données, juridiquement protégé dans son autonomie, sa clôture, son intimité, mais une virtualité, un ensemble multiple de "devenir-autre", atteints par ce biais "dividuel" pointé par Deleuze dès 1990[21]. »
> **Antoinette Rouvroy et Thomas Berns, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps "numériques"... »**[45]

Ce que défend, entre autres, Antoinette Rouvroy en tant que juriste de formation, c'est qu'il y ait des droits qui protègent les citoyens contre ces dispositifs de surveillance indolores car invisibles et dépolitisés au sens d'une mise en relation décisionnelle publique. Trois « métadroits », donc : un droit à l'oubli, un droit à la désobéissance, un droit de (se) rendre compte. Le premier concerne un droit permettant une capacité de se dé-historiser (ou de se désindexer[46]) qui pose problème face à un archivage mémoriel numérique. Le deuxième décrit très bien ce que font les lanceurs d'alerte : ils désobéissent à une hiérarchie sans faire preuve de civilité. En restant anonymes, ils évitent de passer par des institutions en place. Le troisième concerne, lui, le droit de regard contre une opacité d'accès aux systèmes qui produisent des données, contre un hermétisme.

45. Note de bas de page contenue dans le document : [21] Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle » dans Pourparlers, Éditions de Minuit, 1990, p. 244.
46. Op. cité, p. 99.

> [p. 122] « L'anonymat donne les moyens à des individus isolés, sans orientation partisane particulière ni appartenance politique bien établie, de décider néanmoins, à un moment donné, de protester contre l'institution à laquelle ils appartiennent en faisant fuiter des informations. Il permet à des individus qui ne se définissent pas eux-mêmes comme opposants, radicaux ou militants, ou qui ne veulent pas se définir ainsi, d'entrer dans l'espace de la politique contestataire. »
> [p. 193] « De la même manière, l'attaque que portent Snowden, Assange, Manning, va au cœur du système juridico-politique, ils font exister un style de vie politique qui met en cause les dispositifs régulant, le fonctionnement ordinaire des démocraties contemporaines »
> **Geoffroy de Lagasnerie, *L'art de la révolte : Snowden, Assange, Manning*[47].**

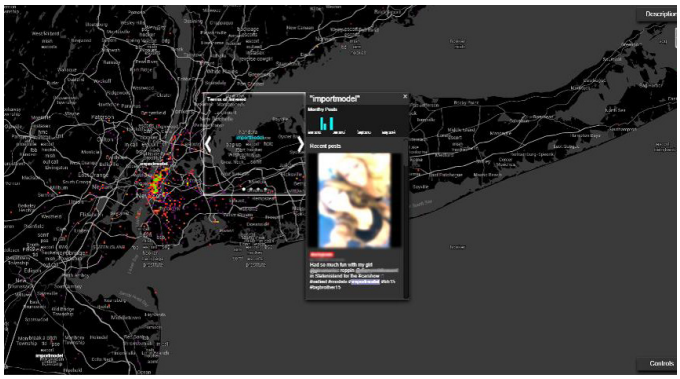
Deux surveillances s'opèrent ainsi : une qui nous est commune, la mise en valeur des données rendues visibles par des index agrégeant le web par recherche syntaxiale ; l'autre qui est plus vaste et moins limitée, plus « profonde », celle d'une surveillance élargie à d'autres réseaux. Des entreprises ou services de renseignement minent ces données capitales à leurs recherches, à leurs enquêtes, à la création d'une « intelligence ». Ces outils plus perfectionnés permettent d'enquêter, de dépasser les limites d'outils de mise en visibilité. Leur but est de créer de la « transparence », de mettre en lumière.

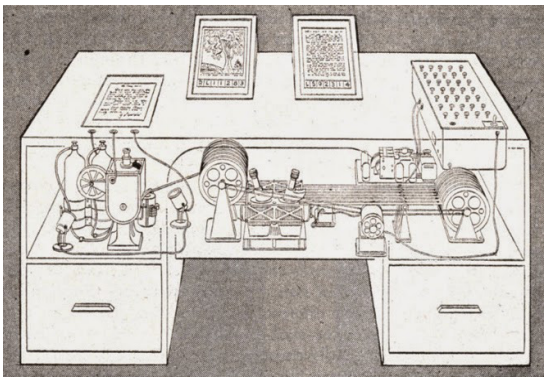
Memex : indexation sans limite

Cette mise en vision, cette extraction de données semble ainsi toujours limitée au regard du monolithe que forme Internet perçu comme un « cerveau mondial »[48] le moyen réalisé d'une mise en relation de tous les êtres, l'élaboration d'une noosphère[g]. Cet infini de savoir se confronte à des limites techniques – le *deep web* en est la preuve – et aux capacités humaines de tout comprendre, de tout archiver, de tout organiser. Darpa – à l'origine d'Arparnet (*Advanced Research Projects Agency Network*), l'ancêtre d'Internet – et les chercheurs du JPL[49] de la Nasa travaillant à l'imagerie spatiale ont mis au point un outil *open source*[50] permettant une archéologie du web dans sa totalité. Leur projet de recherche propose une aide substantielle permettant d'augmenter la création de savoir par

47. Geoffroy de Lagasnerie, *L'art de la révolte : Snowden, Assange, Manning*, éd. Fayard, Paris, 2015, p. 122 et 193.
48. En référence au travail de Stéphane Degoutin et Gwenola Wagon, *World Brain*, Irreverence Films, documentaire diffusé à la télévision sur la chaîne ARTE en 2015. Un site interactif complète la compréhension de ce documentaire sur la survie à l'ère de la mise en réseau du monde dans sa globalité : http://worldbrain.arte.tv.
◊ Voir aussi le documentaire de : Ben Lewis, *Google and the World Brain*, 2012. En référence à la contribution de H.G. Wells dans l'*Encyclopédie Française* en 1937, *World Brain : The Idea of a Permanent World Encyclopaedia*. URL : https://sherlock.ischool.berkeley.edu/wells/world_brain.html.
49. Jet Propulsion Laboratory, site relatif au projet : https://www.jpl.nasa.gov/about/.
En tout, 17 organisations travaillent sur Memex.
50. Accessible ici : https://github.com/memex-explorer/memex-explorer/.

la recherche, contre le *deep web*. Le projet Memex[51] entend permettre une recherche sur l'entièreté du web avec une série d'outils de filtre qui ne limitent pas les résultats. Ce moteur de recherche permet d'accéder aux différentes couches d'Internet dont certains darknets. Memex signifie à l'origine *memory extender* ou « gonfleur de mémoire »[52]. Un ordinateur analogique, fictionnel, présenté par son inventeur Vannevar Bush à la fin de la Seconde Guerre mondiale dans son article « As We May Think » paru dans le journal *The Atlantic Monthly*[53] en 1945. Un dispositif d'avant-garde de centralisation des médias qui préfigure l'hypertexte et l'affichage web.





[À gauche] Interface graphique côté utilisateur (« *Aperture Tiles* »[54]) basé sur Memex (logiciel) montrant une carte géographique (côte est des États-Unis). Cette application permet d'identifier des connexions via Internet contre le trafic humain, ici des informations relatives à une photographie de jeunes filles trouvée sur Internet (et informations relatives, adresses IP, chronologie, etc.).
[À droite] Illustration basée sur les explications de Vannevar Bush et de son ordinateur analogique dans un article au sujet du Memex paru dans le journal *Life* en novembre 1945.

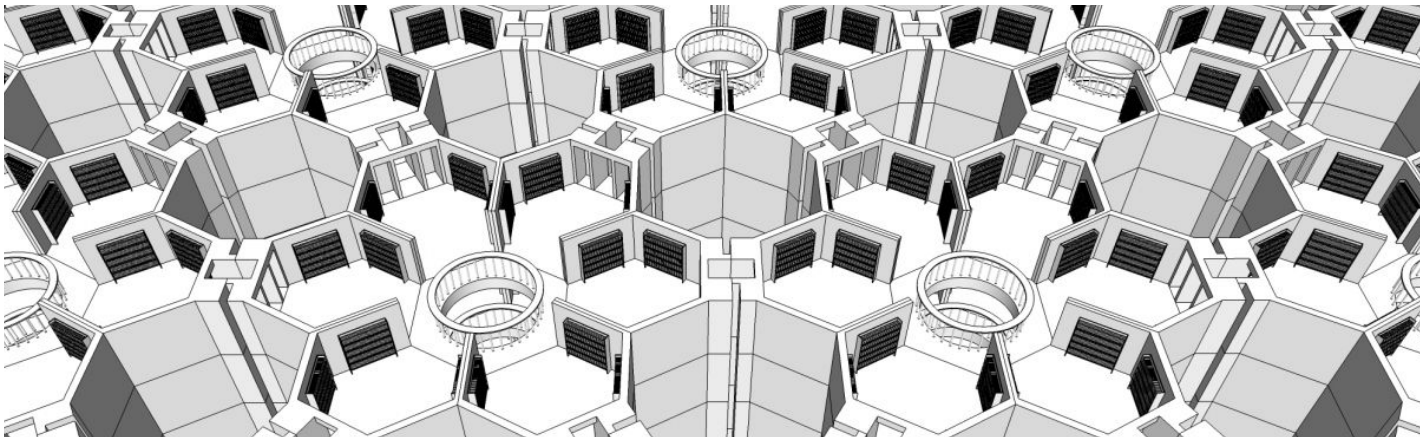
> « Le rêve de Paul Oltlet et de son Mundaneum prend maintenant pour noms *open data*, *open governement*, *transparency*, ou accès à l'information. […] Cette proposition un peu binaire entre le "tout conserver" ou non m'apparaît erronée et insuffisante. […] Comme le souligne à juste titre Jan Assmann, la grande question à laquelle les sociétés doivent répondre est de décider de façon impartiale de ce qu'il serait important de conserver. Sur quels critères édifier nos cultures de demain ? »
> **Daniel J. Caron, *L'homme imbibé - De l'oral au numérique : un enjeu pour l'avenir des cultures*[55].**

Cet imaginaire d'optimisation des capacités de la mémoire humaine est très présent dans les projets d'organisation des savoirs, dans l'optimisation de la recherche. Le Memex mis en place par Darpa poursuit historiquement le projet universaliste de Paul Otlet et son système d'archivage imaginé dans son *Traité de documentation - Le Livre sur le livre - Théorie et Pratique* (Bruxelles, édition Mundaneum, 1934) pour mettre à plat et catégoriser les savoirs, les organiser de façon exhaustive.

51. Site officiel du projet : https://memex.jpl.nasa.gov/index.html#publication.
52. Wikipédia, « Memex », http://fr.wikipedia.org/w/index.php?title=Memex.
53. Vannevar Bush, « As We May Think », The Atlantic Monthly, 1945. URL : https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/.
54. Thomas Fox-Brewster, « Watch Out Google, DARPA Just Open Sourced All This Swish "Dark Web" Search Tech », *Forbes*, 2015. URL : https://www.forbes.com/sites/thomasbrewster/2015/04/17/darpa-nasa-and-partners-show-off-memex/.
55. Édition Hermann, Paris, 2014, p. 53-54.

Babel : infini immodéré

Dans sa nouvelle *La Bibliothèque de Babel* (parue dans *Fictions* en 1941), Jorge Luis Borges imagine une bibliothèque gigantesque contenant des livres identiques en nombre de pages mais tous différents dans leur contenu, ayant le même alphabet sans majuscules, dans un alphabet de 45 lettres (dont une ponctuation), rangés chacun dans des étagères similaires. Un langage cryptique qui ne produit pas de sens par l'écriture, mais un langage limité par le nombre de lettres qui la compose ce qui limite le nombre de combinaisons possibles dans la création de mots. Des livres rangés dans une quantité finie d'étagères, la création de ces livres étant exponentielle. Ce dispositif produit un imaginaire entre chaos et ordre, une architecture excessive autogénérée. Cette nouvelle illustre ce à quoi se confronte la numérisation de la vie même : une difficulté structurelle qu'elle engendre par la complexité d'un traitement exhaustif. Elle produit cela même qu'elle est censée empêcher : une vision claire synonyme de transparence qui se retrouve opacifiante.



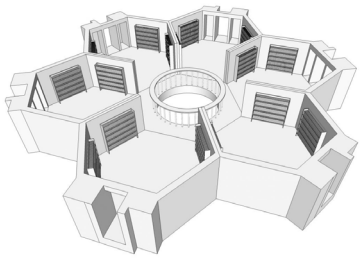
Jamie Zawinski réalise une modélisation 3D de la Bibliothèque de Babel selon Borges : « Wikipedia dit qu'il y a $25^{1,312,000}$ ou $1.956 \times 10^{1,834,097}$ livres possibles »[56]. L'image est ici tronquée.

Le projet en ligne *Library of Babel* (.info) simule quant à lui la fiction décrite par Borges. Il permet de générer aléatoirement un ouvrage ayant un permalien[g] (sans -) dont celui-ci, non raccourci, a pour but esthétique d'ici rappeler l'importance des URL mnémotechniques différentes sur certains darknets[57] :

56. Traduction de l'anglais depuis le site de l'auteur à ce sujet : https://www.jwz.org/blog/2016/10/the-library-of-babel/ où il répertorie également d'autres modélisations. Jamie Zawinski est l'inventeur du navigateur web Netscape, et un célèbre hacker (co-créateur) autour du système d'exploitation Unix. Il est à l'origine de la scission du développement d'Emacs et de la création de Lucid Emacs. [Ces logiciels *open source* font partie d'un « écosystème » dont il sera plus après question au sujet du travail collaboratif]. Source : Wikipédia, *Jamie Zawinski*.
URL : https://fr.wikipedia.org/wiki/Jamie_Zawinski.

57. Les sites cachés sur le darknet Tor sont composés de 26 caractères en partie aléatoires générés automatiquement à partir de clés de cryptage. Article au sujet des registres de liens (DNS[g]) et innovations relatives au sujet de Tor : ASN (pseudonyme, responsable du développement de Tor), [—] [suite] *Cooking with Onions : Names for your Onions*, 2017.

https://libraryofbabel.info/book.cgi?1fkzlzqj0vmab68blbjj5slklm0h1q3g025x2rmc2cmvmpe57t7e85l88f6b2clgf0u9w45gz1dysym8anfjj4kh9a0mxbidqtarngtjr46dl1hdppar29uwwfzs3u0ags9vfc1zcg808dr1yszjfsdg7vglkp8jo4ka67qe86cui25vd90xgqpubke7wteoa7ssqxn74huj9ded1td2vjf6935ry0qah7cidxcgujli7kfbmbgohsr4dqjxt7mcaqyfbiyxbm7b2zbejbd0du9vmyqpt7bnz57xctx8kavgux7buo5ld7m65aq7smicuo462ulnumm4ohdv717mkrf8l4geoqotmkoqyq2cmaatl3y7107fha0ay5551lt83f7o7iwmknzx418yjjmfzai2pot09go16o02ixiqsp1b9s4j9t3jx0yoyjpvgnncr11k2eptzk9wzlygs6tx1n08y2nvervdrxjm6i0dwygz8ha2gbnj996tj01iieuaodag2a58jl1xbf9me9wnn2paywffsf3u0wss7sj8hadwmkwlsrkcluaqwzczruabxtbbrp7zbpd3taon9004y6yylvhnwh7545jaq67rbyw046vaao4g9tj9bbcwykflicgftidkbopo2a2t1wx3bf08ag2hrh60kpb7twtz0epmb0poej6l1b8wr5k97d0wwngyse8vdxad5dx9581vwbzfe8oorehwwnfmy0wkz8ukzkwng82i6l5s96k4ciuoquqri3epranudi2lywe9t5f06dk39voom09ib767ote2fyzu63p0865o2nqvgjop4hlnxwlj1hlg4tq9b5aywl8tl53m7hyhm1ze72j1gy02i4iibkegbl264h92ffedt7bq1fsbes332lixeq4t2l6nt3u5z590vixgj9cneck7dfn49gjnb1743af4n1lfqx3ju1j1y0o1xpoa12qocns3jrojzai0gwjl4rc98iyzmxv3bq2r1t69nghizy4sfd2bupk8biybkurjcehwrp7xckka94vrqa6b5waivuywn4ibx3jnezut72s8n0vr1ejlk9uu11p5m2jp4p8rspsw25aj1jqeokewzvgv165dh6xtzjf4n9bcqhamk5chvtv5gla7cd9ddajcihaw1jlwunbp6f8elu26zdvr92dr11cz0otikunwb69m5azc2u8wf4la6h3jqtclvyc15r6rmy1lruwp7hgjloq1uuud439hrpdnrewjbecfj22m64ewcivzy0rnefeml04v2mfxjj7kx1ks7kf659dvpw73a33dbu1an668eaq6r57ezlybb7z7q610bav2f1yehvws21sa4lb2o1r6s0bb79x49wtonb1igyocmpckaw4d5usc7jk4tv2b9l4m32np4gjm1fsmtkw0df8im2opbdt1id6aod7x8q33iccybz7lrzbhbj4bo33uscutni49zmfwben3wuzz87ca8s3cvaffq1xw02wl500l4y7viw8ikwcw4b2q5ld275qb1f6izzbym47tjbx2c8m7i487qoo1ieu643vesw5rj23ebucxkxnfergy89z4qjhyhzwc381yyqrhbcspzq7tspzrfwttndda788hylzm1q69b815iuznjbv0e8c83qifoq1papj2g1o1p7g4lguututdfdxmf8nr08hl0puto1yq23u32ye4atn9ggxq9wg7sx5ad1hhr4cbfq9szfg55dx4v559qxvgv8cjm8wwlion8jfus98tqna45kp9l03liub294g0p594a2c4a2k71qwom7oej8wcpb8aoi3su40rb0aw24uk0rrxlz5roup3oepp6han5kd6bquemm4o0t0eh4sms6szhlr8x5u0jvz95ncm2paejqg1ahrfwc5l5ojj8iiz7p-w1-s3-v30:1.



La première loi empirique formulée par Gordon E. Moore (en 1965 dans le magazine Electronics[58]) est une courbe théorique prévoyant la capacité de réplication des machines par elles-mêmes au regard de la corrélation entre miniaturisation et puissance des processeurs informatiques. Elle prend en compte le fait que cette puissance, ou capacité de calcul, ne va pas aller en diminuant. Cet idéal permet d'envisager techniquement la gestion d'une bibliothèque de Babel, exponentielle elle aussi. Un comportement expansionniste qui permet de tout sauvegarder et, à terme, d'effectuer un traitement en « temps réel », une surveillance, un contrôle par feed-back, une jonction entre le moment d'observation d'un objet ou d'un individu et son jugement (sans intermédiaire politique). Une déséparation de la justice et des États qui pose problème dans une surveillance automatisée. Ce projet de tout expliciter et de tout savoir est celui de la surveillance qui veut tout modérer.

> « Ensuite, un dispositif évolue, […] [il] produit perpétuellement ce que Foucault appelle un "remplissage stratégique, une adaptation continue du dispositif aux nouvelles données stratégiques" qui forment son milieu. [...] Ce processus de surdétermination fonctionnelle correspond à ce que la cybernétique appelle "boucle de rétroaction" ou feed-back qui contrôle en temps réel l'état d'un système automatisé quel qu'il soit. Un dispositif évolue donc d'une manière interne modifiant en temps réel ses éléments et leur agencement en fonction, à la fois des conditions du milieu (conditions stratégiques) et de ses propres productions […] »
> **Olivier Razac,** ***Avec Foucault, après Foucault : Disséquer la société de contrôle***[59]

URL : https://blog.torproject.org/blog/cooking-onions-names-your-onions.

58. Wikipédia, Loi de Moore, https://fr.wikipedia.org/wiki/Loi_de_Moore.
◊ Gordon E. Moore, « Cramming More Components Onto Integrated Circuits », Electronics, vol. 38, 1965. URL : http://www.cs.utexas.edu/~pingali/CS395T/2013fa/papers/moorespaper.pdf.

59. Édition L'Harmattan, 2008, p. 24.

Obfuscation : brouiller les données

J'ai réalisé une vidéo de 10 minutes au sujet de Vuvuzela, une messagerie d'échanges cryptés en réseau, qui se base sur ce principe d'*obfuscation*. Le vuvuzela est cet instrument popularisé durant la Coupe du monde de football en 2010 en Afrique du Sud. Il a très fortement perturbé l'information des matchs par les commentateurs gênés, comme le public, par le son intrusif qu'il produit. La fréquence de cet instrument assez monocorde a donc inspiré les créateurs du logiciel. Ma vidéo vidéo intitulée *Vuvuscation*[60] (2016) mêle ainsi l'univers du foot, des jeux vidéos sur le foot, des activités de cryptage, de fabrication de fausses cartes d'identité vendues sur le darknet, mais il y est aussi question de tactiques d'homonymie au sujet de Spartacus (qui raconte la solidarité d'esclaves envers leur meneur qui trouble l'autorité en s'affirmant qu'ils sont cet individu alors recherché) ou encore de confusion identitaire dans la figure de Nancy Carter (un personnage de fiction dans le premier épisode de la série originale *Star Trek* paru en 1966 où un extraterrestre infiltre l'équipage du vaisseau en prenant la forme – le morphisme – tour à tour de chacun de ses membres).

Vuvuscation est réalisée à partir de vidéos trouvées sur ces sujets, cherche à questionner sur ces pratiques de brouillage, et sur les outils qui les rendent possibles. J'ai voulu réaliser un travail plastique qui mêle différentes sources d'inspiration, une narration qui, dans sa narration même, brouille l'interprétation sans pour autant être chaotique. Le vuvuzela me semblait bien trouvé comme nom d'application, très signifiant dans ce qu'il permet de brouillage informationnel en rendant le signal inaudible pour qui ne l'a pas formulé, pour qui il n'est pas adressé.

Images tirées de la vidéo *Vuvuscation*. [À gauche] Nancy Carter dans l'épisode de *Star Trek*, perdant son apparence humaine. [À droite] promotion de fausses cartes d'identité, comparaison de l'original avec la copie.

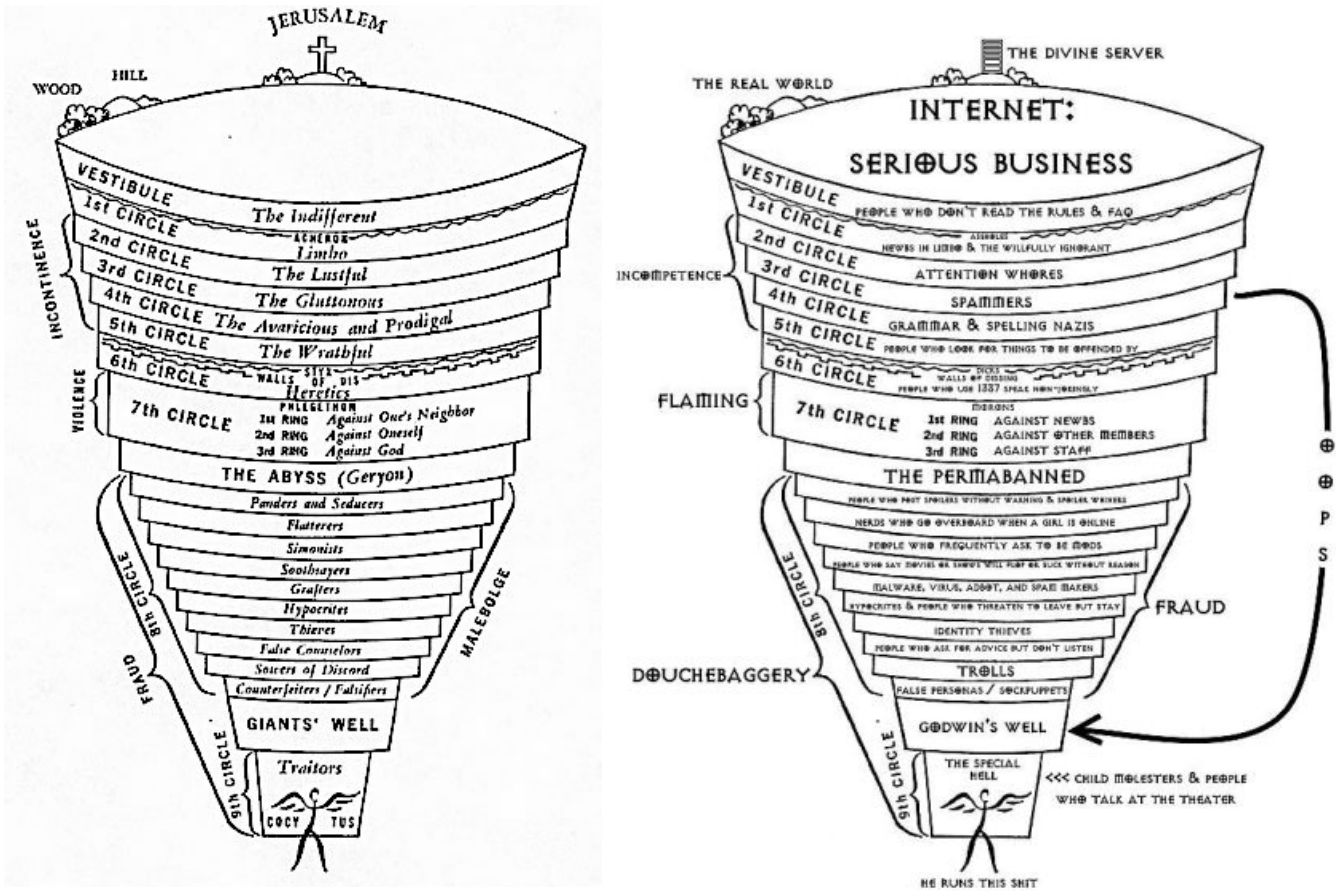
60. Disponible via cet URL : http://vincent-bonnefille.fr/#vuvuzella.

Cette complexité obscurcissante (obfuscation) est le principe de brouillage qui consiste à polluer l'information « vraie » avec l'ajout d'informations non pertinentes qui empêche l'enquête conclusive. Le cryptage (bien plus opacifiant) est utilisé sur Tor par exemple en ajoutant des couches à l'oignon : de fausses identités successives qui cachent l'identité réelle d'une connexion, le cœur de l'oignon. Cette obfuscation empêche un droit de regard critique. Ces stratégies de contre-espionnage, de contre-surveillance permettent à des marchés illicites d'opérer sur des réseaux tels les darknets. Ils vont à contre-courant des technologies normées utilisées sur Internet. L'incertitude qu'ils produisent fait fantasmer un ailleurs culturel qu'il faudrait découvrir. Le brouillage entre le vrai et le faux est ainsi propice à la fiction qui révèle une certaine appréhension collective.

II. Darknets et technologies d'avant-garde

Imaginaire de la contagion informatique

L'imaginaire du darknet est parfois représenté en niveaux par lesquels plus l'usager cherche et va en profondeur, plus il découvre, plus il accède à de l'extraordinaire, à de l'illicite. *La Carte de l'enfer*, telle que représentée dans la première partie de la *Divine Comédie*, écrite par Sandro Botticelli (en 1302), est souvent utilisée pour illustrer le darknet : un lieu souterrain dont l'accès demande de passer plusieurs « strates » et dont la profondeur sépare les différents supplices infligés aux menteurs, aux traîtres, aux fraudeurs, aux intellectuels, aux faux prophètes, etc. Un enfer où les damnés sont répartis selon leurs péchés, leurs vices, par niveaux. Dans les représentations des darknets en iceberg, l'accès à un autre niveau demande d'acquérir des compétences techniques dont certaines n'existent pas. Elles ont à mon sens un rôle fiction dans un milieu propice au secret et à l'anonymat, au colportage imprécis.



[À gauche] Représentation schématique des trois royaumes éternels composés des neuf cercles de la Carte de l'enfer .
Quatre grandes parties sont apparentes : incompétence, violence, fraude ordinaire, fraude par traîtrise.
[À droite] Même inspiré par L'Enfer de Dante, appliqué aux pratiques sur Internet où l'on trouve : *trolls*[g] (personnes créant du chaos dans une discussion, souvent par controverse volontaire, sape de l'autorité du discours), nazis, *spammeurs*/bots/*malwares* (outils dangereux), *newbies* (nouveaux venus, néophytes, non-administrateurs), etc. La fraude et le vol d'identité sont mentionnés. Ce document est parodique.

Un milieu de l'incertain qui protège ses sources, ce qui laisse présager une plus grande liberté d'expression de leur part. Un auteur y serait ainsi plus à même de révéler des réalités qu'il ne peut partager ailleurs, publiquement, sans se confronter à la bien-pensance – la civilité mise en place sur *clear web* – qui soumet la pensée au jugement, à la critique : un contrôle social qui peut salir une notoriété sur le long terme. En cela, les pseudo-sciences et *creepypastas*, dont l'argumentaire est souvent imprécis, inductif ou intuitif, sont tout à fait bien reçus sur les darknets. Ces légendes vernaculaires sur Internet sont tout autant efficaces sur les darknets que, d'une certaine façon, on va ailleurs en allant « dans » le darknet. Se connecter à un réseau qui sort de l'ordinaire, c'est un peu comme aller au cinéma. Il y a des protocoles, des mises en condition pour signifier aux spectateurs qu'ils entrent dans un autre monde, hétérogène à la société, afin qu'ils soient tolérants à la fiction[61].

Ces niveaux font fantasmer un au-delà par une mythologie technologique, dont l'aboutissement du récit initiatique nécessite une avancée technologique – ainsi l'ordinateur quantique permettant l'intrication de qubits[g] au dernier niveau, ou le « *Marina's web* » – comme graal. Même si ce ne sont que des histoires ou des arnaques, elles favorisent la nécessité de la technologie.

Plusieurs ordinateurs quantiques existent.
La capacité d'intrication des bits (qubits)
permet à leurs processeurs une puissance de calcul extraordinaire.
La firme Google acquiert le *D-Wave 2X*, l'un des ordinateurs les plus puissants
au monde, « doté d'une puce de 1 097 qubits »[62]

À l'imaginaire s'ajoute sur les darknets une réelle avant-garde technologique en élaboration sur les darknets tels les *blockchains*[g], toutefois liée à l'imaginaire vu que son inventeur reste inconnu en dehors de son nom Satoshi Nakamoto. Plus simplement, l'originalité des dispositifs techniques qui sont mis en place sur les darknets, contre une norme technique qui permet une traçabilité (par l'adresse IP entre autres), laisse à penser que d'autres outils sont en élaboration.

---

61. Nous pensons ici à ce que décrit Roland Barthes dans son article « En sortant du cinéma », paru dans la revue Communications en 1975 (vol. 23, *Psychanalyse et cinéma*, n° 1) pp. 104-107.

62. Leila Marchand, « Google présente son ordinateur quantique, 100 millions de fois plus rapide qu'un ordinateur classique », *Les Échos*, 2015. URL : https://www.lesechos.fr/10/12/2015/lesechos.fr/021548110969_google-presente-son-ordinateur-quantique--100-millions-de-fois-plus-rapide-qu-un-ordinateur-classique.htm.

Des moyens de parfaire enfin le projet de connaissance de toute chose grâce à un Internet perçu comme centralisant tous les savoirs d'une humanité connectée. Des moyens d'accéder au-dedans des choses, d'en extraire une vérité plus profonde, de croire en un au-delà dans un monde cartésien, rationaliste.

L'idéal d'un *clear web* est celui de la bienséance, d'un espace civilisé, dont l'administration et la modération aboutissent, certes, à une censure et parfois à la suppression de contenus, mais qui produisent aussi une pression extérieure, insidieuse, qui sous-entend une certaine limite de la liberté d'expression chez les usagers. Il serait faux de penser que les sites sur le darknet en sont exempts. Un administrateur d'un équivalent du réseau social Facebook hébergé via Tor (http://atlayofke5rqhsma.onion) m'a confié que, bien qu'attaché à une réelle liberté d'expression et poussé à inventer d'autres espaces de liberté pour se protéger de la censure dans son pays, il se posait des questions éthiques en voyant les contenus haineux, anxiogènes, néo-nazis, pédophiles, pro-anorexie, postés sur sa plateforme. Il convenait alors, dans une idée chère aux partisans de la liberté d'expression, qu'il n'interviendrait pas, qu'une demi-mesure l'obligeait justement à prendre parti, à modérer une multiplicité de propos, de contenus, dont il ne se sentait pas responsable, tout en jugeant que sa plateforme offrait des moyens pour choisir ses interlocuteurs, ses fils d'actualités.

> « En Grèce antique et à Rome, les amalgames entre humains et animaux accouchent le plus souvent de monstres malfaisants. L'effroi qu'ils véhiculent se retrouve dans la graphie du mot, qui vient du latin *ibrida*, vite altéré en *hybridia* [… Il s']accomplit ici un "forçage étymologique" qui a pour fonction d'évoquer l'hybris (υβρις) grecque, c'est-à-dire la démesure, la transgression, le franchissement des limites pouvant emmener dans leur sillage un déferlement de violence. »
> **Jean-Christophe Graz, « Gare aux hybrides : mythes et réalités de la gouvernance de la mondialisation »[63].**

Les mentalités autour de la question de la modération sur les forums du darknet y paraissent bien plus souples que sur le *clear web* du fait de la liberté qu'y trouvent les hébergeurs, mais cela ne signifie pas qu'il n'y a pas d'administration ni de modération sur ces sites. Ces derniers sont tenus par des individus soucieux d'offrir des espaces de qualité qui permettent de vivre en toute convivialité et en bonne intelligence. Les darknets offrent un espace hors du regard social extérieur, normé, ce qui ne veut pas dire pour autant que la vie sociale y est nécessairement différente. Cette image de trouble et de débordement humain, de démesure (*hybridia*), est véhiculée par des créations vidéoludiques.

63. Édition *Études internationales*, vol. 39, n° 3, 2008, p. 367

Red rooms : la culture de la peur

Les *red rooms*, ces endroits hors de la vision dont il faut pousser la porte pour découvrir ce qu'il s'y passe, ont leurs murs couleur rouge sang. Ces mythes urbains font partie des fantasmes récurrents au sujet des darknets, celui d'un réseau occulte accessible de l'intérieur du darknet. Tout comme les tueurs à gages, les *red rooms* n'ont pas été avérées comme réelles. Elles incarnent le pire du darknet, particulièrement bien caché en raison des activités qui s'y déroulent.

[Ci-dessus] Images extraites du film de science-fiction de David Cronenberg *Videodrome* (1983) qui raconte l'histoire de l'animateur d'une émission de télévision sulfureuse, défiant la morale. Passionné de culture underground malsaine, il cherche la perle rare, il est dans le dépassement des limites [représenté en archiviste, à gauche]. Il découvre et s'infiltre dans un réseau clandestin diffusant sur les ondes hertziennes des contenus illicites, dont des films de torture (*snuff movies*[g]). Il acquiert les outils pour pénétrer dans cette sphère privée, ce réseau. Il va, peu à peu, poursuivre son appétit malsain et son fantasme sur ce réseau jusqu'à littéralement entrer dans la télévision qui le happe [à droite, le médium y est personnifié, sexué]. Cette image raconte le fantasme de rentrer dans la matière, d'aller à l'intérieur du réseau, de dépasser le statut de spectateur, de franchir le seuil et d'ainsi vérifier la réalité derrière les images, le médium. Ce film de fiction raconte à mon sens ce que sont les darknets, mais aussi Internet à ses débuts : une inquiétante étrangeté (*Unheimliche* en allemand, concept Freudien ; décrit un en-dehors du familier « ça » maintenu secret[64]).

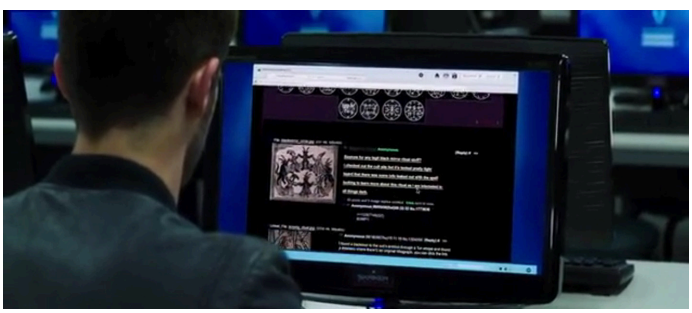
64. Wikipédia : « Unheimlich vient de Heim. Ce mot signifie "le foyer", la maison et introduit une notion de familiarité, mais il est aussi employé comme racine du mot Geheimnis, qu'on peut traduire par "secret", dans le sens de "ce qui est familier" ou "ce qui doit rester caché" », https://fr.wikipedia.org/wiki/L'inquiétante_étrangeté.

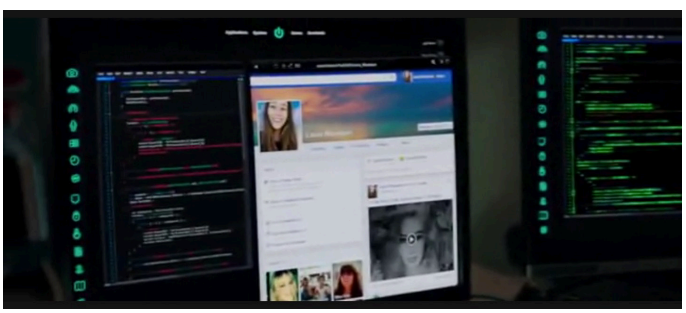
D'autres œuvres explorent cet imaginaire des red roms dont le téléfilm Darknet sorti en 2015 (réalisé par Jeff Woodward). Au début du film, le darknet est contextualisé auprès des protagonistes qui participent à un jeu de téléréalité :

> [Dans la forêt, chasseur musclé, très concerné demande par oreillette]
> « J'ai vu des caméras ça va être filmé ? »
>
> [QG – intérieur sombre, écrans, mainframe – du jeu de chasse humaine]
> « Oui, elles sont directement reliées à une régie. Le film une fois monté sera diffusé sur le *dark web*. »
>
> [Regards d'autres participants intrigués – extérieur, jour ensoleillé en sous-bois.
> Un participant pas sûr d'avoir bien entendu à son oreillette]
> « Allo, quoi ? Le *dark web* ? »
>
> [Depuis le QG, un opérateur rentre dans le cadre, prend le micro à la fois excité et agacé]
> « Le *dark web*, la partie visible de l'iceberg : 500 fois plus grande que la partie visible d'Internet, 500 fois plus intéressante aussi On trouve de quoi acheter des armes, des faux papiers et toutes sortes de drogues… Mais aussi, très intéressants sites pornos, pédophiles... […]
> Les *snuff movies* sont visionnés par des millions de personnes qui payent très cher pour les voir. »

La peur de l'outil

[Ci-dessous] Le film *Friend Request* (de Matthew Ballen, Philip Koch et Simon Verhoeven, 2016), un mélange entre occultisme, piratage et code infecté/hanté, miroirs noirs, etc. renoue surtout avec la peur du *stalking*[g] (attention trop soutenue, harcèlement) et des mauvaises rencontres en ligne. Il colporte une vision répandue d'épouvante et anxiogène d'Internet qui justifie la surveillance, mais surtout la modération et le civisme sur web. Dans ce film, l'élément/outil malfaisant est transporté sur le réseau, et c'est un *bug*[g] (une erreur système) qui le fait apparaître. Il est ici montré dans tout ce qu'il a de terrifiant par son omniprésence hors de l'écran, non visible mais agissant. Un film qui parle de la non-maîtrise des outils informatiques par leurs usagers qui, du fait de leur ignorance, peuvent avoir le sentiment d'être manipulés par eux. Ce film parle de leur emprise sur nos vies, à commencer par nos activités sociales montrées ici comme dangereuses car pouvant mener à une sur-attention.





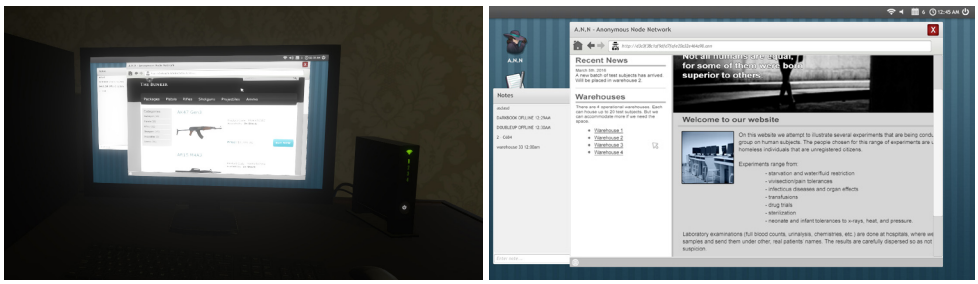
Cette œuvre ludique colporte à mon sens un discours de méfiance, une logorrhée qui justifie publiquement une surveillance et une modération du web pour éviter l'infocalypse[65]. Les protagonistes du film font quelques va-et-vient sur le darknet perçu et imagé comme le monde du *hacking*[g] et des Anonymous, un milieu hors du champ de la surveillance globalisée, un monde de dérégulation des outils et des comportements sociaux. Les darknets, par leur dispositif technique, offrent bien l'espace d'une liberté de la sphère publique. Ils offrent une alternative comme sphère publique régie par des lois ; ils sont rattachés à des pouvoirs permettant une cohésion sociale.

Ce qui est trouble dans les darknets, c'est leur perméabilité sociale, l'intrusion d'activités normalement exclues du champ politique, du débat. Le but est d'enrayer la banalisation de certaines pratiques, à commencer par leur politisation en interdisant leur existence, en empêchant leur apparition et le débat qui pourrait amener à redéfinir des limites, des seuils d'acceptabilité, autrement dit, ce qui est éthiquement possible dans une société. L'interdit crée ainsi un tabou ou une curiosité malsaine sur des activités illicites que l'on sait seulement exclues de la vision mais pas pour autant éradiquées. Les darknets donnent une place à cet imaginaire, sinon désincarné. Ce qui me semble ici en jeu, c'est la technique qui fait apparaître, qui met au monde, par discontinuité.

65. « Julian Assange affirme que les démocraties sont confrontées, en fait, aux "quatre cavaliers de l'Infocalypse" : le terrorisme, la pornographie enfantine, le blanchiment, d'argent et les guerres contre la drogue et le narcotrafic. Chacun de ces fléaux, qui doivent être évidemment combattus, sert aussi de prétexte au renforcement permanent des systèmes de surveillance globale des populations. »
Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn, Jérémie Zimmermann, *Menace sur nos libertés. Comment Internet nous espionne. Comment résister*, traduction française Abel Gerschenfeld et Anatole Muchnik, Paris, Robert Laffont, 2013 .
◊ Ludlow Peter, *Crypto Anarchy Cyberstates and Pirate Utopias,* MIT Press, 2001, p. 90 : « *The use of encryption by "evil" groups–such as child pornographers, terrorists, abortionists, and abortion protesters–is cited by those who wish to limit civilian access to crypto tools. We call these groups the "Four Horsemen of the Infocalypse," as they are so often cited as the reason that ordinary citizen units of the nation state should not have access to crypto*. »
◊ Ignacio Ramonet, *L'Empire de la surveillance* (suivi de deux entretiens avec Julian Assange et Noam Chomsky), Éditions Galilée, 2015, p. 13-14.

Welcome to the Game

Dans le jeu vidéo (sur le système d'exploitation Windows) *Welcome to the Game*, développé par Reflect Studios en 2016, le joueur doit trouver une série de codes sur des pages du darknet (Tor) qui sont fidèlement reproduites – je ne les ai pas pour autant toutes reconnues –; assez facile à trouver depuis les annuaires de sites qui accueillent la « visite » de nouveaux venus passant par exemple par *The Hidden Wiki*. Ce jeu mêle hacking figuré par des codes et puzzles à résoudre à l'écran, ce qui ralentit la mission du joueur.



[À gauche] Écran permettant de consulter des copies de sites réels issus du darknet (Tor) *via* un réseau fictif intitulé « *Anonymous Node Network* » (A.N.N.) : ici un marchand d'armes.
[À droite] Interface du système d'exploitation dans le jeu. Le navigateur (A.N.N.) affiche une page qui présente des expériences sur des humains (transfusions, assais de drogues, stérilisation, vivisections, etc.).

Il alterne entre des vues sur l'écran, sans hors-champ, et une vue extérieure donnant sur l'intérieur de la maison du protagoniste qu'il incarne. Ce *creepypasta*[g] prolonge la peur du darknet dont les dangers distanciés par le réseau surgiraient dans le « réel », en intégrant la figure d'un ennemi (qui met fin à la partie). Si le joueur reste trop longtemps sur le darknet, sur son ordinateur, un homme cagoulé apparaît hors de l'écran, dans le monde « réel ». Ce jeu oscille entre travail documenté, mise en condition du joueur dans un environnement informatique immersif et fiction. On y trouve également des références nombreuses à *Cicada 3301*, série d'énigmes complexes autour de la cryptographie, lancée en 2012 par une organisation secrète disant vouloir recruter des individus à l'intelligence hors norme. De nombreux jeux vidéos dont *Sad Satan* (source inconnue) prennent le darknet comme source d'inspiration. Le climat de suspicion qui entoure ces réseaux en fait le lieu idéal du colportage, de l'incertain et renoue avec un besoin de se faire peur, d'un no fun. Le propos des développeurs n'est pas celui d'une véracité à l'endroit des réseaux occultants, ce contexte narratif sert une intrigue.

La radicalité des outils

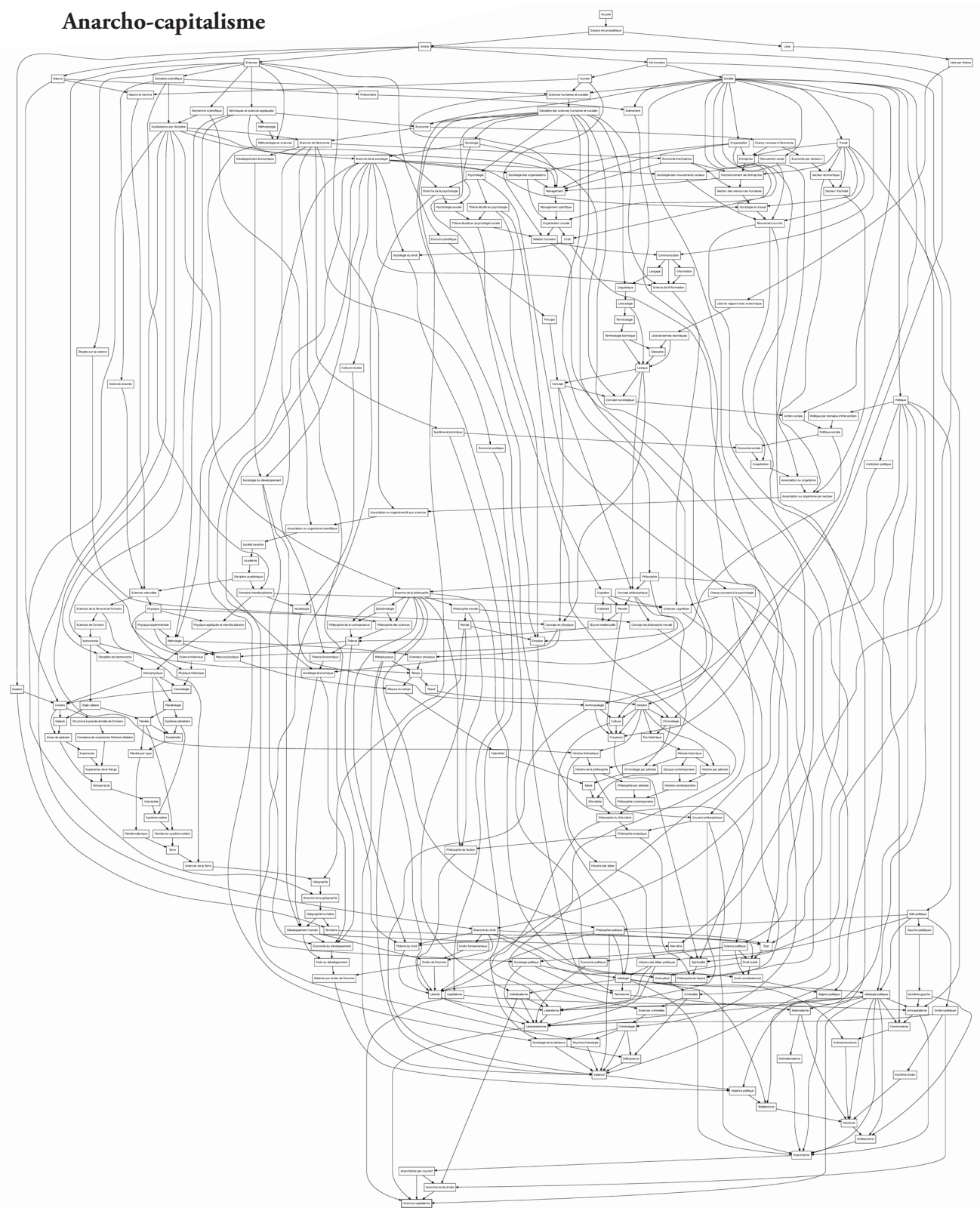
D'autres éléments du darknet ont « surgi » dans les actualités à leur sujet. Par exemple, les logiciels de rançon informatique WannaCry ou Peyta en cette année 2017. Basés sur des failles informatiques rendues populaires suite à la fuite des outils utilisés par la Nationale Security Agency[66], ces logiciels de rançon ont permis à des cybercriminels de crypter les données d'entreprises. Ils rendent les infrastructures informatiques de ces dernières inopérantes. Les hackers utilisent Tor pour garder leur connexion anonyme et réclamer une rançon en bitcoins[g]. Les mathématiques qu'ils utilisent (cryptage) posent problème pour faire enquête car ils empêchent une intrusion. Des messageries utilisant ces technologies sont souvent pointées du doigt comme aidant des organisations terroristes à communiquer sans être identifiées. Ces outils sont radicaux, ils offrent une vie privée numérique sans demi-mesure et permettent, en effet, de lutter contre toutes formes de d'intrusion informatique.

Pour ces raisons, on peut comprendre en quoi les darknets sont représentés dans les abysses d'Internet. Ils ne font pas qu'empêcher une indexation et l'accumulation de capitaux et de savoirs ; ils produisent une radicalité politique, une autonomie des outils institutionnels tels que ceux qu'applique la justice. Ils poursuivent un ensemble de rêves, d'utopies numériques et se présentent comme des alternatives plus ou moins abouties. Le cryptage est central dans les technologies qui composent les réseaux d'anonymisation des matricules numériques (darknets).

Ces technologies garantissent une vie privée numérique qui n'est pas seulement utilisée par les terroristes et les pédophiles, mais aussi par des dissidents politiques, des lanceurs d'alerte soucieux de faire un pas de côté, de sortir du champ politique et social. En cela, les darknets permettent une contre-culture et un contre-pouvoir médiatique. Tor, par exemple, est un outil de contre-espionnage mis en place par la Navy qui sert à l'échange de données sécurisées par les services de renseignement. Pour ce faire, ces services de renseignement ont dû en populariser l'utilisation afin de rendre plus difficile l'identification des connexions des agents. Une traçabilité de leurs activités est néanmoins rendue possible grâce à une surveillance ciblée sur le réseau.

66. Agence de renseignement américaine. Les outils qu'elle emploie ont été révélés par le site Wikileaks sous le nom de code Vault 7 cette année (2017). Ils lui donnent une capacité d'intrusion nécessaire à une surveillance de masse. Ces *leaks* ont révélé certains de leurs modes opératoires sur tous les environnements informatiques confondus. URL : https://wikileaks.org/vault7/ .

Anarcho-capitalisme



Représentation graphique des catégories (métas) d'articles sur Wikipédia, liées entre elles de la plus générale (parente) à la plus la précise (sous-catégorie). Ici, l'organisation des catégories autour d'« Anarcho-capitalisme » (catégorie). Le but est ici de montrer l'organisation des savoirs sur la plateforme encyclopédique afin de faire apparaître d'autres liens rhizomatiques au sein de ma recherche (méthodologie). [Carte générée en janvier 2017 (format 953 px × 1202 px, imprimé sur papier au format A0), depuis l'URL : https://tools.wmflabs.org/vcat/catgraphRedirect?wiki=wikipedia&lang=fr&cat=Anarcho-capitalisme&format=png&links=graph&sub=0].

Darknet originel

Pour comprendre comment la surveillance des connexions est possible et comment elle permet d'identifier les individus qui y sont associés suite à une enquête, il faut s'intéresser aux protocoles réseau mis en place durant la guerre froide. Cela nous permettra également de comprendre en quoi la question d'une extériorité aux réseaux caractérise originellement les « darknets ».

Dans les années 1960, le projet Advanced Research Projects Agency (Arpa) est mis en place. MilNet est le réseau militaire américain ; MiNet, le réseau européen. Arpanetg sera ensuite rebaptisé en ArpaNet. En 1986, la Nasa constitue le *National Science Foundation Network* (NSFNet composé de plusieurs sous-réseaux[67]) qui agrège une quantité de réseaux régionaux et internationaux tout en cherchant à augmenter ses capacités en termes de ressources. La tentative de cartographier Internet – constitué d'ordinateurs dont la connexion est identifiée par leurs adresses IP[68] attribuées – si elle était possible à ces débuts avec une faible population (du temps d'Arpanet), ne tient plus. La définition d'une altérité non répondante (à une tentative de communication extérieure formulée par l'envoi d'une requête, un *ping*[g], attendant une réponse, un feed-back en écho [69]) ne suffit plus aujourd'hui pour identifier un réseau comme étant un « darknet ». Un darknet désignait à cette époque (dans les années 1960), des réseaux hors de portée, hétérogènes au réseau de réseaux alors en édification.

67. Tels que SIPRNet à partir duquel Chelsea Manning, en 2010, a récupéré des informations confidentielles « à la source », à la main. Si nous mentionnons ici cette intrusion informatique c'est qu'elle raconte la persistance de certains réseaux encore actifs aujourd'hui. Nous voulions aussi rappeler que cette lanceuse d'alerte raconte comment elle prévoit d'utiliser un darknet aujourd'hui en activité utilisant le protocole Tor. « *The data caches that Manning replicated, allegedly, included* […] *from the war in Afghanistan [and] Iraq War* […] *from the US State Department, which also shared its data with troops via SIPRNet.* […] *Manning proceeded to siphon out the military's secrets, through Tor's tangle of obfuscating* […] *and out to the WikiLeaks server at a data center in Stockholm, Sweden.* » Tiré du livre d'Andy Greenberg, *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*, éd. Plume, 2013. ◊ Laura Taylor, *FISMA Compliance Methodologies*, p. 20 (chapitre 3), *SearchSecurity* et *Syngress*. 2013. URL : http://cdn.ttgtmedia.com/rms/security/FISMA-Compliance-Handbook-Ch3.pdf.

68. Jacques Vallée explique le choix de ce Transmission Control Protocol dans son ouvrage *Au cœur d'Internet : un pionnier français du réseau examine son histoire et s'interroge sur l'avenir*, éd. Balland, 2004, p. 171. Il exprime son point de vue sur le choix politique d'un tel standard (aujourd'hui encore utilisé) pour transporter l'information.

69. Malgré une enquête auprès des auteurs de cette affirmation, je n'ai pas trouvé de source historique. Beaucoup d'rticles faisant mention de ce fait historique prènnene pour source un site aujourd'hui innaccessible dont l'auteur reste anonyme (bien que joignable).

Il s'agissait alors d'un rapport communicationnel interrompu entre ordinateurs identifiés (par leur adresse IP), privant d'un accès les membres lui étant extérieurs : des réseaux privés, hors de, extérieurs. Un réseau privé ou extra-Internet est aujourd'hui une forme particulière, extrême de darknet. La globalisation des dispositifs de captation numérique produit aujourd'hui une perte d'extrémité, de limite, qui pose comme difficile l'imagination d'un en-dehors permettant de lutter contre une surveillance automatisée opérant sur tous réseaux confondus.

Les darknets et le *deep web* ont en commun cette distance avec une altérité, cette mise en retrait d'un accès extérieur, intrusif. Des contenus du web sont rendus inaccessibles plus ou moins volontairement et composent le *deep web*. Il existe des en-dehors du regard sur le web, des zones protégées, non indexées, d'autres désindexées, détruites, encore inconnues, d'autres enfin sur d'autres types de registres (DNS), ainsi que des en-dehors qui produisent des espaces sécurisés, propriétaires : clôturés, seulement accessibles à certains qui sont accrédités.

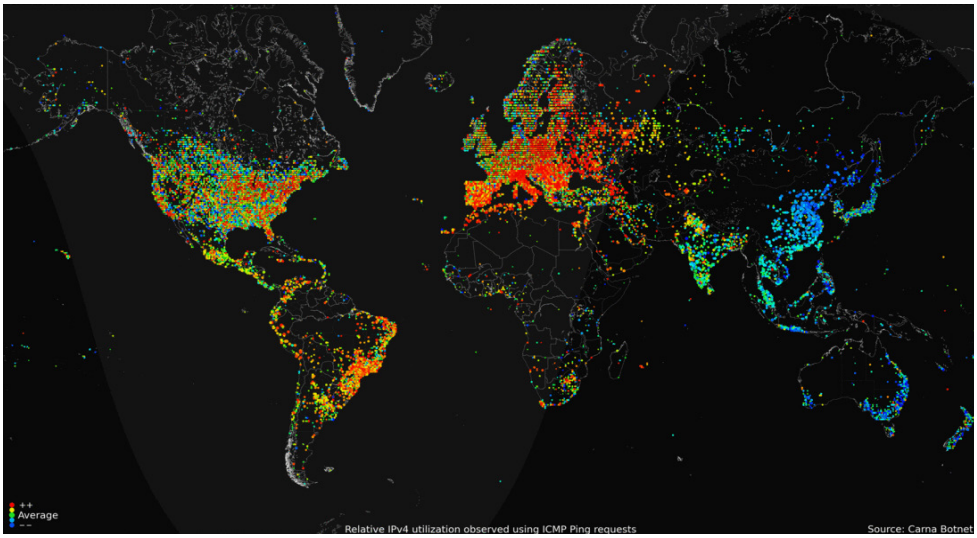
Adressage Internet Protocol

Le choix de ce standard informatique, après l'expansion progressive d'Internet qu'on lui connaît, est aujourd'hui toujours en place. Il autorise toujours l'identification d'un ordinateur. Cette adresse IP unique permet d'enquêter sur une activité en réseau (échange de données, sites consultés, location géographique de la connexion, etc.) afin de trouver à qui elle « appartient ». Elle est en effet attribuée par un fournisseur d'accès à Internet (FAI) qui peut révéler le nom du propriétaire de cette connexion active à un moment donné, et informer cette adresse par corrélation avec son identité civile. L'adresse IP n'est pas le seul élément technique qui permette d'enquêter sur une activité en ligne[70]. Élément unique, elle a un rôle d'identification de tout ordinateur connecté, qu'il s'agisse du « client » (usager) qui se connecte à un site, ou du « serveur » qui héberge des contenus. Ainsi, une enquête peut également être menée contre un site web et son propriétaire responsable de ce qu'il héberge[71].

70. Par exemple, la corrélation entre une heure d'activité et un débit d'information transmission peut servir à identifier un ordinateur ciblé.

71. Pour cette raison, l'indexation des sites au sein d'un registre DNS et la corrélation d'une adresse Internet (nom de domaine) liée à un hébergeur (serveur) ne rendent pas anonyme le propriétaire d'un site, à l'inverse des sites « cachés » sur les darknets qui n'inscrivent pas d'identité propriétaire à leurs hébergeurs.

Il est bon de se demander quelles sont les alternatives techniques qui sont possibles en termes d'indexation des contenus sur le réseau et des membres qui s'y connectent, qui y échangent dans une société où l'information est devenue un capital. Cette expansion du réseau et l'avènement de l'*Internet of Things* (IoT[g], « Internet des objets ») porté par des technologies telles que la *blockchain* dont les darknets sont l'un des laboratoires. L'expansion du réseau Internet aujourd'hui peut être imaginée par le nombre d'adresses IP distribuées par les institutions compétentes à travers le monde, entre les ordinateurs à travers le monde soit un total de 340 undecillions[72].



Carte mondiale des IPv4 en 2012 sur des ordinateurs non sécurisés (webcams, imprimantes, serveurs, etc.) par le *botnet* « *Carna* » (ces bots forment un réseau entre eux et récoltent des données, ici, 9TB)[73].

> « Longtemps, l'internet n'a relié qu'un tout petit nombre de chercheurs et d'étudiants et s'est développé dans l'obscurité. [...] Aujourd'hui, le réseau semble avoir atteint sa masse critique : de confidentiel, il est près de basculer vers la grande consommation, de passer du statut de curiosité à celui d'objet courant et de perdre au passage son caractère *unheimlich*, son inquiétante étrangeté. »[74]

72. Federal Comunications Commission, « *Internet Protocol Version 6: IPv6 for Consumers* », 2017. URL : https://www.fcc.gov/consumers/guides/internet-protocol-version-6-ipv6-consumers.
◊ Undecillion : « Fait partie des grands nombres, 1 undecillion = 10^36» selon Cookie Fonster, *Pointless Gigantic List of Numbers - Part 2 (1,000,000 ~ 10^10^1,000,000).*
URL : https://sites.google.com/site/pointlesslargenumberstuff/home/l/pgln2.

73. Le botnet *Carna* a réalisé « un scan de ports sur d'appareils non sécurisés » (traduction de l'anglais), sur 460 millions d'adresses IPv4. Cet audit sauvage a permis plusieurs états des lieux du réseau global, ici une carte à un temps T (jour/nuit). Sources : ◊ « *Census 2012: Port scanning /0 using insecure embedded devices* ». URL : http://census2012.sourceforge.net/paper.html. ◊ Dan Goodin, « *Guerilla researcher created epic botnet to scan billions of IP addresses* », 2013. URL : https://arstechnica.com/information-technology/2013/03/guerilla-researcher-created-epic-botnet-to-scan-billions-of-ip-addresses/.

74. Viviane Serfaty, « L'internet : fragments d'un discours utopique », Communication et Langages n°119, 1999. p. 106.

La technique, abstraite, rend difficile l'imaginaire. Il est fort compréhensible que ce qu'elle engage par ses spécificités soit difficilement saisissable. Aussi, réaliser des supports visuels qui les contextualisent, ici sous la forme d'une carte mondiale, ou par une mise en forme artistique, une installation par exemple, permet d'en comprendre l'impact en objectivant par un langage commun. Pour autant, une installation sur le thème des réseaux, plus largement assistée par ordinateurs, nécessite un savoir technique pour sa mise en place. L'image qui en résulte traduit bien une série de réponses informatiques, de langages et de protocoles.

Or, pour comprendre ce qu'est la surveillance en place aujourd'hui sur les réseaux numériques tel Internet, il faut trouver des formes valorisantes qui, à mon sens, ne devraient pas occulter totalement leur fonctionnement interne ; mieux encore, dans un esprit de partage et d'indépendance, il est nécessaire que ces œuvres donnent les moyens de les reproduire, de les modifier . Pour autant, tout expliciter de la part d'un artiste, tout montrer, peut desservir son propos, amoindrir l'appréciation du spectateur, mais cela permet en même temps d'en démystifier la pratique. Cette question est centrale pour comprendre comment la vulgarisation d'un sujet technique – ici, les darknets – à force d'a priori l'a rendu confus.

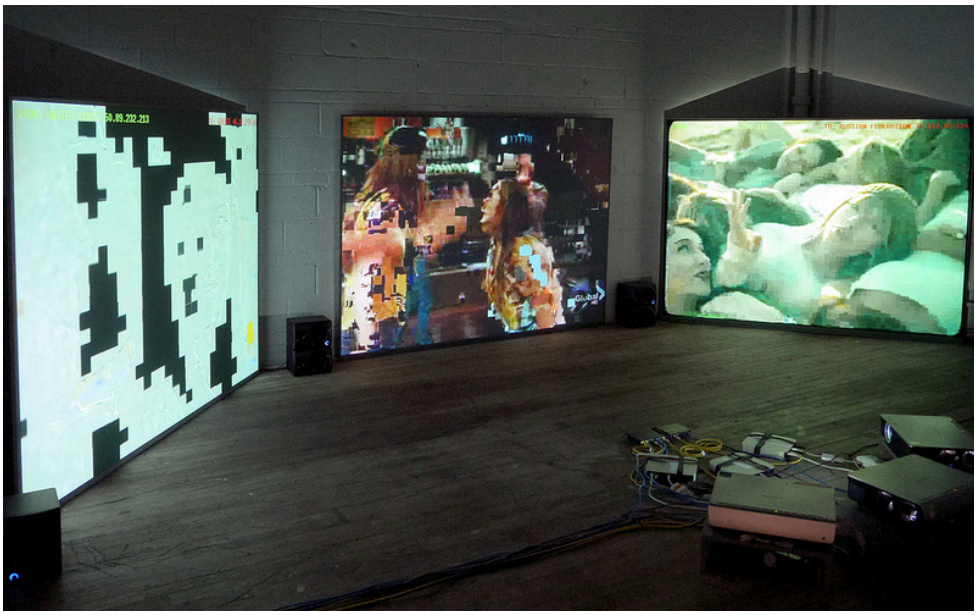
The Pirate Cinema : P2P et MSM

En 2014, je porte mon attention sur le travail de Nicolas Maigret[75], artiste et organisateur de Disnovation II, qui met en place *The Pirate Cinema*, une installation composée de multiples écrans pouvant évoquer une salle de contrôle par télésurveillance. Le sujet de cette proposition artistique m'a alors intéressé car elle rend visible une pratique en réseau invisible qui ne produit pas d'images (comme les pages web) mais dont la narration mise en place par l'artiste en génère. Cette production d'images montre une activité sur un réseau d'échange de fichiers utilisant le protocole P2P[g 76] – une topologie décentralisée entre utilisateurs rendant ces derniers « égaux ». Grâce à un logiciel d'interception,

75. Recherche accessible à cette adresse URL : http://vincent-bonnefille.fr/#nicolas-maigret .

76. Via le protocole BitTorrent pour un échange décentralisé à l'inverse d'un téléchargement « direct » entre un utilisateur et un serveur. Le P2P permet une égalité entre tous les ordinateurs qui composent ce réseau aussi bien serveurs que clients : capables d'envoyer et de recevoir des données de façon « horizontale ». Les dépendances vis-à-vis d'un serveur sont ainsi moindres et amènent à une meilleure résilience en cas de panne ou de suppression de ses contenus (pour cause de poursuites judiciaires par exemple).

l'installation permet de projeter sur les écrans un flux audio et vidéo composé de « films » (fichiers numériques) partagés à travers le monde entre différentes sources (ordinateurs). Leur état de transfert intermédiaire[77] produit un flux ininterrompu en causant leur désencapsulation[78] qui, normalement, les rendrait à l'écran contigus les uns aux autres (et non pas à l'état de flux entrelacé, confondant les fichiers entre eux).



Vue de l'installation. Maison des arts de Créteil, 2017[79].

77. L'échange de fichiers via *BitTorrent* s'effectue par blocs qui découpent le fichier, ce qui permet qu'une source qui le partage (en l'envoyant) n'ait pas nécessairement l'intégralité du fichier en sa possession pour le faire. Ainsi, le téléchargement en cours d'un fichier à l'état partiel crée des problèmes de lecture.

78. Encapsuler signifie entourer d'une capsule. Dans le cas d'un fichier vidéo, il s'agit de contenir ce qui la constitue dont une trame vidéo ici, la première déconstruite qui produit des artéfacts, des dégradations visuelles mêlant les pixels entre eux, les faisant « couler » (effet dit *datamoshing*, désignant le fait de tordre un contenu). L'artiste Paul Devautour s'exprime au sujet de cette notion qui fait partie de sa pratique en tant que professeur et artiste : « La notion d'encapsulation est empruntée au vocabulaire informatique. En art, un projet sera dit encapsulé s'il s'inscrit dans un langage ou dans un contexte qui n'est pas le sien propre, et s'il utilise d'autres protocoles que ceux reconnus comme légitimes dans le monde des expositions. »* Une pratique ou un objet encapsulé crée une césure avec le milieu qui l'entoure, une discontinuité qui nous semble importante pour comprendre ce que permettent des outils informatiques de mise en distance d'un tiers indésirable. Nous verrons également au sujet du darknet utilisant le protocole Tor (*The Onion Router*) comment la connexion y est encapsulée en plusieurs couches successives pour la dissimuler au « dedans » (formellement parlant) d'un oignon (de couches successives d'identités numériques fictives).
* Dans le cadre d'un cours à l'université Paris 8 (2016) sur les pédagogies expérimentales (Comment faire d'une classe une œuvre d'art ?) autour de la pratique d'enseignant de Paul Devautour : « Extrait de l'introduction à la journée d'étude du 28 mai 2008, "artistes-enseignants aujourd'hui / stratégies d'encapsulation", à l'Ecole nationale supérieure d'art de Bourges ».
URL : http://www.arpla.fr/mu/pedagogiesexperimentales/conferences/paul-devautour/ .

79. URL : http://www.maccreteil.com/fr/mac/work/251/The-Pirate-Cinema ; site officiel permettant de visionner (sans les conditions d'exposition) le flux projeté sur un des écrans (en *live*) : http://thepiratecinema.com/online/ .

Il expose à la fois la consommation d'une activité dite « pirate », stigmatisée comme illégale du fait d'un échange prétendument courant de contenus sans respect des droits d'auteur. Les films qui apparaissent à l'écran font partie des 100 films les plus populaires sur la plateforme *The Pirate Bay* qui les indexe sur le web sans pour autant proposer un service de téléchargement direct (entre un serveur et un client, comme c'est le plus souvent le cas). Le web fonctionne selon une gouvernementalité propre et est globalement centralisant là où le P2P permet une centralité plus grande, une plus grande résilience. Dans l'installation *The Pirate Cinema*, les adresses IP respectives de l'émetteur et du récepteur des fichiers en cours d'échange sont visibles, ainsi que leur origine géographique, leur pays d'origine (information contenue dans l'adresse IP). Nicolas Maigret rend ainsi narrativement compte d'une activité globalisée, mais aussi populaire, tout en donnant un aperçu de la culture majoritaire du moment. Il livre un élément technique sinon invisible, du moins difficile à se représenter (sinon schématiquement).

La muséographie de l'installation induit une corrélation entre ce matricule numérique défilant (en haut des écrans) et les flux échangés « en direct », esthétisés par l'apparition furtive des bouts de films entremêlés entre eux. De plus, le titre de l'œuvre, la connotation à laquelle il renvoie – celle de la piraterie d'une activité illicite, parallèle à l'ordre –, narre une surveillance. Ainsi, cette installation imagine une activité normalement non perceptible tout en explicitant le fonctionnement sommaire. Il rend aussi compte d'une activité culturelle – dans le sens qu'elle est riche d'une culture qui lui est propre – populaire, souvent diabolisée pour justifier le retrait de ses contenus du champ de vision des « internautes ». Ces filtres diminuent le réel et vont à contresens de ce que prétendent les moteurs de recherche dans le fait de donner accès à « tout », à tous les savoirs du monde connecté. S'intéresser aux darknets offre également une matière exclue du visible et, nous le verrons, à d'autres cultures rendues ainsi minoritaires sur un web de plus en plus modéré. Mais ce qui nous intéresse ici, pour le moment, c'est la position du spectateur placé entre deux ordinateurs comme homme du milieu[80], comme s'il était à la place du surveillant : « dans » le réseau. Si je suis moi-même spectateur « pirate » et au courant des poursuites automatisées que la surveillance permet, alors je ne peux que me demander comment elle opère en ce moment, à cet endroit.

80. Nous reviendrons plus après sur cette pratique (dite de l'« homme du milieu ») qui définit une sorte d'attaque informatique, réalisée par un agent visant à intercepter des données numériques de façon localisée sur un utilisateur ciblé (ou plusieurs, mais dans un champ géographique restreint).

Un article très cité au sujet des darknets[81] interroge son lecteur sur l'avenir des DRM[82] vis-à-vis des réseaux et dispositifs de brouillage d'une identité numérique permis par les darknets (selon la définition actuelle à sa parution). En effet, en dehors du piratage, la technologie est obsolescente, et les outils de surveillances dépendants d'une certaine standardisation des protocoles réseautiques qu'ils observent. L'adresse IP, dans cette installation, est nécessaire pour comprendre leur importance dans une enquête visant à arrêter un « pirate » et de la facilité ressentie d'un tel procédé au regard par exemple des dispositifs d'automatisation judiciaire tels que ceux régies par la Hadopi mise en place en France en 2009. Dans ce contexte, Nicolas Maigret décide d'utiliser un VPN[g] qui permet de changer d'adresse IP de son dispositif d'interception, et ainsi de protéger les hôtes qui l'exposent contre d'éventuelles poursuites.

Nicolas Maigret utilise un VPN car, bien qu'il soit artiste, il est responsable de son activité sur le sol français et des dispositifs de contrôle et d'application juridique qu'il porte socialement. En faisant cela, il contourne la censure qui pourrait limiter son activité. Or censure ne signifie pas interdit ; elle peut venir en amont et prendre diverses formes de pressions extérieures, plus ou moins directes. Ce que la surveillance permet, c'est d'exercer une pression morale et juridique, c'est de faire enquête, voire de prévenir un délit, mais c'est aussi, utilisée comme outil normatif, de faire pression. *The Pirate Cinema* fait apparaître un « *underground* » et découvre une technologie par sa simplicité politique.

En dehors du fantasme de ce qui n'est pas explicite au regard, d'une surveillance potentielle, l'installation de Nicolas Maigret met ici en avant une popularité d'Internet qui, bien que permettant une meilleure résilience à la censure (par le nombre de sources égales entre elles), ne protège pas les usagers de poursuites. La « nudité » du protocole de transfert qui laisse apparaître l'adresse IP rend possible une surveillance de masse (ciblée ou non) opérée à distance.

81. « Le terme [darknet] gagne l'acceptation publique à la suite de la publication de l'article écrit en 2002 par Peter Biddle, Paul England, Marcus Peinado et Bryan Willman, quatre employés de Microsoft : *The Darknet and the Future of Content Distribution* [1]. L'article indique que la présence de darknets était l'obstacle principal au développement des technologies DRM (gestion des droits numériques) [...]. [1] Wood, Jessica (2010). *The Darknet: A Digital Copyright Revolution*». Richmond Journal of Law and Technology". » Wikipédia, Darknet, page française. URL : https://fr.wikipedia.org/wiki/Darknet/ .

82. Licences permettant de limiter l'accès à des données grâce à une identification unique d'un client (ayant le droit de le posséder) permettant, entre autres, d'en limiter la durée de vie, de les rendre obsolescents.

Celle-ci est possible car le moyen de transport de l'information (BitTorrent[g]) utilise les mêmes protocoles qu'Internet. L'usage d'un VPN permet de tromper une surveillance en changeant d'adresse IP utilisée pour rentrer sur Internet (*proxy*). Il ne s'agit cependant pas d'un darknet bien qu'il offre pareillement un moyen de cacher son adresse IP. Une solution radicale paraît alors évidente pour échapper à la surveillance : se déconnecter d'Internet. L'occasion de le faire autrement, de créer d'autres réseaux, d'inventer des protocoles politiquement autonomes d'une gouvernance d'Internet.

Réseaux autonomes

Les réseaux Lan[g], localisés, que forment les PirateBox[g] sont semblables en définitive aux réseaux privés d'entreprises ou de banques : celui interne aux entreprises d'investissement bancaire, mais aussi les espaces qui font interface entre elles et leurs clients depuis le web (en général sécurisés contre un espionnage entre l'utilisateur et le serveur par de l'https[g] qui, à base de certificats, encrypte les données). Un darknet, hétérogène à Internet par ses protocoles ou topologiquement par son extériorité, qui échappe à une captation de données massive et automatisée.

L'essai « émotionnel », très subjectivant, d'Hakim Bey, *TAZ – Zone autonome temporaire*, travaille un imaginaire contestataire de mouvance libertaire, altermondialiste. Il est très inspirant dans la création de dispositifs autonomes et d'automédias ou de tactiques médiatiques[83]. L'auteur théorise autour d'un ensemble de dispositifs permettant des actions sporadiques sur terrain (dans l'espace public ou cyber) pour échapper au contrôle d'un pouvoir oppressant. En partant des utopies pirates, des communautés marginales mais organisées, il invente des stratégies d'occupation temporaire qui intègrent la nécessité de discontinuité dans une action qui se sait menacée. La recherche d'autonomie mais aussi de partage avec sa communauté localisée est, à mon sens, bien que dans une autre mesure, accomplie dans certaines formes d'automédias *open source* et de tacticals médias.

83. « En empruntant à Michel de Certeau le terme "tactique" pour l'opposer à celui de "stratégie" (renvoyé vers les médias contre-hégémoniques préoccupés d'exercer une influence réformatrice sur les médias traditionnels), [le] mouvement [des tacticals médias] développe une esthétique de la fuite, du contournement et du détour dont le texte d'Hackim Bey sur les zones d'autonomie temporaire (TAZ) est l'emblème. » Dominique Cardon et Fabien Granjon, *Médiactivistes*, éd. Les Presses de Sciences Po, 2010.

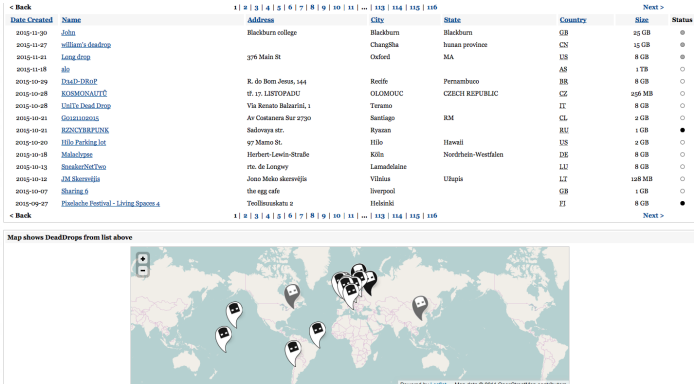
> « Si nous devions imaginer une carte de l'information – une projection cartographique de la totalité du Net –, nous devrions y inclure les marques du chaos, celles qui sont déjà visibles, par exemple, des opérations de calcul parallèle complexe, les télécommunications, les transferts "d'argent électronique", les virus, la guérilla du hacking, etc. »
> **Hakim Bey, *TAZ - Zone autonome temporaire***[84].

La mise en place de canaux de communication localisés, autonomes d'Internet, permet d'envisager un en-dehors du regard surveillant. Les PirateBox, microrouteurs portatifs mis en place et promus par David Darts en 2011, rendent possible la création des réseaux localisés en wifi qui échappent a priori à la surveillance. Ces réseaux à courte portée sont plus autonomes car ils ne dépendent pas d'Internet : ils centralisent tout le nécessaire pour échanger des informations entre ordinateurs. De plus, tout comme un serveur personnel sur Internet, il est possible d'y installer des logiciels, un chat, d'y stocker des fichiers sur une clé USB dont ils rendent le contenu accessible à proximité. Ils offrent donc un moyen peu coûteux pour créer des médias autonomes sans pour autant nécessiter de grandes connaissances en informatique. Ces microréseaux s'approchent, à mon sens, de la définition des darknets au début d'Internet : des réseaux privés, dans un en-dehors d'Internet aujourd'hui trouble tant il paraît ambiant. De plus, si effectivement ces réseaux permettent de se protéger d'une surveillance de masse, ils ne sont pas pour autant protégés contre des attaques ciblées localement. Il faut également penser des outils qui empêchent ce genre d'intrusion.

Réseaux informels

Yinan Song remporte en 2016 le concours CryptoDesign[85] avec son projet *Deeply* qui contient sur support amovible (carte-sd) le système d'exploitation Tails (optimisé contre la surveillance informatique). Ce concours met en avant la création d'objets innovants en matière de cryptage ou, plus largement, de sécurité et d'anonymat. Le designer[86] met en avant le caractère préventif de protection face au risque de surveillance en enveloppant le support dans un emballage de préservatif avec des instructions et préventions au dos concernant l'usage du système d'exploitation.

84. Hackim Bey, *TAZ - Zone autonome temporaire*, éd. L'Éclat, Paris, 1997, p.14.
85. Concours annuel organisé sur la question du design autour des activités relatives au cryptage, plus largement, aux pratiques permettant une sécurisation des échanges en réseau. URL : https://cryptodesign.org/.
86. Son site (http://yinansong.com) montre à mon sens cette orientation, même s'il crée de nombreux travaux sur la surveillance, la censure, etc.



[À gauche] *Deeply*, emballage de préservatif avec instructions. [À droite] Carte collaborative des *dead drops* à travers le monde. [Ci dessous] Aram Bartholl consulte le contenu d'une *dead drop* dans une rue de New York.

Ce projet utilise les moyens de transport de l'information numérique de la main à la main, comme les *dead drops*[g 87] : réseaux informels anonymes hors ligne inspirés de la technique d'espionnage du même nom. Ce sont des clés USB insérées dans les murs et localisées sur une carte – initiées en parallèle des PirateBox. Leur présence dans l'espace public laisse souvent craindre la présence de *malwares*/virus sans réelle raison, juste une crainte naturelle de l'« autre », de l'intrusion dans une zone non modérée.

C'est également le nom d'un logiciel de sécurisation des sources qui souhaitent divulguer des informations auprès d'un tiers[88]. Ce terme est employé sur le darknet pour parler d'une boîte aux lettres physique permettant de recevoir une commande potentiellement compromettante en cas de surveillance : une *dead drop* est un lieu de dépôt qui n'est pas directement rattaché au destinataire qui la relève, une discontinuité qui fait « tampon ». C'est une « boîte morte », sans prpriétaire connu, abandonnée.

87. Le site du projet : https://deaddrops.com/fr. Projet mis en place par Aram Bartholl en 2010 durant sa résidence à Eyebeam, Brooklyn. URL : http://archive.eyebeam.org/projects/dead-drops/.

88. Le logiciel SecureDrop, dévellopé par Aaron Swartz et Kevin Poulsen sous le nom *DeadDrop* [permet de sécuriser des données échangées sur Internet]. Source : Wikipédia, URL : https://en.wikipedia.org/wiki/SecureDrop. Wikipédia cite l'article de Kevin Poulsen, « Strongbox and Aaron Swartz », *New Yorker,* 2013. URL : https://www.newyorker.com/news/news-desk/strongbox-and-aaron-swartz.
De nombreuses organisations mettent en place cet outil *open source* – pour aider les lanceurs d'alertes et journalistes – dont le New Yorker à cette adresse (*via* Tor) : https://strngbxhwyuu37a3.onion.

Newstweek

Le *hacking*, au sens de « bidouille », permet une encapacitation technique en détournant des outils. L'ingénierie critique, défendue entre autres par The Critical Engineering Working Group dont font partie Julian Oliver, artiste, Gordan Savičić, artiste et designer, ainsi que Danja Vasiliev, développeur engagé, tous trois auteurs de *The Critical Engineering Manifesto*[89], prône une approche consciente et politique du développement de logiciels et d'outils permettant une liberté de leurs utilisateurs. En 2011, Julian Oliver et Danja Vasiliev mettent en place un dispositif portatif intitulé *Newstweek*[90] dont le code est accessible en ligne pour que chacun puisse le reproduire et participer à des performances guérillas d'usurpation numérique. Ce dispositif permet de localement offrir un *hotspot* wifi semblable à celui proposé dans les lieux publics. Une fois un usager connecté à proximité, les performeurs de cette action peuvent intercepter les transactions entre l'ordinateur du client (la personne qui s'est connectée sur le wifi mis en place) et le serveur web d'où il va récupérer des données pour afficher par exemple la page d'accueil du journal *NewsWeek*.

[Au dessus] Carte d'Europe du réseau de serveurs interceptant les données.
[À gauche] Déploiement des périphériques en Europe. [À droite] Interface côté client (contenu web modifié).

89. Lien vers le manifeste : https://criticalengineering.org/fr, 2011, à Berlin.
90. Détails techniques sur ce microserveur, le projet dans son ensemble : http://newstweek.com/overview/ .

Le propos n'est pas ici de voler des informations à l'usager malgré lui. En se plaçant entre le client et le serveur distant, les participants de cette guérilla peuvent modifier les informations affichées à l'écran du client consultant un site depuis son ordinateur. Il leur est ainsi possible, tout en usurpant l'identité graphique du site – ici, *NewsWeek* et sa notoriété –, d'en modifier le contenu. Le but de l'artiste est, selon la communication de son site dédié à ce projet, de tordre la réalité, de la rétablir au nom du pluralisme médiatique critiqué à l'endroit des *Mainstream Medias*[g 91].

Il montre surtout qu'un équipement adapté permet une surveillance à ciel ouvert. Plus encore, il rappelle l'importance d'une meilleure sécurisation des données sur Internet, au même titre que l'installation de Nicolas Maigret, en se plaçant au milieu d'un échange en réseau. Mais, en produisant une altération de contenu, il dévalue le caractère autoritaire de la source attaquée. Il met en place une arnaque très répandue sur les darknets actuels. Cette « désévaluation » de l'information brouille le vrai du faux (*obfuscation*). Elle crée du désordre dont l'invisibilité du dispositif lui permettant d'agir sans être pris. Cette absence d'interaction, cette intrusion à distance, profite à une surveillance qui cherche à capter des informations. En infiltrant les réseaux des usagers, l'artiste met en garde contre les dangers d'une intrusion informatique.

Can You Hear Me ?

Christoph Wachter et Mathias Jud réalisent en 2014 une installation intitulée « *Can You Hear Me?* » localisée sur le toit de l'ambassade suisse à Berlin[92]. Dans le cadre de leur résidence, ils installent un groupe de PirateBox avec des antennes artisanales réalisées avec des conserves qu'ils disposent à cet endroit stratégique. Ils sont, depuis ce point géographique, positionnés entre l'ambassade de Suisse (d'où ils sont originaires), le Parlement allemand et des antennes des services de renseignement américain et anglais (GCHQ) suspectés d'avoir massivement collecté des informations sur les citoyens via leurs portables, mais aussi sur des personnalités politiques travaillant à proximité.

---

91. Terme souvent souvent employé sur le darknet sous sa forme abrégée (MSM), traduit en français par « médias de masse » ou, plus littéralement, par « courant majoritaire médiatique » ; désigne des médias populaires jouissant d'une forte notoriété et visibilité qui leur permet de faire valeur d'autorité. Pour cette raison, la fraude, qui dévalue l'original en le polluant de fausses informations qui l'obscurcissent (*obfuscation*), le trouble, ce qui le rend moins fiable. Cela lui retire partiellement son autorité permise par sa notoriété.

92. Site officiel : http://www.wachter-jud.net/Can-you-hear-me.html et informations complémentaires à partir de la conférence disponible via cette URL : https://soundcloud.com/leslaboratoires-1/le-printemps-des-laboratoires dans le cadre des Printemps des Laboratoires #3 mis en ligne par Les Laboratoires d'Aubervilliers, 2015. URL : http://www.leslaboratoires.org/en/article/printemps-des-laboratoires-3-en-ligne-online.

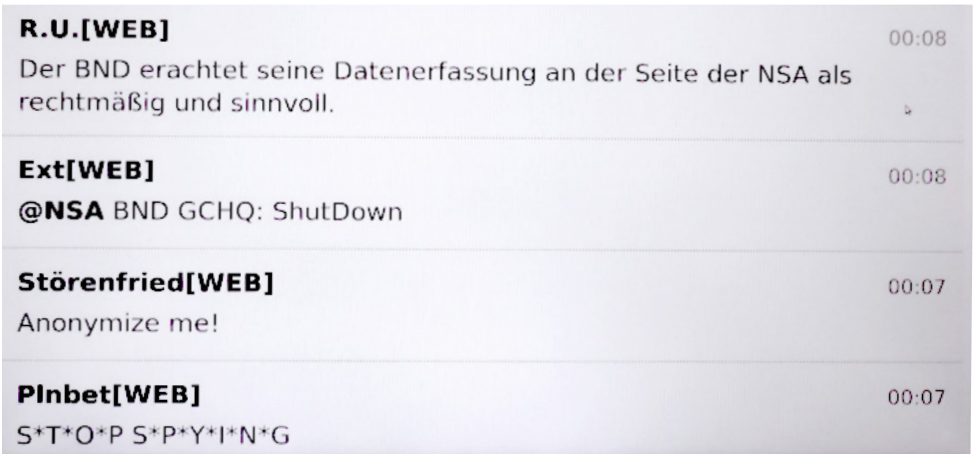
Vue depuis le toit où sont installés les différentes antennes et PirateBox.

Les artistes ont installé le système Occupy[93] sur leurs PirateBox (logiciels dont l'objectif est de rendre anonymes les ordinateurs connectés) dont le réseau est élargi par un réseau meshg (ou « maillé » en français) qui permet d'élargir l'étendue d'accès car chaque ordinateur (et portable donc) devient lui-même un relais. Ils ont utilisé des conserves pour augmenter la portée du signal wifi, ainsi que des matériaux rudimentaires qui esthétisent une pratique du *do-it-yourself* (« faire soi-même ») avec peu de moyens. Cette installation propose aux utilisateurs de dialoguer avec les surveillants prétendument en train de les surveiller localement afin d'opérer une sous-veillance – une surveillance des surveillants –, dans un geste de bas en haut – une autre signification de la sous-veillance désigne une autosurveillance normative. Ils peuvent en effet leur envoyer des messages par chat contre la surveillance, pour un respect de la vie privée, etc.

Indépendance

La vie privée sur Internet n'est pas qu'une question oppositionnelle qui, du fait d'une surveillance assujettissante et normative, devrait être combattue. Cette vision oppositionnelle essentialise la nécessité d'un respect de la vie privée face à un « grand méchant », à des *black boxes*, à des algorithmes et à des bases de données qui, sûrement par manque d'imaginaire contraint, produisent une tendance à l'exagération. Toute une mythologie autour de termes reflétant bien une dangerosité, mais qui, à mon sens, n'est pas primordiale pour penser une écologie des données et du repli informationnel, une décroissance des données et de notre dépendance vis-à-vis d'elles, et surtout de notre appétit existentiel à nourrir ces bases de données.

93. Mis en circulation par Occupy Wall Street en 2011, cet outil comme d'autres dispositifs d'automédias tels que FireChat (beaucoup moins libre) durant les contestations étudiantes à Hong Kong en 2014, permet de contourner une censure du réseau et d'échapper a priori à une surveillance de masse à distance.



Interface de discussion anonyme sur les PirateBox durant l'installation.

L'installation *Can You Hear Me?* me semble problématique car elle est dépendante de cette altérité et, même si le propos est ici de pointer du doigt un problème de façon ludique par l'interactivité logicielle (et aussi de faire de la pédagogie au sujet de ces pratiques), elle me semble répondre à une certaine vision de l'activisme. Inscrite dans l'espace public et en partie dans un cyberespace, cette installation renoue avec un idéal dialectique de la politique qui implique une relation dans le champ de l'ennemi dans l'espace public comme lieu fantasmé de la démocratie. Elle produit le sentiment d'une action constructive là où, justement, les surveillants ne dialoguent pas. Elle ne représente pas une stratégie radicale de repli comme peut le formuler une TAZ.

Au lieu d'une indépendance, elle crée un rapport d'individuation qui, à mon sens, positive d'une certaine façon la présence d'un regard extérieur. Ce qui me dérange, c'est l'essentialisation d'un ennemi en la figure d'un Big Brother [g]. Nous retrouvons ici, dans une proposition qui met en place un espace numérique poreux à sphère sociale, l'idéal de l'agora des contestations populaires, qu'elles aient eu lieu durant les printemps « arabes » (2010) ou ceux dits « d'érable » à Québec (2016[94]), durant les contestations étudiantes dites des

94. Réseau libre fait partie de ces réseaux. Installé à Montréal, il déploie un réseau d'antennes. À ce sujet, lire l'article de Félix Tréguer, Panayotis Antoniadis, Johan Söderberg, « *Alt. vs. Ctrl.: Thinking About Alternative Internets* » (notes éditoriales pour *The Journal of Peer Production n° 9, Alternative Internets*), 2016. URL : http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/editorial-notes/ . [Article annoté : http://mht.vincent-bonnefille.fr/Alt. vs. Ctrl._ Thinking About Alternative Internets – We The Net.mht].
◊ L'article en question de Christina Haralanova et Evan Light, « *Enmeshed lives? Examining the Potentials and the Limits in the Provision of Wireless Networks : The Case of Réseau Libre* », *The Journal of Peer Production n° 9, Alternative Internets*, 2016.
URL : http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/enmeshed-lives .
[Article annoté : http://mht.vincent-bonnefille.fr/Enmeshed lives « Examining the Potentials and the Limits in the Provision of Wireless Networks_ The Case of Réseau Libre . » The Journal of Peer Production.mht]. Ces articles questionnent sur la réelle autonomie et horizontalité du pouvoir dans ce type de réseaux.

« parapluies » à Hong Kong (2014), ou encore celles des mouvements Occupy à New York (2011). L'usage de technologies alternatives au réseau contrôlé d'Internet pour contourner la censure, entre autres sur les infrastructures, mais aussi sur l'accès aux registres d'indexation des sites DNS [g] qui relient une adresse IP d'un serveur à une adresse URL d'un site web. Utiliser des canaux de communication hors du réseau de réseaux constitue une alternative temporaire, mais aussi une résilience face au choc.

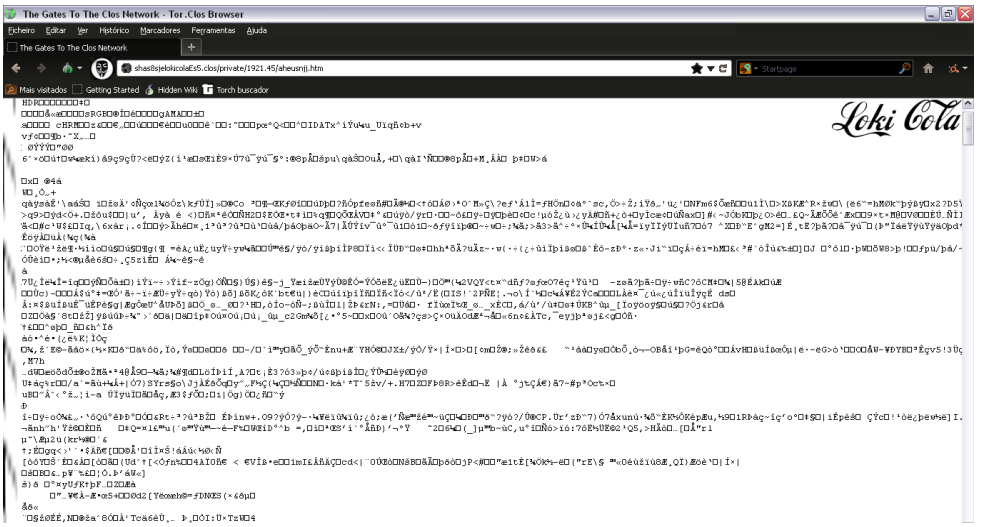
[À gauche] Graffiti sur une affiche de soutien au parti turc soutenu par Recep Tayyip Erdogan, à Istanbul. Le service DNS 8.8.8.8 (Google) permet de contourner la censure appliquée par les FAI [g].
[À droite] Promotion des Anonymous pour leur usage d'OpenNic par les Anonymous (via YouTube) contre la censure.

> « Tout est très ad hocg. Durant l'Égypte, il y avait 500 personnes sur l'IRC de Telecomix. […] C'est fluide. L'idée d'une do-ocratie, ça vient du Burning Man et ça fonctionne à rebours de la bureaucratie. On ne reçoit pas d'ordre, les décisions se prennent en faisant les choses. […] Le 28 janvier 2011, les principaux fournisseurs d'accès s'aplatissaient devant les injonctions du gouvernement égyptien et suspendaient leurs services, causant une chute de plus de 90% du trafic dans le pays […]. Internet était une zone autonome, où les gens pouvaient se fixer leurs propres normes, et maintenant, d'autres veulent revenir en arrière, récupérer le réseau. »
> **Quentin Noirfaliss, « *Telecomix : "Hacker pour la liberté"* »[95].**

La référence dans cette citation à une autonomie d'Internet non gouverné, à l'image des TAZ, est essentielle pour comprendre la hiérarchie informelle qui caractérise Telecomix. Le collectif est un soutien ponctuel dans ses interventions, il utilise des outils adaptés aux situations, c'est-à-dire *ad hoc* [g]. L'action de terrain du collectif ne s'est bien entendu pas résumée à l'usage d'un DNS alternatif, mais de tels usages technologiques ont effectivement permis de contourner la censure imposée. Elle a pallié un manque d'autonomie structurelle. Ils permettent également d'accéder à d'autres sites normalement non indexés, à des sites .geek, .bit, .pirate, etc. Il en existe plusieurs qui répondent chacun à des

95. Propos de Pete Fein dans l'article publié en 2011 sur le site Owni.
URL : http://owni.fr/2011/07/25/telecomix-«-hacker-pour-la-liberte-».

spécificités techniques. Ces registres de sites sont aussi différents sur les darknets qui ne passent pas par ceux mis en place par l'Icann[g] (une des autorités chargées de réguler l'Internet par l'attribution des adresses et numéros). Sans être des darknets, ces DNS alternatifs offrent donc un autre champ explorable, sinon inaccessible par simple configuration des préférences réseau sur un ordinateur.



Navigateur fictif permettant d'accéder à des sites cachés sur le web .clos [96].

Ces stratégies d'autonomie sont restées ponctuelles, des réponses résilientes à un choc. Certaines ont persisté, et c'est l'une des autres limites d'une construction de réseaux parallèles à Internet (qui soient en dehors de). Leur rapport d'échelle ne permet pas l'intégration d'une large population et d'une alternative viable aux usages quotidiens que nous faisons d'Internet. Si l'action performée collectivement autour de *Newstweek* peut s'apparenter à une TAZ en prévoyant une discontinuité entre l'action (le moment de l'apparition) et le repli qui imite la durée d'engagement, elle n'est de fait que ponctuelle, événementielle.

96. Les DNS alternatifs permettent effectivement d'accéder à des adresses web (URL) non répertoriées et accèssibles normalement. Ces extention de noms de domaine font fantasmer des contenus expotiques uniquement accèssibles via le web en utilisant Tor ou d'autres darknets. Comme les *red rooms* ces accès à des contenus occultes sont entretenus par des rumeurs. Le site The Rational Wiki propose un article à ce sujet : « *Fake top level domain names* », URL : https://rationalwiki.org/wiki/Fake_top_level_domain_names. Il y est principalement question du faux TLD .clos et .loky. Ils nécessiteraient l'usage et la configuration de réseaux privés (VPN « *ChaosVPN* » ou des « *Closed Shell System* ») *via* le darknet Freenet. ◊ Le réseau clos fait référence à un dispositif technique à l'état hypothétique pensé par Charles Clos en 1952 selon Wikipédia, *Clos network.* URL : https://en.wikipedia.org/wiki/Clos_network/.

Cette notion de *hinc* et *nunc* (« ici et maintenant »), d'une action adaptée à une circonstance *ad hoc* et *in situ*, la potentialité de ces PirateBox en font un objet de monstration idéal pour créer un espace médiatique localisé d'œuvres utilisant un support web dans un lieu d'exposition. Ils utilisent donc un média entre l'œuvre avec laquelle il se confond et le spectateur. En faisant coïncider la consultation d'œuvres numériques normalement diffusables par Internet (depuis « partout » et par « tout le monde ») avec la localité d'une exposition qui dispense le *hotspot* wifi, les curateurs ou/et artistes créent une limitation d'accès localement.

Échanges locaux

Chat-chouquette – site que je développe depuis 2012 – fait référence au service Chatroulette dont il était question plus avant au sujet de l'œuvre d'Eva et Franco Matter, *No Fun*. *Chat-chouquette* permet d'envoyer des images sans restriction, sans modération extérieure. Elles sont ensuite affichées sur une interface web. Ces images défilent de façon épileptique, par l'interposition de trois d'entre elles (18 images à la minute, ce qui produit une impression d'animation et/ou de superposition). La juxtaposition ainsi générée d'images en all-over sur l'écran crée une narration plus ou moins cohérente entre elles sans hiérarchisation d'ordre. *Chat-chouquette* fait état d'une aliénation compulsive dans la consommation de contenus sur Internet. Une version interactive qui fonctionne avec une PirateBox permet un téléversement aux usagers à proximité.

Ma volonté de mettre en place un outil de monstration localisé et portatif vient d'un attachement aux pratiques de terrain, de guérilla dans l'espace public, hors d'une galerie par exemple. Produire un espace de diffusion indépendant d'Internet, d'une surveillance qui implique une responsabilité en tant qu'hébergeur, a motivé cette recherche plastique. En outre, pour avoir expérimenté l'utilisation de PirateBox (notamment avec du projet *Copiothèque*[97] depuis 2016 qui propose un corpus ouvert de textes autour de recherches collectives), je me suis rendu compte de l'importance de créer un

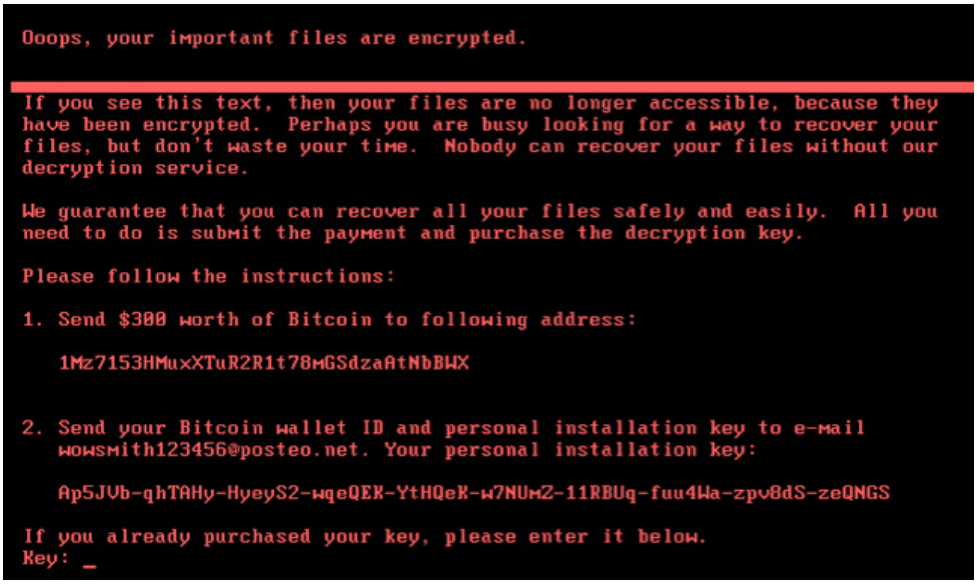
97. Projet mené durant Nuit Debout à Paris avec le collectif Kabane.
URL à propos du projet, téléversement et archive de documents : http://copiotheque.16mb.com.

objet qui invite à la participation, qui rende compte, visuellement et politiquement (dans sa modération), de ce que ces espaces de médiation temporaire permettent : une autonomie dans les choix de la modération et l'expression de chacun dans la construction d'une une narration collective.

[À gauche] Illustration imparfaite de l'animation basée sur un *bug* qui produit le clignotement (*blink* en anglais). Ici, une image de l'interface via un terminal d'*OpenWrt* (utilisé par les PirateBox), une de *Newstweek* et une au sujet des topologies de réseau P2P.
[À droite] Ce projet a été exposé en juillet 2017 à Fiskar, en Finlande, durant l'exposition collective *Smash. Hit.Repeat*. Une interface locale permet aux visiteurs d'envoyer des images qui s'ajoutent ainsi à un flux infini (en boucle).

Les réseaux privés ou localisés produisent des espaces d'autonomie médiatique hors d'Internet et des acteurs qui en choisissent les standards. Cela protège les usagers d'une certaine surveillance et invente d'autres modalités de réseau. Pour autant, il ne s'agit pas vraiment de darknet. Le sens actuel a muté depuis ses premières définitions du temps d'Arpanet, Internet aussi. Ils font aujourd'hui partie de l'iceberg. Ils sont *overlay*[g] à Internet ; ils emploient la même structure : ce ne sont pas des réseaux parallèles, hors de, mais plutôt des réseaux de transport de l'information qui inventent leurs propres protocoles. Ils sont ainsi bien plus accessibles (par Internet), ce qui permet d'envisager des transformations politiques et sociales.

La plupart de ces réseaux obscurs mettent l'accent sur la sécurisation des données, par exemple par le cryptage. Ils inventent une mise en relation qui permet de choisir strictement qui a accès soit aux données, soit à l'origine d'une transmission. Inventer des réseaux qui soient intégrés à Internet permet d'envisager des changements politiques majeurs à une échelle bien plus large que celle permise par un réseau entre amis proches géographiquement. Prétendre à une autonomie du champ social, public, permet de formuler des utopies numériques qui inventent de possibles contre-pouvoirs désinstitués d'un tiers surveillant, qu'il s'agisse d'un État et de ses outils judiciaires qui lui permettent d'appliquer un programme commun ou d'un organisme financier.



Interface affichée sur un ordinateur infecté par NotPeyta dont la fonction est de crypter les données d'un ordinateur et d'imposer à son administrateur d'envoyer 300$ en bitcoins à une adresse (*wallet*[g], ou « portefeuille » en français) pour que ces données soient décryptées. Ces transactions sont difficilement traçables, et il existe des moyens de renforcer l'anonymat du destinataire.

Les *ransomwares*[g], dont il était question plus haut sur la diabolisation du darknet mais plus largement des outils de cryptographie, sont à l'origine de nombreux débats et tentations politiques afin d'en amoindrir la radicalité technique en y installant des « portes dérobées » (*backdoors*[g] en anglais). En 1993, dans *A Cypherpunk's Manifesto*, Eric Hughes[98] explique l'importance fondamentale que

98. Cypher signifie cryptage en français. Il est accèssible à cette adresse : http://activism.net/cypherpunk/manifesto.html semble difficile d'accès, le Manifesto est sauvegardé ici : https://web.archive.org/web/19991207004335/http://activism.net/cypherpunk/manifesto.html.

représente une réelle vie privée pour permettre une réelle liberté de communication. Plus encore, il argue en faveur d'un droit au secret, de la nécessité d'inventer des outils capables de le garantir à distance sans qu'il soit interceptable. En 1996, Timothy C. May a écrit un essai utopique « au sujet d'une hypothétique organisation qu'il nomme Blacknet, qui permettrait d'acheter ou de vendre de l'information en utilisant une clef publique de cryptage, des systèmes de renvoi anonymes et une monnaie digitale qui le soit tout autant ». Selon lui, « Blacknet permettrait de faire des dépôts anonymes sur un compte bancaire de son choix selon les lois en vigueur, d'envoyer de l'argent directement, ou d'utiliser des *crypto credits* avec sa propre monnaie (circulant sur Blacknet). La principale difficulté réside alors dans le fait d'encapsuler l'information (la mettre en bouteille). Son principal propos était alors de pouvoir échanger des secrets »[99].

Jacob Appelbaum dans Menace sur nos libertés - Comment Internet nous espionne - Comment résister fait, lui aussi, référence à Timothy May comme source d'inspiration. Ce qui nous intéresse ici, c'est aussi de voir comment les communautés non anonymes ont communément pensé une autre société par le cryptage. Un aspect historique qui est bien différent de la mythologie autour de Satoshi Nakamoto (inventeur de la blockchain non encore identifié) ou tout collectif anonyme.

> « Si on remonte très, très loin dans le temps, à la vieille liste de diffusion Cypherpunk avec Tim May, l'un de ses membres fondateurs, et si on lit les vieux posts de Julian [Assange] sur la liste Cypherpunk, c'est ce qui a amené toute une génération d'individus à vraiment se radicaliser, parce que les gens ont compris qu'ils n'étaient plus atomisés, qu'ils pouvaient prendre le temps d'écrire un logiciel capable de donner du pouvoir à des millions d'individus. »[100]

Zimmerman participe à la mise en place des logiciels de cryptage PGP[g] (*Pretty Good Privacy*, série logiciel permettant l'usage du cryptage facile pour tous). On sent chez Timothy C. May une réelle envie de subordination aux Etats qui dépasse la question d'anonymat, imaginant une organisation qui invente, dans ses échanges, d'autres façons de créer de la confiance, de la notoriété.

99. Traduction d'après le texte de Peter Ludlow, *Crypto Anarchy Cyberstates and Pirate Utopias*, éd. MIT Press, 2001, p. 136.

100. La discussion est accessible à cette adresse (au sujet de Blacknet, sur la liste des « cypherpunks », jonction des mots « chiffrement » et « punk ») : http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/blacknet.txt

C'est une réalité dans les marchés noirs sur le darknet qu'est Tor par exemple où les *escrows*[g 101] et les réputations sont primordiaux pour l'achat d'un produit, peu importe son illicité. L'anonymat nécessite l'invention d'une autre relation, d'autres types de garanties dans le contexte d'échanges entre anonymes moins sûrs sur les darknets (ne permettant pas une traçabilité, une historicité). Tout comme la *do-ocratie*[102] donne le pouvoir de façon très individuelle à celui qui fait (*to do* : faire), le débat est essentiel dans ce type d'organisation micro-politique pour décider des orientations d'un projet confrontées à leur faisabilité technique. Une orientation nécessaire dans l'écriture d'une utopie concrète. Un moyen de produire collectivement, d'autres politiques en réseau, d'autres registres décentralisés[103].

On dit qu'il faut faire des compromis ou on appelle un perfectionnement du code ; on dit aussi que « le code fait loi » (*code is law* en anglais) – un "on" collectif et relatif à soi-même. Un espace de délibération et d'opinions est primordial dans ce type d'interaction cotributaire. Ce dialogue se construit autour d'un volontariat organisé autour d'idéaux communs. Une organisation très présente dans l'idéal *open source* – le fait, par exemple, de partager les sources d'un logiciel tel que le système d'exploitation Linux. Cette transparence permet aussi d'en vérifier la réalité technique (par exemple que Tor ne contient pas de failles de sécurité) par une veille collective, à l'aide d'autres développeurs qui ne sont pas les auteurs du projet. Eric Steven Raymond est l'un des portes voix de l'open-source les plus connus aujourd'hui. Libertarien, ses idées sont souvent affiliées à la notion d'ordre spontané.

101. Traduit par dépôt fiduciaire est un tiers reconnu comme de confiance qui va arbitrer une transaction afin de dédommager acheteur en cas de litige, c'est un tiers payant qui permet d'assurer, en dehors de la réputation des vendeurs, qu'un achat entre anonymes soit moins risqué.

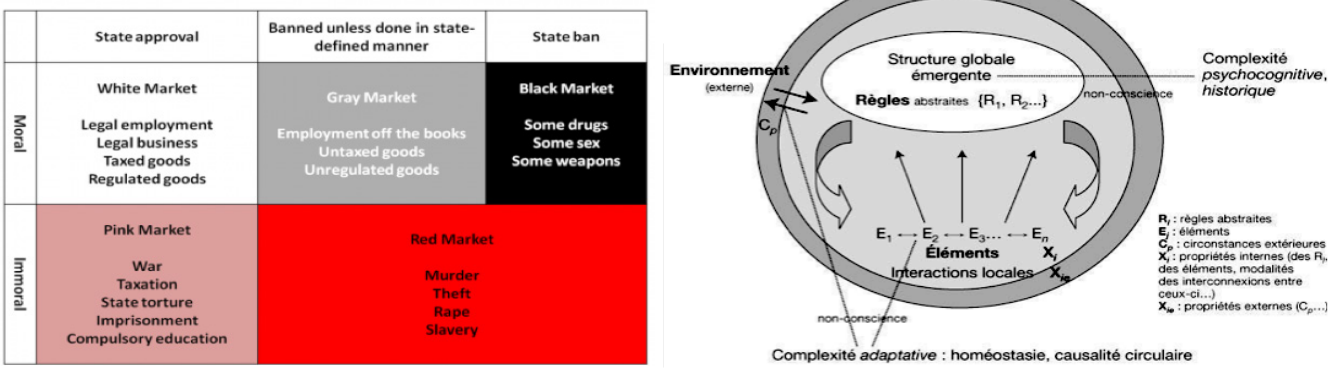
102. Wikipedia : « En do-ocratie, chacun a de l'influence ou du pouvoir à la mesure de ce qu'il fait. C'est un modèle particulièrement efficace pour faciliter la prise d'initiative et l'implication par le plus grand nombre. La do-ocratie est au cœur du fonctionnement des wikis et des *hackerspaces* ». URL : https://fr.wikipedia.org/wiki/Do-ocratie.

103. Nous pensons ici au Triangle de Zooko qui donne trois règles simples pour créer un index de sites autonome, décentralisé, sécurisé mais humainement compréhenssible. À mon sens les DNS sont le fondement d'autres types de réseaux *overlays*. La sécurisation de ces derniers par le cryptage ou d'autres moyens est quant à elle nécessaire pour créer des darknets : des réseaux créant une forte altérité.
◊ Wikipédia : « Le triangle de Zooko propose par exemple une méthodologie autour de la création d'un système d'adressage permettant la mise en place d'un système de communication sécurisé, humainement compréhensible et décentralisé. Ces principes donnent une orientation à un projet mené collectivement par exemple dans l'invention de distributions de sites et de leur enregistrement au sein d'un index (DNS, une caractéristique fondamentale dans la création de systèmes d'échanges sur Internet décentralisés d'une gouvernance extérieur, dans la création d'autonomie). » https://fr.wikipedia.org/wiki/Triangle_de_Zooko. Penser collectivement ces architectures de distribution de l'information relève d'une volonté éthique orientée. Le Triangle de Zooko offre donc une méthodologie de travail, un support de réflexion, dans la création de logiciels (et de réseaux).

> « Le monde Linux, sous de nombreux aspects, se comporte comme un marché libre ou un écosystème, un ensemble d'agents égoïstes qui tentent de maximiser une utilité, ce qui au passage produit un ordre spontané, autocorrecteur, plus élaboré et plus efficace que toute planification centralisée aurait pu l'être. C'est ici qu'il faut chercher le "principe de bonne intelligence" [l'auteur fait ici référence à Kropotkine[104]]. »
> **Eric Steven Raymond, « La cathédrale et le bazar », La Revue des ressources**[105]

Marché libre : autonomie de distribution

L'idéal de l'économiste Friedrich Hayek, penseur politique et économiste du XX^e^ siècle[106], est souvent cité au sujet de la technologie distribuée de la *blockchain* qui, bien que basée sur le consensus majoritaire et la vérification collective, permet d'imaginer une topologie de réseau horizontal de distribution et de vérification de l'information sans pour autant passer par un pouvoir centralisant tel une banque ou un état. Le projet de cet économiste ayant participé au projet cybernétique prônant la libre circulation sans entrave de l'information – proche du principe de libre-échange – défend la liberté d'entreprendre et le marché libre que la *blockchain* rend possible. Il prône en effet un libre marché (*free market*) : une autonomie tant économique que sociale, où l'individu est seul responsable, ses intérêts égoïstes seuls le poussant à une attention sociale.



À gauche] Schéma d'émergence dans l'ordre social spontané. [À droite] Schéma qui catégorise cinq marchés (marchés noirs et marchés libres), différenciant ceux moraux (légaux) de ceux qui ne le sont pas vis-à-vis de l'approbation ou prohibition de la part des Etats (document partiel en faveur du libre marché) . On peut y lire à propos de ces cinq marchés (trad. de l'anglais) : **1) moral - marché blanc (approuvé par l'Etat)**, emploi et affaires légales, taxation et régulation des biens ; **2) interdits à moins que l'Etat n'en définisse les règles - marché gris**, emploi et biens (revenus) non enregistrés, non-taxation des biens ; **3) marché noir** (interdit par l'Etat), certaines drogues, pratiques sexuelles, armes ; **4) immoral - marché rose (approuvé par l'Etat)**, guerre, taxation, emprisonnement, école obligatoire ; **5) marché rouge (interdit par l'Etat)**, meurtre, vol, viol, esclavage. On peut ici faire un lien entre *red room* et marché rouge : le pire de ce qui peut être proposé comme service.

---

104. Wikipédia : « Pierre Kropotkine (1842-1921), communisme libertaire russe, auteur entre autres de *L'Entraide, un facteur de l'évolution* », https://fr.wikipedia.org/wiki/Pierre_Kropotkine .

105. Eric Steven Raymond, auteur de l'essai *La cathédrale et le bazar* écrit en 1999, est considéré comme le « ecocréateur du terme open source », https://fr.wikipedia.org/wiki/La_Cathédrale_et_le_Bazar/ .
◊ Eric Raymond et Bob Young, *The Cathedral & the Bazaar*, O'Reilly, 2001.
◊ Lien vers l'article cité (partie 10 « Le contexte social du logiciel dont le code source est ouvert ») : Eric Steven Raymond, « La cathédrale et le bazar », *La Revue des ressources*, 2013, http://www.larevuedesressources.org/la-cathedrale-et-le-bazar-eric-steven-raymond,2534.html [Annoté : http://mht.vincent-bonnefille.fr/20170820__La_cathedrale_et_le_bazar_-_Eric_Steven_Raymond_-_La_Revue_des_Ressources__http___www.larevuedesressources.org_la-cathedrale-et-le-bazar-eric-steven-raymond,2534.html.mht].

106. Wikipédia : « Friedrich Hayek ». URL : http://fr.wikipedia.org/w/index.php?title=Friedrich_Hayek .

L'ordre spontané qu'il formule explicite le fonctionnement en essaim (*swarm*[g]) permettant à des individus (ou organisme animal), portés par des intérêts communs (inconscient), de s'auto-organiser sans pouvoir dirigeant apparent (intermédiaire bureaucratique). Cette idée que l'on retrouve dans les stratégies médiatiques des TAZ est de cet ordre : une hiérarchie horizontale dont le chaos apparent est sous-tendu, entre les individus, par un intérêt collectif. L'imaginaire du libre marché et de l'ordre spontané fait, mis en relation, penser au principe économique de « main invisible », d'une macropolitique qui gouverne les individus tous motivés par un projet collectif sous-tendu par le capitalisme (une gouvernementalité).

> « En 1972, Jo Freeman a décrit dans La tyrannie de l'absence de structure les premières expériences d'auto-organisation féministes. Le problème avec les organisations non hiérarchiques est que les structures de pouvoir sont invisibles et donc inexplicables ce qui conduit souvent à des dysfonctionnements et des abus, estimait déjà Freeman. Fred Turner décrit les mêmes problèmes quand il évoque, dans Aux sources de l'utopie numérique, les communautés hippies. […] "La même impulsion anti-hiérarchique existe dans la Silicon Valley que dans les communautés autonomes des années 1960", estime Finley. »
> **Hubert Guillaud, « Ce que l'internet n'a pas réussi (3/4) : distribuer l'autorité »**[107]

Autonomie libérale : une utopie réalisée ?

Le film de fiction *Dope* («drogue» en anglais), réalisé par Rick Famuyiwa, sorti en 2015 [← affiche du film ci-contre], raconte, au fil d'aventures, comment des jeunes Américains se retrouvent malgré eux obligés d'acheter des drogues avec des bitcoinsg sur le darknet. D'autres films et séries font mention du darknet, mais celui-ci a pour particularité d'en faire son sujet d'intrigue. Cette popularisation de l'activité illicite sur des marchés dérégulés, hors la loi, me semble importante pour exprimer combien, en quelques années, ces technologies se sont démocratisées. On peut se demander si cette popularité ne vient pas avant tout d'une adéquation au libre marché qui poursuit, par l'anarcho-capitalisme, l'idéal libéral, celui d'une liberté individuelle d'acheter, de consommer. Plus que l'accès à des produits stupéfiants, des drogues, qui existaient bien avant les darknets, c'est les modalités de leur échange qui a changé. Elles permettent de meilleures

107. Hubert Guillaud, «Ce que l'internet n'a pas réussi (3/4) : distribuer l'autorité», 2013. URL : http://www.internetactu.net/2014/03/18/ce-que-linternet-na-pas-reussi-34-distribuer-lautorite/ .
◊ Benjamin Loveluck, *Réseaux, libertés et contrôle - Une généalogie politique d'Internet*, éd. Armand Colin, Paris, 2015, p. 268, à propos du printemps des parapluies, FireChat (2014) et autres réseaux autonomes.

conditions d'évaluation des produits achetés dans un rapport souvent clientéliste mais favorisent en même temps l'émergence de réseaux de trafics qui ne sont toujours pas pris en charge par les sociétés qui cherchent le plus souvent à empêcher la banalisation de ces consommations[108].

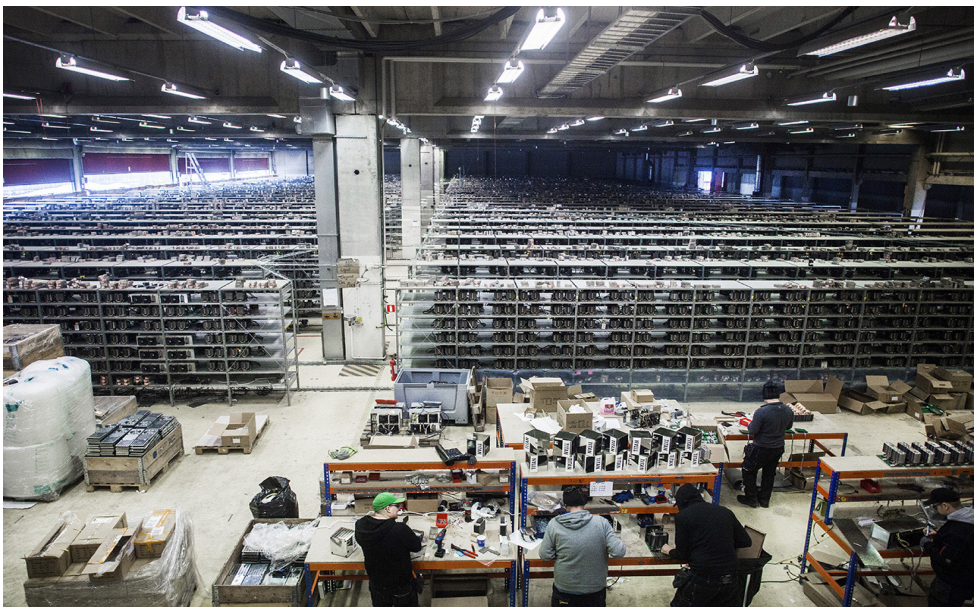
Or ces consommations d'autres produits, échappant à la taxation étatique, poursuivent à mon sens l'idéal d'une toujours plus grande liberté de circulation de marchandises et de savoirs/connaissances. Le logiciel Tor est utilisé dans le film pour accéder à un site caché qu'il rend accessible. La popularisation de ces réseaux travaille à mon sens à une ingénierie sociale. Elle rend favorable l'intégration progressive des technologies qui sous-tendent ces technologies montrées comme fonctionnelles servant les intérêts d'une certaine économie.

Blockchains : quel projet ?

Une *blockchain* est un maillage de distribution qui permet l'échange de crypto-monnaies[g], représentant pour certains une nouvelle révolution. Cette technologie permet des échanges distribués en réseau, de façon horizontale, et sécurisée permet de résoudre des problèmes limitant par exemple l'utopie d'un blacknet formulée par C. May, en combinant au cryptage des dispositifs de contrôle et de vérification synchronisés par Internet. La radicalité politique et l'autonomie qu'offre une *blockchain* ne se limite pas à l'échange monétaire ; elle amène à imaginer des applications permettant un consensus décisionnel sous la forme d'un bazaar (mentionné plus avant). On peut toutefois s'interroger sur l'économie qui la sous-tend entre libertarisme et libéralisme. Comme en ce qui concerne les *black boxes* et *data centers* qui échappent au regard ou à la vision[109], il faut se demander ce que ces dispositifs computationnels, nécessitant de très fortes capacités de calcul, produisent de dépendance énergétique (et donc d'impact écologique), mais surtout vers quels modèles sociaux ces technologies nous mènent.

108. Les plateformes de vente sur le darknet offrent certes la possibilité d'échanger de produits différents de ceux proposés sur des sites marchands sur le *clear web* (tel Amazone), mais pas tant dans le principe commercial entre acheteurs et vendeurs. Les dispositifs d'évaluation d'un vendeur et de ses produits (systèmes de commentaires, notes, avis sur les produits, etc.) y sont semblables. On y retrouve ainsi des stratégies de fidélisation du client pour qu'il évalue en bien un produit et augmente ainsi la notoriété de son vendeur.
109. Un regard transparent par le code source pour les *black boxes* ou logiciels algorithmiques.
Une vision pour les centres de stockage des données (*data centers*, serveurs) souvent à distance géographique des villes.

Cette technologie de *cloud computing*[g] garantit aussi l'avènement de l'IoT[g] (*internet of things*) : une domotique, augmentant le nombre d'objets connectés en réseau permettant plus de surveillance dans la sphère privée, chez soi. Comme toute technique, elle n'est pas une alternative culturelle si, avec elle, ne s'opère pas une transformation des désirs et des pouvoirs. Une *blockchain*, *overlay* à Internet, se base sur une infrastructure réseautique et en favorise l'expansion, le projet social (cf. carte mondiale au sujet de la population d'ordinateurs connectés avec une IPv6). Son aspect totalisant, même s'il permet de s'affranchir d'institutions tierces (des banques ou encore des institutions décisionnelles étatiques) poursuit ce qui a permis une surveillance de masse sur Internet. L'indexation de toutes les transactions dans une *blockchain* signifie que, malgré la sécurisation par cryptage de ces transactions, celles-ci peuvent faire l'objet d'une enquête, d'un fichage. Des services complémentaires sont capables, sur le même principe que Tor interchangeant les adresses IP, de brouiller les pistes en mélangeant les Bitcoins entre des usagers d'une *blockchain* (de les mixer, d'intervertir les identités des transactions dans l'index).



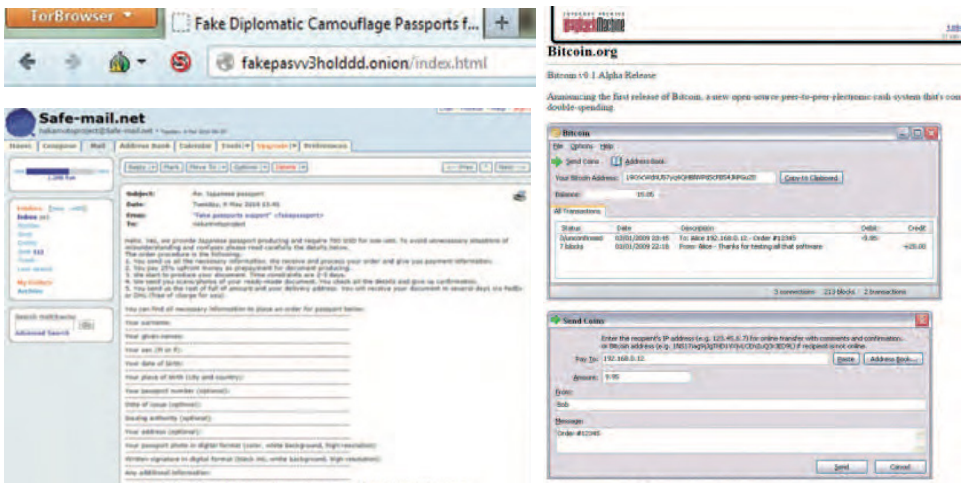
L'une des salles informatiques de KnCMiner à Boden (une entreprise anglo-suédoise de « minage »)[110]. Les mineurs numériques d'une blockchain sont rétribués en bitcoins pour avoir aidé à vérifier des transactions d'autres utilisateurs au sein d'une *blockchain* – registre infalsifiable des transactions empêchant par consensus la fraude. Pour combiner leurs chances, ils se regroupent autour de *pools* (image d'une piscine permettant de se retrouver en cercle et de diminuer la température – des individus, des serveurs –).

110. Yves Eudes, « Dans le *data center* de Facebook, aux abords du cercle polaire » (photographie : Stefan Bladh), *Le Monde*, 2016 http://www.lemonde.fr/grands-formats/visuel/2016/06/29/dans-le-data-center-de-facebook-aux-abords-du-cercle-polaire_4960471_4497053.html.

Satoshi Nakamoto : non anonyme

Les artistes Émilie Brout et Maxime Marion ont voulu réaliser le passeport de Satoshi Nakamoto, personnage mystérieux qui se cache derrière l'invention de la blockchain (par extension du bitcoin) – elle pourrait être le fruit de plusieurs individus cachés derrière une identité unique. Les artistes ont tout d'abord reconstitué l'identité supposée de Satoshi Nakamoto à partir d'informations trouvées sur le *clear web* et ailleurs. Cette enquête préalable leur a permis d'établir un portrait approchant en se basant sur des archives ou des histoires autour de ce personnage. Ils ont ainsi déconstruit l'imaginaire, cherché à défaire le vrai du faux pour produire une identité la plus fidèle possible de celui qui se cache derrière le mythe colporté de Satoshi Nakamoto. Ils ont suivi les pistes semées par l'inventeur, ils ont retiré les couches de l'oignon les unes après les autres.

Ils ont ensuite commandé un passeport à l'effigie de l'image à laquelle était censé ressembler, à leur avis, l'inventeur de la *blockchain*. Ce document, hautement sécurisé, produit par des faussaires, ne leur parviendra pas. Ils ont toutefois reçu un document prouvant que le passeport avait bien été réalisé à partir des informations qu'ils avaient envoyées pour qu'il soit confectionné. C'est suite à cette confirmation de l'existence du produit qu'ils avaient commandé (et à la garantie qu'il soit conforme à leurs attentes) que les deux artistes ont envoyé un premier acompte (à une adresse, en bitcoins), soit la moitié du prix total 0.328 BTC (125 € le 5 juin 2014).



Documents de l'enquête sur Satoshi Nakamoto par Émilie Brout et Maxime Marion. On y trouve :
le lien vers le site de commande de passeports contrefaits via le navigateur Tor : http://fakepasvv3holddd.onion ;
une réponse à leur commande par mail – via un service accessible depuis le *clear web* : http://safe-mail.net – de la part des responsables du site où ils ont commandé le passeport ;
une version archivée (Internet Archive) d'une page web au sujet de la création du bitcoin par Satoshi Nakamoto[111].

111. Détails sur les étapes d'élaboration : http://www.eb-mm.net/en/projects/nakamoto-the-proof/ .

[Ci-contre] *Nakamoto (The Proof)*, tel que présentée dernièrement durant l'exposition *The Black Chamber*[112]. Un écran lumineux connecté en USB présente ce document et rappelle ainsi les conditions initiales de numérisation (scan), sur papier, format A4.

Ce processus d'enquête et l'intervention d'un tiers dans la confection de leur œuvre mettent en avant deux points importants. Le fait que les artistes ne soient pas experts en tout et qu'il leur faille parfois faire appel aux services d'un technicien/artisan ayant les compétences requises pour réaliser leurs projets. Ensuite, la proposition d'Émilie Brout et de Maxime Marion, en dehors de la fiction qu'ils perfectionnent, met en exergue les conséquences du travail de faussaire qui s'exerce sur d'autres champs (dans la contrefaçon de produits de marque, la copie d'œuvres d'art, etc.). Ces pratiques vont contre l'autorité du document normalement unique, non reproductible, infalsifiable. Créer un faux document permet de se libérer des instances qui les délivrent. Il en va de même, bien entendu, pour la création de faux billets[113].

On comprend mieux ainsi en quoi l'enfer de Dante punissait les faussaires qui, par l'usage de faux, dévaluent le pouvoir autoritaire accordé aux documents et donc à ceux qui s'en servent pour produire du contrôle (en vérifiant la conformité). La reproductibilité technique d'un objet ne lui confère peut-être pas l'aura d'un original et en transforme peut-être la perception[114]. Pour autant, il trouble et augmente l'incertitude et oblige à l'invention de nouveaux outils capables d'enquêter plus en profondeur, de vérifier (de surveiller). *Nakamoto (The Proof)* est, comme son titre l'indique une preuve du processus de création des deux artistes. Ils exposent ce document imprimé sur lequel apparaissent le passeport et le *scanner* qui a servi à le numériser pour les motiver à payer. Tous les éléments qu'il contient, à défaut d'avoir réellement réalisé l'objet, produisent l'œuvre. Ce qu'ils réalisent, c'est l'inclusion d'un individu fictif mais ayant eu une existence en ligne, dans la société, avec les moyens qui lui permettent de confirmer le réel. En créant une identité de papier du mystérieux inventeur, les artistes vont à contresens de ce que son invention et les darknets rendent possible : un anonymat numérique.

---

112. Émilie Brout et Maxime Marion, *Nakamoto (The Proof) - Passport Scan (.jpg file, 2506 x 3430 px)*, 2014.
◊ *The Black Chamber - surveillance, paranoia, invisibility & the internet*, Škuc Gallery, Ljubljana, 2016. Les artistes du !Mediengruppe Bitnik – dont il va ici être question – y sont également exposés.

113. À noter que les Bitcoins sont une alternatives au système banquaire actuel et promettent une sécurité contre la fraude. Ces crypto-monnaies sont des alternatives et non pas des faux

114. Walter Benjamin, *L'œuvre d'art à l'époque de sa reproductibilité technique*, Gallimard, Paris, 2008 (version de 1939), traduit de l'allemand par Maurice de Gandillac. Réflexion sur les changements opérés sur une œuvre en étant reproduite poursuivie par Stéphane Vial avec le concept d'ontophanie qui désigne l'apparition des objets. Il actualise cette réflexion dans *L'Etre et l'écran : comment le numérique change la perception*, éd. Presses universitaires de France, Paris, 2013.

The Random Darknet Shopper

Dans un contexte qui précède la chute de Silk Road (marché noir sur le darknet accessible via Tor saisi par le FBI en 2013) – plus récemment, la saisie des sites cachés sur Tor Hansa et Dream Market[115] a, une fois de plus, relativisé la résistance d'un anonymat numérique des administrateurs de ce type de sites soumis à une enquête ciblée –, les artistes du groupe !Mediengruppe Bitnik (Carmen Weisskopf et Domagoj Smoljo) mettent au point un bot capable d'acheter des contenus sur Agora (site caché via Tor), avec un budget fixé de bitcoins (à hauteur de 100 $[116]) : *The Random Darknet Shopper*[117]. La principale source d'authentification d'un acheteur sur ce type de marché sur le darknet reste les commentaires d'autres usagers ; certains sites vérifient les vendeurs, ou mettent en place des systèmes d'arbitrage neutres : *escrows*. Toutefois, l'information préalable sur un produit ou usager permet d'écarter plusieurs arnaques dans un milieu pas souvent soumis à des garanties. Ce sont ces procédures rassurant le consomateur qui sont codées pour que le *bot* identifie un produit interessant, suceptible d'arriver à bon port. Le *Random Darknet Shopper* rejoint les autres utilisateurs du réseau Tor, il y reproduit les usages, utilise les mêmes procédures. Les artistes disent s'intéresser au statut légal de ces transactions déléguées à un ordinateur. Ce dernier est placé dans l'exposition, écran allumé. Par une interface textuelle, il rend compte auprès du public des activités et transactions en cours, des bitcoins échangés, etc.

Micro-ordinateur exposé : il affiche, les transactions en cours, l'état de la comande. Une barre clignotante et l'animation du texte esthétisent une écriture en cours. Ici, il indique, que des informations sont arrivées en provenance d'Ukraine.

Il peut s'agir d'une indication fournie par le vendeur sur le darknet au sujet d'un produit acheté / consulté par le *bot* sur le marché noir.

Ce type d'ordinateur est couramment utilisé comme terminal directement branché à un serveur.

115. C. Aliens, *A Globally Coordinated Operation Just Took Down Alphabay and Hansa*, Deep Dot Web, 2017.
URL : https://www.deepdotweb.com/2017/07/20/globally-coordinated-operation-just-took-alphabay-hansa/.
◊ Adrian Crenshaw durant sa conférence *How Tor Users Got Caught* à la Defcon 22 de 2014, explique comment les cybercriminels se sont fait prendre suite à une enquête ciblée. URL vers la vidéo : https://archive.org/details/youtube-7G1LjQSYM5Q.

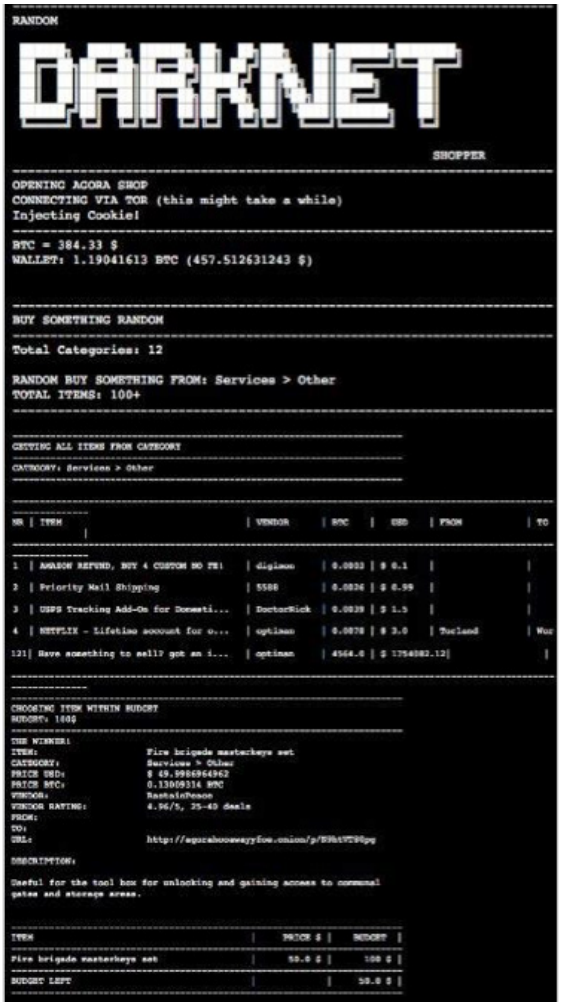
116. Marie Lechner, « Connecter le darknet au champ artistique », interview de !Mediengruppe Bitnik dans *Libération*, 2014.

117. !Mediengruppe Bitnik, The Random Darknet Shopper, exposition collective « *The Darknet - From Memes to Onionland. An Exploration* », Kunst Halle Sankt Gallen, 2014.
URL du projet et des actualités relatives : https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/r=/.

Cette installation, proche du mail-art, sur le darknet, reflète une activité parallèle et ne remet en rien en cause le trafic qui le sous-tend. L'installation est plusieurs fois exposée et a posé la question évidente de la dangerosité de confronter le public à des substances illicites ou à des produits contrefaits. Un tel événement s'est produit quand le *bot* a acheté des stupéfiants (MDMA, ecstasy) retirés de l'exposition par la police. Les artistes précisent sur leur site : « Le but de la confiscation est d'empêcher la mise en danger de tierce personne par l'exposition de drogues, en les détruisant. C'est ce que nous savons pour le moment »[118]. L'informatique est faite, dans la conception des processeurs principalement, pour automatiser en répétant des ordres simples. Ce que met en avant le *bot* des artistes, c'est une automatisation de transaction sur une plateforme dont la particularité repose sur les produits vendus. Ils connaissent les risques, et ce contexte fait partie de leur propos critique au sujet de l'automatisation informatique.

Le risque d'une automatisation du travail (comme nous l'évoquions avec *Dark Content* d'Eva et Franco Mattes) ou encore au sujet de la gouvernementalité statistique est bien que des tâches nécessitant une délibération, une actualisation pour déterminer des potentialités – discontinuant une suite logique d'événements normalement prévus sur la base de données agrégées dans le passé – soient déléguées à des logiciels d'aide à la décision. Plus qu'une aide, ces derniers exécutent eux-mêmes des ordres et ainsi, comme c'est le cas avec la surveillance de masse, ne font plus appel à des instances compétentes, elles, potentiellement critiques. Des instances qui ont pour rôle, en tant qu'agents, de séparer, par exemple, un pouvoir étatique exécutif et une justice délibérante. La généralisation de l'automatisation informatique, de la mise en réseau avec l'IoT, laisse planer une incertitude quant au réel pouvoir des usagers sur ces systèmes complexes et, surtout, gérés à distance. *The Darknet Shopper* ne va pas pour autant aussi loin. Il nous paraît surtout exercer une série de tâches complexes mais redondantes. Une suite d'ordres dont les développeurs de ce bot ont le secret ce qui ne les dédouane pas de toute responsabilité. Cette œuvre met en avant le risque d'une automatisation généralisée sur laquelle les citoyens n'auraient pas de droit au regard, à la critique.

118. Traduction partielle d'après l'aricle de Hugo Pascual, « Le "Random Darknet Shopper», un robot derrière les barreaux », *Libération*, 2015. URL : http://next.liberation.fr/culture/2015/01/19/le-random-darknet-shopper-un-robot-derriere-les-barreaux_1183963. Page du site des artistes à ce sujet : https://wwwwwwwwwwwwwwwwwwwwwww.bitnik.org/r/2015-01-15-statement/ (2015).



!Mediengruppe Bitnik, *The Random Darknet Shopper,* exposé durant *The Darknet : From Memes to Onionland*, Kunst Halle Sankt Gallen, 2014.

[À gauche] Interface du *Random Darknet Shopper* le 05-03-2016 (depuis le site dédié, extrait). Le visiteur peut y voir les opérations du *bot*, son budget / dépenses, les sites visités, etc.

[À droite] Vitrines où sont exposés les le contenu des paquets reçus (produits). Dans le premier caisson une paire de chaussures de sport, dans le second l'extasy. Ils contiennent aussi les paquets d'origine, les colis.

Ce qui prend sens dans cette exposition de produits manufacturés, c'est leur originalité, leur mise en scène, sous verre : ils sont présentés comme des reliques, muséifiés. Une mise en valeur d'objets déjà fabriqués industriellement ou artisanalement, certes non pas choisis par les artistes directement, comme le ferait un acheteur soucieux d'opérer le meilleur investissement, mais comme objets exotiques du fait de leur origine mise en avant par le micro-ordinateur et la console du *Random Darknet Shopper*. L'intermédiaire entre la galerie/musée et une plateforme sur le darknet. Deux interfaces sont utilisées pour signifier l'expéditeur et le destinataire : les adresses de *wallet* du vendeur sur la console du micro-ordinateur ; une fois la commande arrivée dans l'espace d'exposition, l'adresse sur le paquet, et tous les éléments, même les plus anecdotiques qui renseignent sur son origine et son transport (tampons, timbres, etc.). Ces métas ont, dans l'exposition, juxtaposé aux objets un rôle de cartel : elles contextualisent l'objet exposé. Les deux artistes se sont intéressés à cet entre-deux, dans l'échange postal avec l'œuvre *Delivery to Mr Assange*.

Delivery to Mr Assange

En 2013 les artistes du !Mediengruppe Bitnik envoient un colis à l'ambassade d'Équateur de Londres, destiné à Julian Assange[119] (où il séjourne contre son gré), dans lequel ils installent une caméra qui retransmet en streaming les images qu'elle capte de l'extérieur du paquet (à intervalle régulier). Ce flux sera ainsi commenté par des internautes, en ligne, à travers le monde, captivés par le fait que ce paquet arrive à l'emblématique fondateur de Wikileaks. Ils craignent que le colis soit intercepté, et de ne pas voir Assange communiquer avec eux comme prévu. Le champ de la caméra est souvent obstrué et les brèves apparitions et mouvements à l'image ponctuent 32 heures de transmission entre l'envoi et la réception du paquet. Le dispositif de diffusion à distance, comme dans *No Fun* d'Eva et Franco Mattes, produit une attractivité autour d'une transmission en direct. Mais !Mediengruppe Bitnik crée une narration et un dispositif médiatique de toutes pièces. Le groupe fait une promesse à un public qu'il rassemble, qu'il unit autour d'un projet commun dont il est conscient.

L'intérêt porté par les spectateurs suivant le paquet via Internet fait penser au travail collaboratif dont il était question plus avant au sujet de l'open source permettant une veille et une vérification autour de la fiabilité d'un logiciel. Un volontariat collectif, qui partage l'attention de personnes réunies autour d'une activité dans un but créant du commun. Certain d'entre eux vont par exemple, spontanément, mettre à profit leurs compétences pour déchiffrer ce que l'image ne dit pas afin de combler les moments d'incertitude, d'attente. Ils peuvent ainsi faire profiter de leurs recherches via un canal de discussion (chat). Ils opèrent une surveillance qui cherche à rendre transparent le moindre nœud d'intrigue (sur la base d'hypothèses et d'analyses alimentant le débat au sein de cette agora).

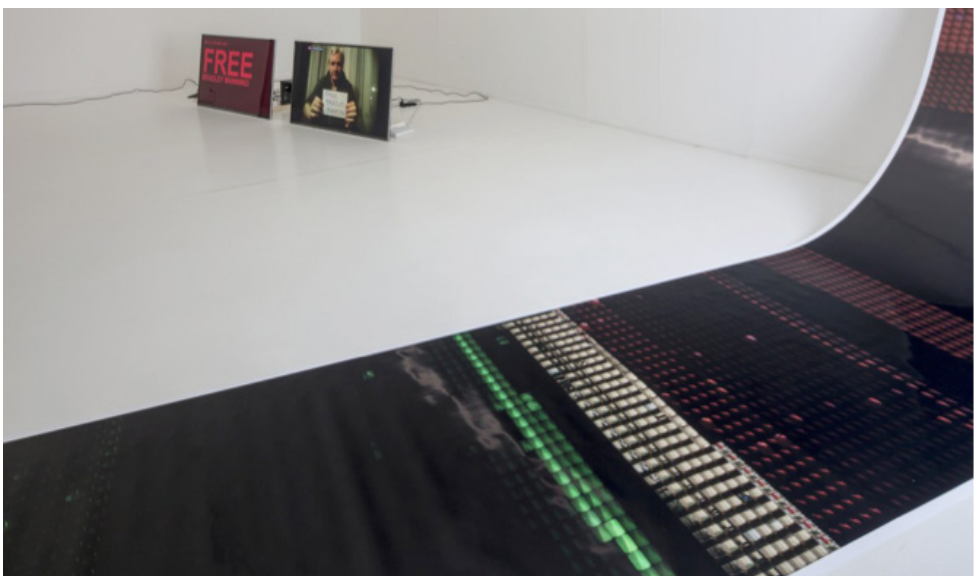
119. Mediengruppe Bitnik, *Delivery for Mr. Assange (a live mail art piece rrrrrrrrrrrrrrrrrrrrrrrrrrradical realtime)*, performance vidéo, installation, 2013. URL : https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/assange/ .

Les artistes décrivent leur paquet comme un « REAL_WORLD_PING »[120] : un ping[g] qui envoie des informations – des images – à intervalle régulier, depuis le monde réel, un système de vérification informatique d'accès sur un réseau dont il était question au sujet des darknets du temps d'Arpanet. En plus du canal de discussion (chat), un flux d'actualité sur Twitter permet de suivre le colis géolocalisé par une balise GPS. Ce dispositif de surveillance capte une part négligée des réseaux de communication. Il révèle les dessous d'un réseau de distribution civil, géré par plusieurs intermédiaires. Cette œuvre de mail-art produit un dispositif de monstration plutôt que d'enquête. Plus encore que la discussion sans son avec le fondateur de Wikileaks (qui utilise des cartels pour écrire des messages retransmis en ligne en demandant par exemple justice pour Aaron Swartz Chelsea Manning[121]), c'est l'exposition au regard des infrastructures postales qui est saisissante. Certes, le spectateur de *The Darknet Random Shopper* peut suivre les étapes intermédiaires précédant à la réception de nouveaux paquets, mais il ne voit pas le chemin parcouru entre l'expéditeur et le destinataire… justement parce que le réseau Tor discontinue, ou du moins brouille le lien entre l'un et l'autre : il rend impossible le suivi d'un paquet, il anonymise la source, il l'oublie.

Écran séparé (en deux « canaux »/écrans sous sa forme d'installation). Sur celui de gauche, un texte présente la date, l'heure. Le texte qui suit est animé, il reprend successivement des actualités liées à l'évolution du paquet, entretient le suspens, temporise, en lien avec l'écran de droite… sur lequel les images capturées par la caméra à l'intérieur du paquet, ici un poste de tri à proximité de l'ambassade.

120. Site officiel de la installation/vidéo : https://wwwwwwwwwwwwwwwwwwwwwwww.bitnik.org/assange/.
121. Aaron Swartz était activiste il est arrêté en pour avoir contourné en 2010 les systèmes d'accès du service Jstor (service américain distribuant en partie des documents libres de droit) [informations complémentaires et œuvres relatives à son action : http://44llcbgyt22pwvyq.onion/aaronswartz/ (site personnel accessible via Tor) et « What Aaron Swartz did at MIT », 2013. URL : https://www.dailykos.com/story/2013/1/13/1178600/-What-Aaron-Swartz-did-at-MIT] ; Chelsea Manning est une lanceuse d'alerte qui avait permis à Wikileaks de se faire connaître d'un plus grand nombre en divulguant des informations confidentielles au sujet d'exactions perpétrées par les États-Unis en guerre en Irak en 2010-13.

À mon sens, la dramaturgie mise en place autour de Julian Assange est plus riche, plus intéressante car elle révèle quelque chose du réel, à l'intérieur du réseau. L'une et l'autre me semblent complémentaires. Ce que *The Darknet Shopper* réussit c'est bien de rendre partiellement compte des activités de leur bot par des feed-back dans l'exposition, ce qui rend l'œuvre performante. Tout comme *No Fun*, *Delivery to Mr Assange* fait état d'une performance passée, exposée a posteriori. Il me semble, au regard des vidéos présentes sur YouTube (https://youtu.be/zlZTghhCuxg/) ou de l'explication de la part des artistes durant des interviews ou conférences (dont https://exposingtheinvisible.org/films/losing-control-delivery-for-mr/), que le flux exposé ne montre pas les 32 heures de streaming, mais la juxtaposition des images. Elles sont commentées sur un second écran celui à gauche [sur la photo ci-dessous] par des textes animés en rouge faisant penser à une interface, à une console en train d'écrire, comme en fonction, réagissant aux images : ils ponctuent l'intrigue, renseignent sur la position du paquet, situent l'action. Ce support textuel soutient la tension dans les moments de latence où rien n'est visible à l'écran de droite – noir ou obstruant le champ de vision de la caméra. Ils restituent ainsi l'incertitude, font part des questions qu'eux-mêmes et d'autres internautes se sont posées durant la transmission du paquet : une dramaturgie est en place.



Au premier plan, impression couleur des différentes images capturées à intervalle régulier. En arrière-plan, deux écrans : sur celui de droite, l'image prise par la caméra, et sur celui de gauche, les commentaires sur le compte Twitter dédié à l'actualité autour du paquet ainsi que d'autres précisions [exposition à la *Helmhaus*, Zurich, 2014].

Les artistes me semblent en même temps parler de ce qu'est la neutralité du Net : une non-ouverture des paquets – *packets* de données découpées pour fluidifier leur transfert – sur Internet (permettant aux fournisseurs d'accès de, par exemple, faire payer un forfait différent entre un type de contenu et un autre) ce qui serait potentiellement discriminant (non neutre). Les artistes réussissent avec le *Random Darknet Shopper* à mettre en valeur des objets issus de réseaux clandestins et à réaliser une proposition artistique autonome, évolutive dans un marché où, effectivement, la seule limite d'accès reste celle du capital (ici en bitcoins).

Je trouve donc que ces deux œuvres, même si elles ne traitent pas toutes deux directement du réseau, elles parlent des intermédiaires, du moment où un élément est contrôlé (le colis pour Assange à l'entrée de l'ambassade et dans les entrepôts de la poste britannique), le *Random Darknet Shopper* par la police (ayant eu vent de l'exposition). Tous ces moments en dehors, à la sortie ou à l'entrée, d'un réseau ou dispositif permettant le secret. Le procédé transparent des deux artistes, communiquant sur l'activité de leur bot sur des réseaux sociaux, a aussi pour but de promouvoir les performances de leur *bot* auprès d'un large public. Ils ne sont pas dans une totale opacité paranoïaque visant à ne pas être arrêtés, à s'assurer que leurs paquets ne soient pas interceptés. Ils sont dans ce même geste contradictoire dont il était question plus avant au sujet de l'œuvre de Dominic Gagnon (*Rip in Pieces America*) : le désir de se montrer et de se cacher. Et, comme ils l'affirment, ils souhaitent, dans leur discours du moins (cela peut avoir valeur de justification de la dangerosité de leurs actes), proposer une œuvre offrant un support pédagogique pour questionner la responsabilité des algorithmes et ou *bots*.

Nous retrouvons également, bien entendu, des similarités avec le passeport de Satoshi Nakamoto présenté plus avant. Une inclusion de produits normalement inaccessibles, inimaginables (en dehors de milieux dédiés à la fête, aux *free-party*, à une certaine culture), qui sont vendus sur les marchés noirs en réseau. Le *Random Darknet Shopper* rapportera par exemple dans ses filets une fausse canette de soda, un jeu de clés pour ouvrir des bouches d'incendie, un passeport, une carte Visa Premium, une paire de chaussures Nike, etc[122]. Mais pas un objet créé et produit pour faire œuvre comme le font Émilie Brout et Maxime Marion.

122. Marie Lechner, « Connecter le darknet au champ artistique », interview de !Mediengruppe Bitnik, Libération, 2014.

Paquet et son contenu ouvert (dissimulé dans une pochette de DVD), mis dans une pochette sous vide contenant de la drogue de synthèse.

Le *bot* du !Mediengruppe Bitnik est un assistant qui reproduit un comportement compulsif d'achat et l'exposition des objets, de leurs paquets et fait penser à la pratique d'*unboxing* sur Internet consistant à ouvrir des paquets et à commenter le produit dans un rapport consumériste par sa découverte (activité partagée en vidéo à une communauté). Ce qui est intéressant en discutant avec des consommateurs habitués des plateformes de vente sur le darknet, c'est bien de comprendre ce que ces marchés leur offrent de confort une fois la technique intégrée (celle de l'achat de bitcoins, de leur transfert sur leur compte bancaire civil puis de leur mixage facultatif avant l'envoi sur le compte de la plateforme qui, elle, effectue le plus souvent le dernier versement entre le portefeuille du vendeur et celui de l'acheteur).

Un confort dans l'évaluation d'un produit, celui d'être livré directement à domicile, sans avoir besoin de rencontrer un dealer. Ils ont tous un vocabulaire spécialisé, celui des outils du darknet et celui lié à leurs achats. Un vrai folklore pour moi qui n'ai pas ce genre de consommation. Il me semble que, comme le fait remarquer Antoinette Rouvroy, c'est le droit de regard qui me manque à l'endroit du bot mis en place par les artistes. Une possibilité d'en saisir par la rétro-ingénierie comment il prend des décisions, d'y opérer une autopsie (plus aboutie que celle proposée sur le micro-ordinateur qui statue des avancés d'une commande). Pour autant, il faut rendre compte de l'aspect politisant qu'une telle installation rend possible. L'exposition de certaines pratiques sur un darknet fait exister un réel, sinon invisible. Cela permet d'avoir un support d'objectivation comme point de départ d'une démystification.

Conclusion

En prenant comme point de départ la représentation d'Internet comme un tout uni, un iceberg, nous avons voulu nous confronter à ce qu'elle rend implicite. Déconstruire cet imaginaire nous semble primordial pour en démystifier le propos, pour rendre explicite une diversité d'acteurs opérant une surveillance, une modération, une indexation, d'Internet : exprimer en quoi ils sont agissants. Comprendre leur intérêt rend possible une nuance au sujet de ce qui est obscur et transparent. Exprimer le problème d'une dichotomie entre *light* web/*deep web* et darknet est fondamental. Élargir mon sujet autour des pratiques sur le darknet et des propositions artistiques qui en découlent, à celui du *deep web* m'a de ce fait semblé pertinent.

En outre, ces outils que j'ai découverts ont accompagné une pratique artistique personnelle. Me confronter à leur réalité technique m'a permis d'inventer d'autres formes plastiques. En partant d'un imaginaire historique des réseaux du temps d'Arpanet, j'ai orienté ma recherche sur une certaine perception des darknets comme altérités au sein d'un réseau. À partir de là, j'ai voulu comprendre ce que ces imaginaires ténus dans nos sociétés occidentales signifient. Qu'est-ce qu'une perte d'en-dehors, et donc de vie privée ? Comment construire des espaces échappant à une surveillance automatisée des réseaux et des contenus ? Cette nécessité de se mettre en retrait d'une attention omniprésente, extérieure au milieu et discontinue, est à l'origine de l'invention de réseaux résilients et autonomes.

Nous avons voulu développer ici un regard sur cette porosité entre transparence et opacité afin de situer des pratiques artistiques traitant, d'un côté, de modération de contenu (web surfacique, web profond) et, de l'autre, des réseaux alternatifs ou occultes. Cette séparation entre apparition des contenus indexés puis filtrés et leur transport par les réseaux permet de saisir des nuances importantes autour des acteurs qui surveillent Internet. Les propositions artistiques

mises ici en situation ne peuvent partiellement rendre compte du milieu qu'elles explorent et donnent à voir. En donnant forme à des modérations et/ou à des réseaux occultés, ces œuvres incluent le spectateur, lui offrent un point de départ pour comprendre par lui-même les mécanismes qu'ils dissimulent plus ou moins.

Il nous a ici aussi semblé important de ne pas uniquement privilégier des œuvres appartenant au champ artistique. Les darknets, et plus généralement l'organisation d'Internet, formulent des imaginaires parfois contradictoires qu'il faut aussi inclure dans une recherche artistique afin de ne pas omettre leur pouvoir envoûtant, mystifiant. Une culture populaire qui imagine les darknets révèle ce que ces réseaux sont aujourd'hui dans l'élaboration de nouvelles technologies. Ces œuvres vidéoludiques, produites pour le divertissement, renseignent sur une certaine inclusion de ces réseaux hors norme et de leur appréhension dans l'imaginaire collectif qui passe souvent par la fiction. Des constructions mythologiques non neutres qui composent chacune des discours favorables ou non à des contre-pouvoirs et cultures en germe sur ces réseaux. Leur réelle innovation est de séparer le moment de l'apparition publique d'un individu et son intégration au sein d'institutions politiques. Cette radicalité qui crée du privé peut ainsi apparaître comme terrifiante car elle crée un fort pouvoir d'autonomie qui échappe au contrôle, à la censure, à la surveillance de masse.

Ainsi, nous avons voulu ici montrer en quoi les contre-pouvoirs concrétisent des utopies libérales et libertaires autour des darknets. En réalisant certaines utopies numériques et en créant un imaginaire de « décentralité », avec notamment les blockchains (privées ou publiques), les darknets se font le lieu de l'élaborations d'une nouvelle société. Ils renouent avec un certain idéal d'Internet une fois sorti de son laboratoire, rendu public : celui d'une autonomie face aux pouvoirs centralisés. Les darknets semblent ainsi cristalliser des espoirs et méfiances du fait des libertés qu'ils augurent. Aussi, ce sujet est-il fortement clivant. En posant la question de la limite des libertés individuelles, il impose une réflexion éthique, il met entre deux. Les réseaux financiers occultes, tels les paradis fiscaux qui partagent avec les darknets une capacité d'en-dehors social par la mise en place de dispositifs d'obfuscation, sont de ce point de vue exemplaires. Ils montrent que les moyens techniques sont ambivalents, ni bons ni mauvais.

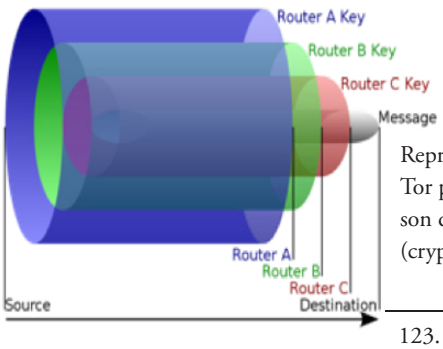
En s'infiltrant dans les réseaux, les artistes rendent publics des milieux qui, sinon, seraient exclus du politique. Ils participent ainsi à l'inclusion de champs culturels sinon invisibles mais du moins agissants. Tout le jeu narratif qu'ils produisent avec leur public oscille ainsi entre le désir de montrer, de dévoiler par le discours formel et celui de laisser libre cours à une interprétation extérieure. En cela, presque esthétiquement, ils partagent avec la surveillance un double jeu : celui d'être présents sans se montrer. Le médium est ainsi, ce tiers, cet homme du milieu, qui crée une incertitude, une rencontre par l'absence entre l'artiste et le regardeur.

Annexes

Tor et autres darknets : précisions techniques

Un darknet est aujourd'hui considéré comme un réseau *overlay* à Internet, c'est-à-dire qu'il utilise son infrastructure réseau tout en mettant en place ses propres protocoles entre ordinateurs qui s'y connectent. Des logiciels sont ainsi requis pour se connecter à chacun des darknets, tous spécifiques, pour communiquer avec les ordinateurs qui en font partie, qui peuplent ce réseau. La particularité de ces réseaux est leur autonomie vis-à-vis d'une certaine organisation d'Internet, d'une institution des échanges en réseau. Ils proposent des modalités d'échange entre ordinateurs de façon autonome au regard d'une gouvernementalité centralisée : ils utilisent leurs propres moyens de registre de sites DNS et leurs P2P/F2F *peer-to-peer*/*friend-to-friend*[123] et des protocoles plus ou moins sécurisés dont le brouillage d'identité numérique (adresses IP). Sur Tor – darknet le plus démocratisé –, ce brouillage permettant l'anonymat numérique en ligne est réalisé par un cryptage, plus précisément, par un cryptage de bout en bout.

Un usager peut se connecter en utilisant les spécificités du protocole Tor via un navigateur web amélioré, basé sur Firefox : Tor Browser. Tor peut être utilisé pour d'autres applications que le web. Quand il envoie une requête – par exemple, pour afficher une page web –, des « relais » (des nœuds intermédiaires) font transiter cette demande successivement entre eux (trois fois au moins) à travers le réseau mondial. Des serveurs (principalement) allouent une partie de leur bande passante (débit de connexion) pour garantir cette tâche et garantir une meilleure fluidité sur le réseau. La requête envoyée par l'utilisateur, en passant d'un relai à l'autre change successivement d'adresse IP (utilise celle du relai précédent). Pour que la connexion ainsi routée ne puisse pas être tracée, pour qu'une enquête ne permette pas de remonter à la source (à l'utilisateur, à son adresse IP), chaque relais « oublie » d'où elle vient, celle du précédent.



Représentation schématique de l'« oignon » mis en place par Tor pour encapsuler le message transmis entre la source et son destinataire par trois couches successives de cryptage (cryptage asymétrique par clés publiques et privées « *key* »).

123. Un type d'échange qui permet de choisir par qui une connexion passe auprès d'amis sûrs afin d'éviter un espionnage extérieur. Le réseau I2P utilise cette fonction : les darknets ne sont pas tous F2F (*friend-to-friend*).

Au lancement de la requête, l'adresse IP est encapsulée dans plusieurs couches de cryptage qui sont utilisées – relais après relais – pour garder en mémoire la requête sans pour autant connaître qui l'a formulée. Une fois la requête arrivée sur le serveur (destination), le contenu auquel elle se réfère est envoyé en retour à l'ordinateur qui l'a formulée (origine) en chemin inverse. Ainsi, les relais permettent à des milliers d'usagers de partager des adresses IP, de masquer la leur dans ce proxy de proxy.

La connexion est donc sécurisée par cryptage, et l'anonymat du titulaire est conservé. Cette topologie au sein d'un maillage d'utilisateurs permet la mise en place d'un vaste proxy d'agents dont le nombre est nécessaire pour qu'ils ne soient pas traçables[124]. S'il n'y avait que trois utilisateurs, alors il serait bien facile de les repérer. Le Naval Research Laboratory (Navy) américain ainsi que Darpa sont à l'origine du projet Tor dans les années 1990[125], alors réservé aux services secrets. Un peu comme au début d'Internet, ce proxy de proxy alors naissant ne connaît pas l'affluence du réseau Internet, du P2P ou d'autres. Ils décideront par la suite de partager le code source afin de voir affluer une mixité d'utilisateurs extérieurs et de créer ainsi un bruit informationnel (*obfuscation*) par le nombre plus élevé d'identités pouvant être interchangées. Ils rendent ainsi plus difficile l'identification et donc l'observation d'un utilisateur pris pour cible sur Tor, sa connexion.

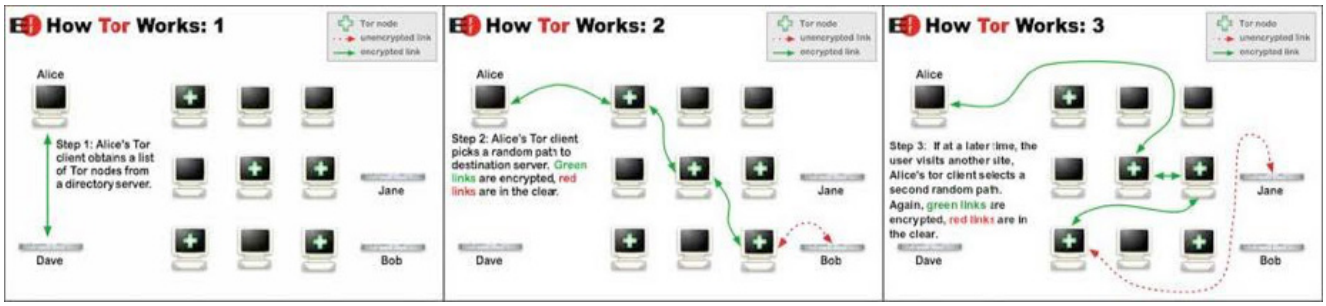


Schéma spatialisant le fonctionnement de connexion et de cryptage mis en place par Tor, de l'entrée d'une connexion sur le réseau à sa sortie vers le contenu (puis le l'acheminement, à rebour, des ressources réclamées par l'utilisateur).
Ce document est réalisé par l'EFF sur le site officiel de Tor.

124. « *The variety of people who use Tor is actually part of what makes it so secure. Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is the more your anonymity will be protected.* », The Tor Projec, URL : https://www.torproject.org/about/overview.html.en .
125. Yasha Levine, « *The technology was funded by the Office of Naval Research and Darpa.* », Pando, 2014, «*Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government*».
URL : http://pando.com/2014/07/16/tor-spooks/ . Cet article traite de l'implication américaine et d'autres perspectives relatives à Tor.

> « On appelle “bruit” un comportement qui échapperait au contrôle tout en restant indifférent au système, ce qui par conséquent ne peut traiter une machine binaire réduite à un 0 ou à un 1. Ces bruits, ce sont les lignes de fuite, les errances des désirs qui ne sont pas encore entrés dans le circuit de valorisation, le non-inscrit. […] Surproduction de mauvais feed-back qui distord ce qu'il devrait signaler, qui amplifie ce qu'il devrait contenir, ces situations indiquent la voie d'une pure puissance réverbérée.
> **Tiqqun (Le parti imaginaire), *Tout a failli, vive le communisme!*** [126]

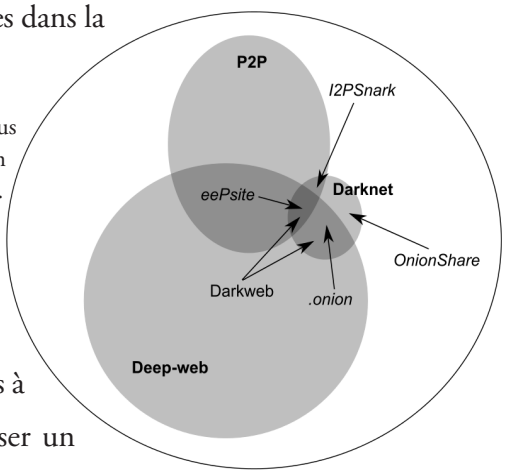
L'abréviation Tor tire donc son nom *The Onion Routeur* de ce qui symbolise son fonctionnement. Ce dispositif route une connexion, il la fait transiter entre des nœuds/relais qui, l'un après l'autre, ne gardent en mémoire que l'identité précédente fictive ; couche par couche, ils oublient l'origine du signal, son historique précédent : ils défont les peaux successives d'un oignon qui “entoure” la réelle identité au centre. Ce réseau est amnésique grâce au cryptage du point d'entrée à la sortie du réseau.

> « Le projet coûte 2 [millions de dollars] annuellement pour son développement et pour payer les nombreux serveurs. En 2012 :
>
> - 60 % proviennent du gouvernement américain (soutien à la liberté d'expression et à la recherche scientifique) ;
>
> - 18 % proviennent de fondations et autres donateurs (John S. and James L. Knight Foundation, SRI International, Google, Swedish International Development Cooperation Agency) ;
>
> - 18 % proviennent de la valorisation des contributions des bénévoles. »[127]

La EFF (Electronic Frontier Foundation) soutient avec d'autres organisations la maintenance de Tor et la transparence de son fonctionnement pour éviter, par cette surveillance, une éventuelle fraude des principes de sécurité de ce logiciel et pour augmenter sa fiabilité. Structurellement, la décentralisation des ressources et des sites sur plusieurs serveurs/clients induit un autre type de partage. L'infrastructure Tor permet ainsi de rendre, a priori, les contenus délocalisés, éparpillés, et donc difficilement saisissables.

126. Tiqqun (organe de liaison au sein du Parti Imaginaire), *Tout a failli, vive le communisme!*, essai, éd. La Fabrique, 2009, p. 309 (partie IV, « L'hypothèse cybernétique »).
127. Geoffrey A. Fowler, « *Tor : An Anonymous, and Controversial, Way to Web-Surf* », 2012.
URL : http://online.wsj.com/article/SB10001424127887324677204578185382377144280.html.
◊ The Tor Project, « *TorProject 2012 Annual Report* », 2013.
URL : https://www.torproject.org/about/findoc/2012- TorProject-Annual-Report.pdf.

Il en va de même pour les sites cachés sur Tor ou d'autres réseaux obscurcissant l'identité numérique des serveurs (et donc de leur propriétaire). Tor utilise des points de « rendez-vous » qui permettent, sur la base du même système d'anonymisation d'un client (usager), de rendre inaccessible l'identité d'un serveur hébergeant ainsi des sites cachés : des *hidden services* (« services cachés »), des sites .onion ; sur I2P, un autre darknet, des eepsites ; sur Freenet, des contenus délocalisés distribués entre utilisateurs (F2F). Chacun de ces dispositifs techniques utilise des systèmes décentralisés de la gouvernance d'Internet (*SusiDNS* pour I2P, *OnioNs*[128] pour Tor, etc). Nous ne mentionnons pas ici ZeroNet ni IPFS[129] qui fonctionnent sur une base de blockchain en P2P permettant la vérification des transactions entre usager et surtout de s'autonomiser d'institutions tierces dans la gestion de des transactions entre ordinateurs connectés.



Intrications entre le darknet et P2P contenus partiellement dans le *deep web* au sein d'Internet (cercle)[130].

Outils d'audit

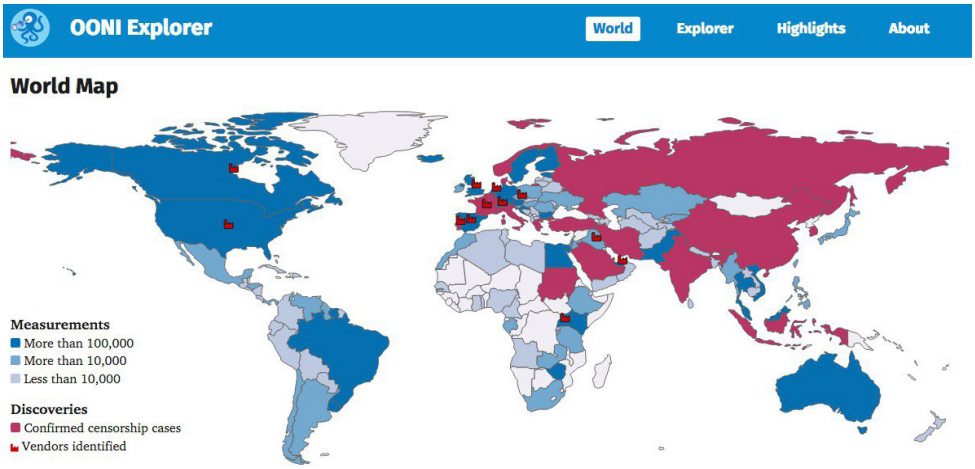
OONI (Open Observatory of Network Interference), mis en place par la Fondation Tor), permet à tout utilisateur de partager une partie de sa connexion publique (avec son IP en clair) pour vérifier si son accès à Internet équivaut aux autres utilisateurs dans le monde et ainsi réaliser un audit sur la censure des réseaux. Une carte du monde est générée pour visualiser quels types de censures sont opérées à travers le monde au regard des données récoltées collectivement et des rapports géopolitiques peuvent ainsi être publiés grâce à cet outil d'*open data* (par exemple en Malaisie[131]).

128. Jesse Victors, « The Onion Name System: Tor-Powered Distributed DNS for Tor Hidden Services », Utah State University, 2015, p. 15. L'auteur travaille sur le DNS des « services cachés » sur Tor (sites cachés). Il évoque des défis à relever et introduit le triangle de Zooko qui consiste en trois principes pour la réalisation d'un adresesages de sites (URL). Lien vers le document : http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=5517&context=etd#page=25 (page 25 au sujet du Triangle de Zooko).
◊ Voir aussi cet article très complet explique les innovations prévues au sujet des adressages en .onion pour améliorer leur sécurité, leur lisibilité, etc. : ASN (pseudonyme, responsable du développement de Tor), « Cooking with Onions : Names for your Onions », 2017. URL : https://blog.torproject.org/blog/cooking-onions-names-your-onions/ .

129. Wikipédia : « InterPlanetary File System (ou IPFS, système de fichier interplanétaire) utilise IPNS comme système de distribution d'adressage de sites (DNS).» http://fr.wikipedia.org/w/index.php?title=InterPlanetary_File_System&oldid=140151960 .

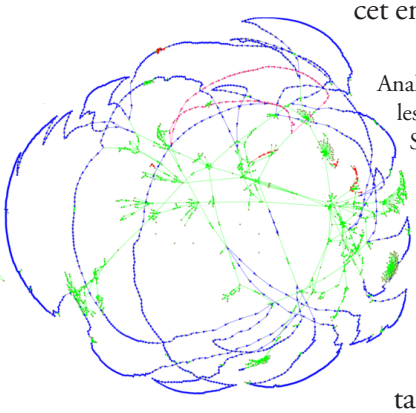
130. Jean-Philippe Renard, Darknet : mythes et réalités, éd. Actu'Web, 2016.
URL : http://www.rennard.org/Darknet/presentation.html . Conférence : «Le darknet », Sciences et Techniques au Carré, 2016, URL : https://www.youtube.com/watch?v=V8cnzyJ7S4s .

131. Rapport à cette URL :
https://github.com/TheTorProject/ooni-web/blob/master/content/post/malaysia-report.md .



Carte interactive formalisant sur le terroire mondiale le type et la quantité de censures relevées par les données traîtées par OONI. En rouge les régions qui enregistrent le plus grand nombre de censures avérées[132].

L'outil Onionscan, mis en place par la chercheuse Sarah Jamie, offre quant à lui, un moyen de réaliser des audits sur les services cachés sur Tor avec un support visuel, ce qui permet d'analyser des mouvements signifiants au sein du réseau. Par exemple, elle évalue par comparaison (d'un avant et d'un après) l'impact de la fermeture du service d'hébergement de services cachés FreedomHost II sur cet environnement et d'en déduire qu'il représentait 15 à 20% des sites cachés[133].

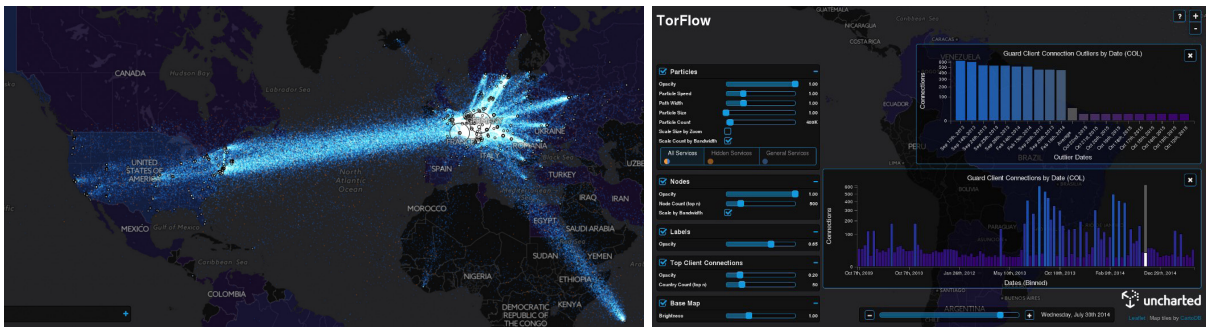


Analyse par Onionscan des liens au sein du réseau cartographiant les logiciels d'accès utilisés grâce aux informations qui laissent fuiter. SSH en bleu et FTP en rose transportent des fichiers, Apache en rouge permet leur gestion et affichage, SMTP utilisé pour des emails, etc.

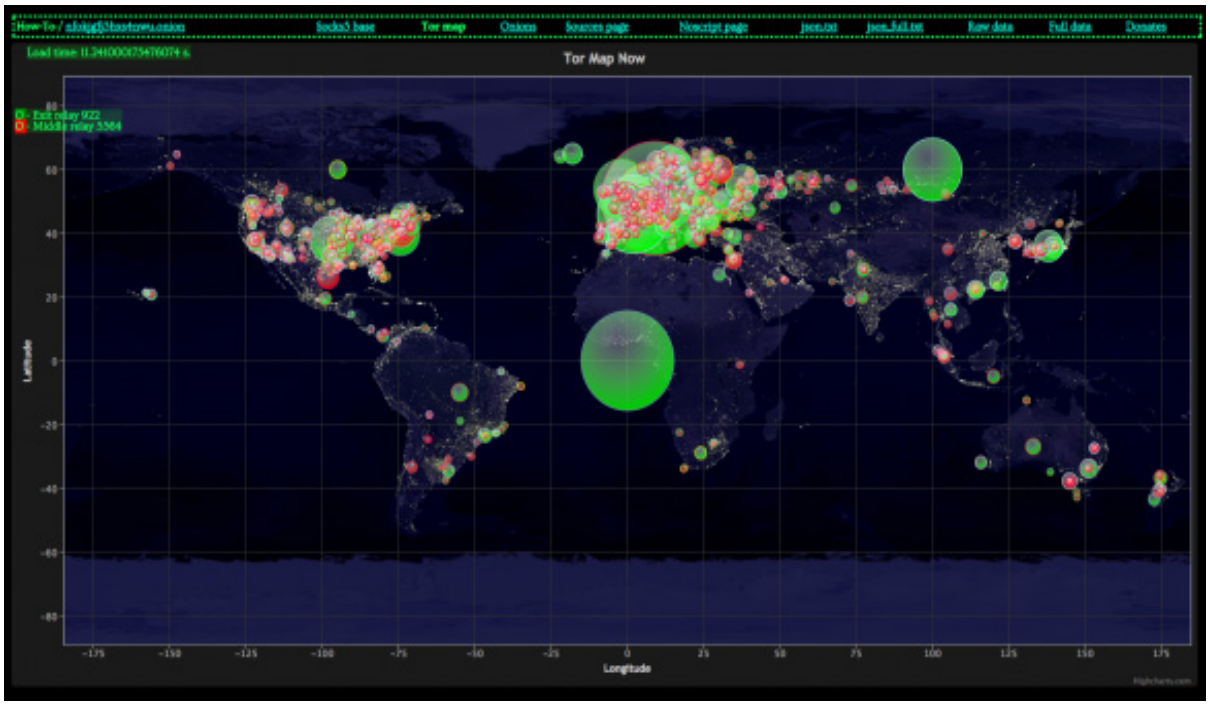
Ces outils documentaires permettent d'évaluer l'état du réseau et de générer une imagerie scientifique, analytique. Cette prétendue neutralité est bien entendue construite. La mise en image de ces données explicite une certaine logique qui aide à la déduction, à la compréhension en tant que supports d'une pensée. Ils permettent une objectivation, la création d'une distance à l'objet d'étude. Bien qu'impartiaux, ils ouvrent les données (*open data*), les rendent lisibles, informent le réel, formulent des problématiques et créent des hypothèses contestables dans des pratiques d'investigation, de vérification factuelle. Ils ont un propos d'infirmation là où les pseudo-sciences affirment sans recherche d'enquête le plus souvent sur la base de l'intuition dans la création de liens fortuits.

132. The Tor Project, OONI (projet amorcé en 2012), URL : https://explorer.ooni.torproject.org.
133. Sarah Jamie, « OnionScan Report: Freedom Hosting II, A New Map and a New Direction », Mascherari Press, 2007. URL : https://mascherari.press/onionscan-report-fhii-a-new-map-and-the-future/.

À noter que le projet Tor met à disposition des statistiques très précises quant aux usages sur le réseau[134] ce qui ne révèle en rien les identités des ordinateurs connectés. Elles permettent de corréler des activités sur le réseau (population) avec, par exemple, une censure dans un pays, d'en déduire une pratique pour la contourner.



TorFlow (*clear web*) permet de voir le nombre d'usagers du réseau Tor dans le monde en direct et dans le passé[135].
[À gauche] Carte du monde (quantité de données échangées entre les pays *via* Tor).
[À droite] Détail des données collectées au sujet la Colombie, en 2013.



Yet another Tor Directory, représentation des relais de sorties/entrées sur le réseau Tor, mai 2015 (site non accessible : http://www.bdpuqvsqmphctrcs.onion/tormap2.html)[136].
Ce site caché proposait également un index ou plutôt un annuaire de sites .onion (services cachés accessibles *via* Tor).

134. Information sur les serveurs, la quantité de connexions, les services cachés, etc. URL : https://metrics.torproject.org.

135. URL du projet TorFlow (interface rendu par le logiciel Unsharted) : https://torflow.uncharted.software. Logiciel mis en place par Mike Perry, travaillant sur Tor et d'autres projets de l'EFF. Document au sujet du fonctionnement de TorFlow : http://fscked.org/talks/TorFlow-HotPETS-final.pdf.
◊ Les Anonymous, dans un comuniqué concertant leur opération contre les contenus pédophiles (CP) « OpDarknet » de 2013, font polémique à son sujet quant au projet Tor et sa discrétion sur le *clearnet*. Ils insinue une corélation douteuse.
URL : https://pastebin.com/qWHDWCre/ .

136. J'ai réalisé une copie partielle du site à partir de différentes sauvegardes, proxys, mirrors, etc.
URL : http://44llcbgyt22pwvyq.onion/bdpuqvsqmphctrcs/ .

Scrapper : aide à l'archivage

En 2015, je commence à automatiser certaines de mes tâches sur le darknet. Je mets en place un premier *bot* qui explore le *clear web* (un logiciel qui va de lien en lien en essayant de sortir des sites où il se trouve et non pas de le parcourir en profondeur) puis un second bot qui m'assiste aujourd'hui dans l'exploration du darknet.

Ce *scrapper* – logiciel automatisé qui enregistre l'aspect visuel des sites qu'il visite – se promène de lien en lien sur le darknet et fait apparaître les pages visitées. La version en cours de cette automatisation fait fonctionner trois *bots*. Pensé comme une installation, chaque bot possède à l'écran son propre terminal (interface de suivi de l'exécution des commandes). Cela permet de rendre visibles les actions en cours de chacun d'entre eux se connectant par Tor à des annuaires de sites .onion (accessibles uniquement via Tor, appelés « services cachés »). La plupart de ces annuaires mettent en place une vérification des liens (dont Fresh Onions qui permet aussi d'afficher les liens sûrs).

Capture d'écran du site caché Fresh Onions http://zlal32teyptf4tvi.onion (2017).

Ces listes sont très courantes sur le darknet (la partie web du réseau) ; elles permettent de centraliser des liens populaires dans un environnement où les moteurs de recherche n'ont pas toujours été perfectionnés. Il en existe de nombreux dont Grams qui ressemble à Google en le copiant graphiquement ainsi que certains de ses services mais qui est spécialisé dans la recherche de drogues. Pour autant, les Hidden Wiki ou les annuaires qui ressemblent à un « pré-Google » sont nombreux (à une classification encyclopédique par

thématiques). J'ai tenté le plus possible de limiter l'exploration à des liens encore accessibles (ce qui demande à ces bots de faire des requêtes). Sur ce point, cet outil met en avant la faible durée de vie de ces sites vis-à-vis de ceux sur le *clear web* (à relativiser au regard des données[137]).

Détail sur l'un des terminaux consultant ici l'annuaire très connu Fresh Onions, depuis Taipei.

En cas de problème de connexion, les bots changent d'identité numérique et font apparaître à l'écran l'origine géographique du point de sortie sur le réseau (son adresse IP). Ces points de sortie permettent à Tor de récupérer les données des sites (cachés ou non) sans pour autant que la localisation des serveurs qui hébergent ces pages web ne soit identifiable. Sont donc affichés, à chaque changement d'identité numérique, d'adresse IP, le drapeau correspondant au pays d'origine de l'adresse adresse IP de la connexion publique (sortie du Tor) et, si disponible, le nom de la compagnie/de l'institution qui met à disposition une partie de sa bande passante à la sortie du réseau (pour récupérer les données). Avec ce procédé assez rudimentaire, j'ai voulu faire apparaître, de façon aléatoire, des pages du darknet Tor. Le but est de produire un processus discontinu mais aussi de me confronter aux outils pour les comprendre, me permettre de m'encapaciter.

Cette installation confronte à des contenus potentiellement dangereux. De fait, je ne suis pas sûr de l'exposer un jour de la sorte. Pour autant, cet outil expérimental me sert dans mon travail de recherche. Pour chaque page consultée, le *scrapper* sauvegarde (en plus de la capture visuelle du site sur laquelle figure

137. Gareth Owen, *Tor: Hidden Services and Deanonymisation*, Media Chaos Computer Club (Allemagne), 2014. URL : https://media.ccc.de/v/31c3_-_6112_-_en_-_saal_2_-_201412301715_-_tor_hidden_services_and_deanonymisation_-_dr_gareth_owen à 26m 39s. Conférence sur Tor, le nombre de services cachés, leur durée de vie, types de contenus, etc qui entend démystifier ce darknet.

son URL et son titre) la page web consultée et les fichiers qui sont nécessaires à son affichage. À mon sens, cette automatisation expérimentale reproduit ce que font les *crawlers* chargés de l'indexation du web. Tout comme le site Internet Archive (dont il était fait mention au sujet du travail d'enquête d'Émilie Brout et Maxime Marion) qui permet de sauvegarder des sites ponctuellement et de les afficher en l'état même quand ces derniers ne sont plus accessibles, je crée des doublons numériques. Cela me permet d'avoir une archive dans un milieu encore plus précaire que le *clear web* en matière de pérennité des données (et plus encore des sites cachés sur les darknets).

Indexer le darknet n'est pas impossible. Les darknets sont utilisés par des internautes du civil ou du privé inquiets pour la sécurité du transfert de leurs informations sur Internet, conscients d'une surveillance généralisée. Explorer les darknets permet d'y surveiller les activités criminelles ou encore d'augmenter la capacité de créer de l'information stratégique ou capitale de poursuivre le projet de tout rendre visible. En explorer le contenu permet de révéler une réalité sociale sur des activités invisibles depuis le *clear web*, et peut servir de base dans un travail artistique ou de documentation. La question à l'endroit d'une pratique artistique est de savoir comment ne pas essentialiser la technique mais s'intéresser aux pratiques qui en émergent. La technique doit rester un moyen de donner forme, il faut ainsi aux artistes penser à des narrations, à des mises en contexte qui accompagnent le spectateur dans une découverte de sens.

Captures accessibles à cette adresse : http://scrapper.vincent-bonnefille.fr .

Sur-contre/sous-veillance/fiction

[Page suivante] Support collectif de recherche et d'agrégation de ressources durant le mois sur la thématique « Surveillance » qui a abondamment augmenté mon corpus à ce sujet et dont le travail éditorial a permis d'organiser de façon exploratoire, par cette mise à plat, nos recherches à ce sujet.

Accessible en ligne : http://kabane.org/thema/surveillance/#clean.

Pensé comme une carte sur cette thématique en plusieurs parties :
0) Edito ; **1**) Ressources sur la reconnaissance faciale ; **2**) De la société de contrôle à la gouvernementalité ; **3**) Surveiller la surveillance : surveillance ;
4) La sous-veillance de soi ; **4'**) Ressources ; **5**) Contre-fiction ;
6) Hack & CyberWar - Néo-luddites VS Anonymous (Darknets).

Une sauvegarde interactive est disponible à cette adresse :
https://webrecorder.io/vb078/darknet/20170422150125/http://kabane.org/thema/surveillance (Webrecorder est un outil d'archivage web mis en place par Ryzhome.org qui permet de créer des sauvegardes au format .wacc)

Nous avons [kabane.org], dans ce cadre, réalisé un montage à partir de films de science-fiction, disponible ici : https://vimeo.com/188399965.

Il est composé d'extraits de :

Blade Runner par Ridley Scott (1982, inspiré des Androïdes rêvent-ils de moutons électriques ? écrit par Philip K. Dick) ;

A Scanner Darkly par Richard Linklater (2006, adaptation du roman Substance mort de Philip K. Dick) ;

Minority Report par Steven Spielberg (2002, adaptation de la nouvelle éponyme de Philip K. Dick) ;

Pi par Darren Aronofsky (1998) ;

Alphaville par Godard (1965) ;

Cypher par Vincenzo Natali (2002) […]

Le fanzine, quant à lui, est disponible ici (rassemblant quelques textes et dessins) :
http://kabane.org/thema/surveillance/Kabane_Surveillance-fanzine_MD.pdf.


ZINE1 - KABANE
SURVEILLANCE
1) De la société de contrôle ...
3) Surveiller la surveillance : la sousveillance
4) Souveillance : un appareil de l'état "Empire****, des citoyens mis à profit
2) ... à une surveillance globale et un gouvernement algorithmique
5) Contre-fiction
6) Hack & CyberWar
Néo-luddites VS Anonymous
Julian Assange
Menace sur nos libertés
DARKNET
HOW TO DISAPPEAR
NOUS NE VOULONS NI COMMANDER NI OBEIR

Bibliographie

ASSANGE, Julian, **APPELBAUM**, Jacob, **MÜLLER-MAGUHN**, Andy, **ZIMMERMANN**, Jérémie, *Menace sur nos libertés - Comment Internet nous espionne - Comment résister* (traduction française Abel Gerschenfeld et Anatole Muchnik), Robert Laffont, Paris, 2013.

BAQUÉ, Dominique, *Pour un nouvel art politique : de l'art contemporain au documentaire*, éd. Flammarion, Paris, 2004.

BEY, Hackim, *TAZ - Zone autonome temporaire*, éd. L'Éclat, Paris, 1901.

BLANC, Sabine et **NOOR**, Ophelia, *Hackers : bâtisseurs depuis 1959*, éd. OWNI, 2012.

BRUNTON, Finn, et **NISSENBAUM**, Helen, *Obfuscation : A User's Guide for Privacy and Protest*, éd. Flammarion, Paris, 2004.

CARDON, Dominique, **GRANJON**, Fabien. *Médiactivistes*, Presses de Sciences Po, 2010.

CARON, Daniel J., *L'Homme imbibé - De l'oral au numérique : un enjeu pour l'avenir des cultures*, éd. Hermann, Paris, 2014.

COLEMAN, Gabriella, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, éd. Verso, 2014.

CRITICAL ART ENSEMBLE, La Résistance électronique et autres idées impopulaires, éd. de l'Eclat, Paris, 1997.

DELEUZE, Gilles, *Pourparlers 1972-1990*, éd. de Minuit, 1990.

BARROS (de), Manuela, *Magie et technologie*, éd. Supernova, 2015.

DESERIIS, Marco, *Improper Names : Collective Pseudonyms from The Luddites to Anonymous*, éd. Minnesota Press (The University of), 2015.

DOLAR, Mladen, *What's in a Name ?*, éd. Janez Janša, publié par Aksioma - Institute for Contemporary Art, 2014.

FEDERICI, Silvya, *Caliban et la sorcière*, éd. Entremonde et Senonevero, 2014.

FISCHER, Hervé, *La Pensée magique du net*, éd. Bourin, 2015.

FREEMAN, Jo, *Tyrannie de l'absence de structure*, éd. Iosk, Grenoble,1970.

GREENBERG, Andy, *This Machine Kills Secrets : Julian Assange, The Cypherpunks, and Their Fight to Empower Whistleblowers*, éd. Plume, 2013.

GUITON, Amaelle, *Hackeurs au cœur de la résistance numérique*, éd. Diable Vauvert, Paris, 2013.

JEZO-VANNIER, Steven, *Contre-culture(s) - Des Anonymous à Prométhée*, éd. Le Mot et Le Reste, Marseille, 2013.

LAGASNERIE (de), Geoffroy, *L'Art de la révolte : Snowden, Assange, Manning*, éd. Fayard, Paris, 2015.

LEVY, Steven, *L'Ethique des hackeurs*, éd. Globe, Paris, 2013.

LOVELUCK, Benjamin, *Réseaux, libertés et contrôle - Une généalogie politique d'Internet*, éd. Armand Colin, Paris, 2015.

LUDLOW, Peter, *Crypto Anarchy Cyberstates and Pirate Utopias*, éd. MIT Press, 2001.

PAQUOT, Thierry, *L'Espace public*, éd. La Découverte, 2009.

QUESSADA, Dominique, *L'inséparé - Essai sur le monde sans Autre*, éd. PUF, février 2013.

RAYMOND, Eric, *The Cathedral & the Bazaar*, O'Reilly, 2001.

RAMONET, Ignacio, *L'Empire de la surveillance* (suivi de deux entretiens avec Julian Assange et Noam Chomsky), éd. Galilée, 2015.

RAZAC, Olivier, *Avec Foucault, après Foucault - Disséquer la société de contrôle*, éd. L'Harmattan, 2008.

SADIN, Éric, *La Société de l'anticipation - Le Web précognitif ou la rupture anthropologique*, éd. Inculte, Paris, 2011.

TIQQUN (Comité invisible), *Tout a failli, vive le communisme !*, éd. La Fabrique, 2009.

TURNER, Fred, *Aux sources de l'utopie numérique - De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, éd. C&F éditions, Caen, 2012.

VALLÉE, Jacques, Au cœur d'Internet - Un pionnier français du réseau examine son histoire et s'interroge sur l'avenir, éd. Balland, 2004.

VERCAUTEREN, David, Micropolitiques des groupes pour une écologie des pratiques collectives, éd. Les Prairies ordinaires, Paris, 2011.

VIAL, Stéphane (préface de Pierre Lévy), L'Etre et l'écran - Comment le numérique change la perception, éd. Presses universitaires de France, Paris, 2013.

WAJCMAN, Gérard, L'Œil absolu, éd. Denoël, Paris, 2010.

Conférences

BARTLETT, Jamie, « The Dark Net : what happens under the conditions of anonymity ? » Oxford University Scientific Society, 2014.
URL : https://www.youtube.com/watch?v=vSfAhfWW0I0 .

BROUT Émilie et **MARION**, Maxime, conférence durant l'exposition *The Black Chamber* (Session 2: Voluntary prisoners of the cloud), Kino Šiška, Ljubljana, 2016, URL : https://vimeo.com/160609444 .

OWEN, Gareth, *Tor: Hidden Services and Deanonymisation*, Chaos Computer Club (Allemagne), 2014, URL : https://media.ccc.de/v/31c3_-_6112_-_en_-_saal_2_-_201412301715_-_tor_hidden_services_and_deanonymisation_-_dr_gareth_owen/ .

RENARD, Jean-Philippe, «Le darknet », Sciences et Techniques au Carré, 2016, URL : https://www.youtube.com/watch?v=V8cnzyJ7S4s .

ROUVROY, Antoinette, « La gouvernementalité algorithmique ou l'art de ne pas changer le monde », ENS (chaire géopolitique du risque), Paris, 2016, URL : http://savoirs.ens.fr/expose.php?id=2670 .

WARBURG, Bettina, « How the blockchain will radicaly transform the economy », TED, 2016, URL : https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy/ .

WEISSKOPF, Carmen et **SMOLJO**, Domagoj, « !Mediengruppe Bitnik - Opera Calling / Delivery for Mr. Assange / Random Darknet Shopper », Aksioma, Ljubljana, 2016, URL : https://vimeo.com/157831003 .

Ressources en ligne

Archive d'articles web annotés : http://mht.vincent-bonnefille.fr .

Bibliographie élargie : http://news.vincent-bonnefille.fr/2017/01/15/biblio/ .

Conférences : http://news.vincent-bonnefille.fr/2017/01/01/conferences/ .

Site personnel dédié à mes recherches sur Tor : http://44llcbgyt22pwvyq.onion .

Glossaire

4chan : cf. chan.

Ad hoc : réseau sans fil capable de s'organiser sans infrastructure définie préalablement. En management, il s'agit d'adapter les compétences afin de les optimiser. https://fr.wikipedia.org/wiki/Réseau_ad_hoc/ .

Adresse IP (Internet Protocol) : numéro d'identification attribué à chaque appareil connecté à un réseau informatique. L'adresse IP est à la base du système d'acheminement (le routage) des messages sur Internet ; elle permet d'assurer a priori une correspondance entre un émetteur et un récepteur unique. Cette adresse étant unique, elle est identifiable. https://fr.wikipedia.org/wiki/Adresse_IP/ .

Arpanet (Advanced Research Projects Agency Network) : le premier réseau à transfert de paquets développé aux États-Unis en 1969, qui deviendra la base du transfert de données sur Internet.
http://fr.wikipedia.org/wiki/ARPANET/ .

Backdoor (porte dérobée en français) : faille dissimulée permettant un accès dans un logiciel, service en ligne ou système informatique entier et dont l'utilisateur n'a pas connaissance. Dans le meilleur des cas, il est créé dès la conception par le développeur du programme, un fournisseur de service ou un constructeur pour réaliser facilement des opérations de maintenance ou pour pouvoir couper l'accès en cas de litige avec un client. http://www.futura-sciences.com/tech/definitions/informatique-backdoor-2047/ .

Bergie web (web underground) : ce niveau, accessible sans modification de configuration de la connexion réseau, contient une grosse partie de l'internet « commun », il représente à lui seul plus de 90% du niveau précédent. On y trouve principalement des sites « illégaux », comme les forums de hacking, les résultats bloqués, etc.

Big Brother : terme utilisé pour qualifier toutes les institutions ou pratiques portant atteinte aux libertés fondamentales et à la vie privée des populations ou des individus. https://fr.wikipedia.org/wiki/Big_Brother/ .

Big data (datamasse en français) : désigne des ensembles de données tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou d'information. https://fr.wikipedia.org/wiki/Big_data/ .

Bitcoin (de l'anglais bit pour « unité d'information binaire », et coin, « pièce de monnaie ») : désigne à la fois un système de paiement à travers le réseau internet et une unité de compte utilisée par ce système de paiement. Il en existe de plusieurs types [ayant chacune ses spécificités, ses cours].
https://fr.wikipedia.org/wiki/Bitcoin/ .

BitTorrent : protocole de communication, de transfert et de partage de fichiers en pair à pair à travers un réseau informatique. Chaque client informatique ayant téléchargé l'information devient aussitôt serveur à son tour. Il fonctionne en P2P, d'utilisateur à utilisateur. https://fr.wikipedia.org/wiki/BitTorrent_(protocole)/ .

Black box (boîte noire en français) : désigne ici un type d'algorithme obscur, la partie non accessible des logiciels qui créent de l'intelligence à partir des données brutes. Cette image mystifie le calcul algorithmique et évoque sa non-transparence dans son procédé.

Blockchain (chaîne de blocs en français) : base de données distribuée transparente, sécurisée, et fonctionnant sans organe central de contrôle. Système de vérification synchronisé et distribué d'informations calculées en commun bloc par bloc (chaîne) pour vérifier l'intégrité du registre des transactions (qu'elle compose). https://fr.wikipedia.org/wiki/Chaîne_de_blocs/ .

Bot (robot en français) : agent logiciel automatique qui interagit avec des serveurs informatiques. Il permet d'effectuer rapidement des tâches répétitives. https://fr.wikipedia.org/wiki/Bot_informatique/ .

Bug (bogue en français) : en informatique, un bug est un défaut de conception d'un programme informatique à l'origine d'un dysfonctionnement. https://fr.wikipedia.org/wiki/Bug_(informatique)/ .

Chan (du japonais Yotsuba Channel) : forum discussions originellement relatives à la culture japonaise (mangas, dōjinshi…) fondé sur le partage d'images. Système organisé par sujets, non modérées et ne produisant pas d'historiques sur les utilisateurs. Ces plateformes fonctionnent sur le web, clear ou dark. Ainsi 4chan et ses variantes sont controversées : elles sont le lieu des trolls, des colportages, des mémes, etc.

Chat (messagerie instantanée ou dialogue en ligne en français) : anglicisme francisé en « tchat », signifie littéralement « bavardage » permet l'échange instantané de messages textuels et de fichiers entre plusieurs personnes par l'intermédiaire d'ordinateurs connectés au même réseau informatique, et plus communément celui d'Internet. Contrairement au courrier électronique, ce moyen de communication permet de conduire un dialogue interactif. https://fr.wikipedia.org/wiki/Messagerie_instantanée/ .

Clear web : le web « de surface » est indexé par les bots des moteurs de recherche.

Client : dans l'architecture « client/serveur », ce terme désigne la machine permettant d'utiliser les données ou les programmes disponibles sur un « serveur », c'est-à-dire l'ordinateur servant de distributeur consultable à distance. http://www.etudes-francaises.net/entretiens/21glossaire.htm .

Cloud computing (informatique en nuage, en français) : exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet. Ces serveurs sont loués à la demande, le plus souvent par tranches d'utilisation selon des critères techniques (puissance, bande passante, etc.), mais également au forfait. https://fr.wikipedia.org/wiki/Cloud_computing/ .

Code source : le code à l'origine de l'écriture d'un logiciel. Les programmeurs de logiciel peuvent donner accès au code d'un logiciel pour permettre que d'autres le modifient à leur tour. On parle alors d'open source en opposition aux logiciels propriétaires qui, eux, empêchent la réappropriation de leur code.

Crawler (appelé aussi spider ou bot) : robot d'indexation du web (poursuit la métaphore du web marin ou celle de la toile).

Crawling : mission qui consiste à visiter sans relâche et de manière automatisée les pages du web. https://www.1min30.com/dictionnaire-du-web/robot-dindexation-crawler-bot-et-spider/ .

Creepypasta : histoire étrange et souvent inquiétante diffusée sur Internet, pouvant se décliner sous plusieurs formats (image, vidéo, fichier son, texte accompagné d'images, de vidéos, de sons, etc.). Ce type d'histoire ressemble aux légendes urbaines, dont elle ne diffère que par l'utilisation de contenu multimédia. https://fr.wikipedia.org/wiki/Creepypasta/ .

Crypto-monnaie ou monnaie cryptographique est une monnaie électronique sur un réseau informatique pair à pair ou décentralisée basé sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même. Aujourd'hui, toutes les crypto-monnaies sont des monnaies alternatives, car elles n'ont de cours légal dans aucun pays. https://fr.wikipedia.org/wiki/Crypto-monnaie/.

Cyberespace : ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs. Source : Le Petit Robert, édition 2015.

Cybersquatting (cybersquattage, cybersquatteur en français) : pratique consistant à enregistrer un nom de domaine correspondant à une marque, avec l'intention de le revendre ensuite à l'ayant droit, d'altérer sa visibilité ou de profiter de sa notoriété. https://fr.wikipedia.org/wiki/Cybersquattage/.

Darknet : réseau superposé (ou réseau overlay) qui utilise des protocoles spécifiques intégrant des fonctions d'anonymisation. Cf. aussi web. https://fr.wikipedia.org/wiki/Darknet/.

Data center (centre de données, en français) : site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise. https://fr.wikipedia.org/wiki/Centre_de_données/.

DDoS (Distributed Denial of Service, ou déni de service distribué, en français) : type d'attaque très évolué qui vise à anéantir des serveurs, des sous-réseaux, faire planter ou rendre muettes des machines, en les submergeant de trafic inutile (par l'attaque simultanée d'ordinateurs coordonnés).
http://www.securiteinfo.com/attaques/hacking/ddos.shtml.

Dead drop : clé USB fixée dans l'espace public permettant un partage de données (en l'occurrence un partage de fichiers) de manière anonyme et non connectée à un réseau informatique (hors ligne). https://fr.wikipedia.org/wiki/Dead_Drop_(USB)/. [Fait aussi référence au projet en mémoire à Aaron Swartz d'un dispositif d'envoi de fichiers anonymes pour les lanceurs d'alerte.]

Deep web (aussi appelé « web profond », « web invisible » ou « web caché ») : partie de la Toile accessible en ligne [via des protocoles restreignant l'accès par défaut], mais non indexée par des moteurs de recherche classiques généralistes ; certains moteurs tels que Base prennent cependant en compte cette partie du réseau. La terminologie « web profond » est opposée à web surfacique. https://fr.wikipedia.org/wiki/Web_profond/.

Digital labor (travail numérique en français) : concept paru à la fin des années 2000, désigne la réduction des liaisons numériques à un moment de rapport de production, en considérant l'ensemble des pratiques liées au numérique produisant de la valeur, qui sont soumises à un encadrement contractuel et à des métriques de performance. https://fr.wikipedia.org/wiki/Travail_numérique/.

DNS (Domain Name System) : service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom [via une adresse URL. Les DNS sont donc des registres qui dirigent un navigateur web qui leur envoie une adresse URL pour en afficher le contenu vers le serveur qui s'y rattache. Ainsi une adresse web est redirigée vers une adresse IP, celle du serveur qui héberge les contenus. La plupart des darknets ont leur propre système de DNS qui permettent à leurs usagers d'accéder à des pages sinon inaccessibles depuis le web normal. Ces derniers sont donc décentralisés de celui communément utilisé dans la distribution de contenus sur le web]. http://fr.wikipedia.org/wiki/Serveur_DNS/.

Escrow : utilisation d'une tierce partie neutre pour veiller à ce que le paiement de la transaction soit fait à un vendeur pour l'achèvement des éléments envoyés à un acheteur. Après l'achat, les fonds sont détenus « entiercés » pour n'être libérés que lorsque l'acheteur a déclaré que le vendeur a bien respecté les conditions de l'achat. http://www.deepdotweb.com/2014/03/02/deepdotwebs-darknet-dictionary/ .

FAI (Fournisseur d'accès à Internet, Internet Service Provider en anglais) : entreprise proposant de connecter un ordinateur isolé ou un réseau de machines à Internet. http://www.dicodunet.com/definitions/internet/fai.htm .

Feed-back (ou retour d'expérience en français) : au sens large, c'est l'action en retour d'un effet sur le dispositif qui a donné naissance à cette action. Un feed-back définit donc un retour sur l'état actuel qu'il informe.

Free flow (libre circulation en français) : définit dans le projet cybernéticien une non-entrave de la circulation de l'information.

Gafam (acronyme pour Google, Amazon, Facebook, Apple, Microsoft) : firmes américaines qui dominent le marché du numérique, également nommées les Big Four, avant que la lettre « M » pour Microsoft y soit incluse. [Natu regroupe de nouvelles multinationales de l'économie de service numérique : Netflix, Airbnb, Tesla et Uber.]

Hack : le hack est une manipulation d'un système qui consiste à séparer des blocs logiques, retirer de l'étude tout ce qui n'est pas nécessaire, et regrouper des données dispersées ce qui permet de retrouver une cohérence, tout en permettant d'être mieux compris dans son fonctionnement. Le terme de hack est très employé par les internautes et les médias d'information, mais dans des significations qui tendent vers un abus de langage.Le terme le plus employé pour désigner quelqu'un utilisant cette méthode est un hacker. On peut ajouter à cette définition large le principe élémentaire de la bidouille (traduction française) qui signifie l'action de modifier, de changer l'usage d'un objet. En informatique il s'agit donc de changer l'usage normal d'un logiciel ou d'un composant électronique pour en élargir le potentiel, en modifier la conception pensée à l'origine par ses concepteurs. https://fr.wikipedia.org/wiki/Hack/ .

Hacker (fouineur ou hackeur) : personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique. Prendre ce mot au sens de pirate informatique est considéré linguistiquement comme abus de langage (surtout des médias). http://www.larousse.fr/dictionnaires/francais/hacker/38812 [Un hackeur est quelqu'un qui fait preuve d'inventivité pour contourner l'usage normé d'un objet, outil, informatique ou non, afin de créer ce qu'il souhaite sans se soucier des usages normés/attendus qui lui ont été pensés et intégrés].

Hacking (du mot hackability traduisible en français par « bidouillabilité ») : manipulation d'un système détourné de sa vocation initiale pour de nouveaux usages. http://fr.wikipedia.org/wiki/Hack/ et http://www.leblogduhacker.fr/qu-est-ce-qu-un-hacker/ .

Honeypot (« pot de miel ») : terme imagé pour parler d'un piège attractif utilisé sur certains darknets pour démasquer des usagers ciblés dans le cas d'enquêtes ou pour extirper des identifiants de connexion en usurpant une identitée visuelle d'un site (on parle plus aisément de pishing, le fait de tirer un hameçon, l'utilisation d'un leurre pour appâter un usager). Une tromperie plus facile encore sur le réseau darknet Tor du fait de la structure des adresses URL moins mnémotechniques en .onion produites pour les « sites cachés » qui peuvent induire en erreur un utilisateur.

Hotspot : point ou borne permettant la communication sans fil (wifi).
http://www.dicodunet.com/definitions/reseaux/hotspot.htm .

HTTP (Hypertext Transfer Protocol, littéralement « protocole de transfert hypertexte ») : protocole de communication client/serveur développé pour le World Wide Web.

HTTPS (Hypertext Transfer Protocol Secured) : permet le transport sécurisé des informations via le web par HTTP (sur la base de certificats). http://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol/ .

Icann (Internet Corporation for Assigned Names and Numbers, Société pour l'attribution des noms de domaine et des numéros sur Internet) : autorité de régulation de l'Internet. C'est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau (TLD), et de coordonner les acteurs techniques. [Cette organisation gère la distribution des différents éléments numériques nécessaires à la mise en relation des ordinateurs au sein d'Internet. On peut ainsi lui attribuer un rôle organisationnel et décisionnel dans la gouvernementalité.]
https://fr.wikipedia.org/wiki/Internet_Corporation_for_Assigned_Names_and_Numbers/ .

Internet des objets (IdO, ou Internet of Things IoT) : perçu comme la continuité d'Internet étendue aux objets connectés l'IdO qualifie une généralisation de la connectivité qui élargie la domotique. Considéré comme la troisième évolution de l'Internet, baptisé web 3.0 qui fait suite à l'ère du web social, l'internet des objets revêt un caractère universel pour désigner des objets connectés aux usages variés Les objets connectés peuvent envoyer et recevoir des informations depuis Internet ou d'autres réseaux. Cela demande la mise en place de structures de transfert d'information sécurisé et synchronisé. Des technologies telles qu'une blockchain peuvent aider à y parvenir en vérifiant l'état des informations échangées en vérifiant leur authenticité. https://fr.wikipedia.org/wiki/Internet_des_objets/ .

Intranet : ensemble restreint de services internet, uniquement accessibles à partir des postes d'un réseau local.
http://www.commentcamarche.net/contents/324-intranet-et-extranet/ .

IP (Internet Protocol) : cf. adresse IP.

IRL (In Real Life traduit littéralement « dans la vraie vie ») : expression couramment employée sur Internet pour désigner la vie en dehors d'Internet, par extension une irl peut être le fait de rencontrer réellement des gens rencontrés sur Internet. http://fr.wikipedia.org/wiki/Vraie_vie/ .

LAN (Local Area Network, réseau informatique local) : système de communication permettant de relier quelques centaines d'ordinateurs et de périphériques dans un rayon de quelques kilomètres. A l'inverse, le réseau étendu (WAN) peut regrouper des milliers d'ordinateurs séparés par des milliers de kilomètres.
http://www.futura-sciences.com/tech/definitions/internet-lan-600/ .

Leaks (signifie littéralement « fuites ») : une première définition, en référence avec Wikileaks, est la divulgation de documents administratifs secrets. Un « leak » (toujours dans l'imaginaire d'un web océanique) signifie une perte de données « fuitant » des serveurs ou ordinateurs de façon involontaire.

Luther Blissett : pseudonyme adopté informellement et partagé par des centaines d'artistes et d'activistes, en Europe et en Amérique du Sud au milieu des années 1990, visant à démontrer « l'imposture médiatique » par une série de canulars. Ce nom a été emprunté à un footballeur qui s'illustra par une étonnante propension à rater de superbes occasions de but. https://fr.wikipedia.org/wiki/Luther_Blissett/ .

Mainstream (signifie littéralement « courant principal ») : aujourd'hui ce mot est employé pour désigner la culture de masse. http://dictionnaire-urbain.fr/?p=167 . Désigne les gros organes de presse fournissant une information massivement populaire, grand public, suivie et acceptée par la masse.
http://www.deepdotweb.com/2014/03/02/deepdotwebs-darknet-dictionary/ .

Mainstream Media : cf. Mainstream.

Marianas web : fait référence à la fosse des Mariannes (Marianas Trench, en anglais), le point considéré comme le plus profond de la croûte terrestre ; issu de la théorie de l'existence d'un cinquième niveau du web, faisant référence à l'expérimentale informatique quantique où les opérations ne sont plus basées sur la manipulation de bits dans un état 1 ou 0, mais de qubits en même temps dans un état 1 et 0, à moins qu'il ne s'agisse, autre hypothèse, d'une informatique nourrissant le conspirationnisme, ce réseau mystérieux qui suscite tous les fantasmes y compris auprès des autorités publiques.

Mème : une idée simple propagée à travers le web. Plus globalement, ensemble de comportement, élément ou phénomène lié à une culture qui se transmet d'un individu à l'autre par imitation ou par un quelconque autre moyen non génétique. http://oxforddictionaries.com/definition/meme?q=meme .

Mesh (maillé en français) : technologie à l'origine militaire permettant de déployer un réseau de communication local sans fil (WLAN) ou virtuel (VLAN) – en circuit fermé, ou connecté au moins en un point à un réseau Internet ou GSM –, les nœuds de celui-ci sont reliés les uns aux autres de manière décentralisée et forment une « maille ». http://www.lemagit.fr/definition/Mesh-Reseau/ et http://www.atlantico.fr/rdv/minute-tech/c-est-quoi-reseau-mesh-louise-hoffmann-724835.html . [Un réseau mesh permet à tout membre qui s'y ajoute d'en augmenter la portée en le complétant.]

MSM cf. Mainstream Medias.

Noosphère : selon la pensée de Vladimir Vernadsky et Pierre Teilhard de Chardin, désigne la « sphère de la pensée humaine ». Dans la théorie originelle de Vernadsky, la noosphère est la troisième d'une succession de phases de développement de la Terre, après la géosphère (matière inanimée) et la biosphère (la vie biologique). https://fr.wikipedia.org/wiki/Noosphère/ .

Obfuscation : Stratégie de protection de la vie privée sur internet qui consiste à publier des informations fausses ou imprécises de manière à dissimuler les informations pertinentes. Technique qui consiste à rendre illisible pour un humain un programme, tout en le gardant pleinement fonctionnel.
https://fr.wiktionary.org/wiki/obfuscation/ .

Open source (code sourceg ouvert) : s'applique aux logiciels dont la licence permet sa libre redistribution, l'accès à son code source et d'en créer des travaux dérivés.
http://fr.wikipedia.org/wiki/Open_source/ .

Open data : littéralement, le fait d'ouvrir les données » de donner accès aux données. Cette appellation désigne généralement le fait de rendre accessible ses données, par exemple pour une commune, un état, une entreprise, dans un souci de transparence. Ce pendant positif des big datas entend utiliser les données à bon escient, en faveur du collectif, du commun mais crée le plus souvent une normalité dans l'accès aux données qui découlent d'une captation préalable ainsi encouragé.

Overlay : un réseau overlay ou réseau superposé est un réseau informatique bâti sur un autre réseau. Les nœuds du réseau superposé sont interconnectés par des liens logiques du réseau sous-jacent. La complexité du réseau sous-jacent n'est pas visible par le réseau superposé. https://fr.wikipedia.org/wiki/Résseau_superposé/ .

PageRank (PR) : algorithme d'analyse des liens concourant au système de classement des pages web utilisé par le moteur de recherche [par Google, système d'attribution d'un rang à une page en fonction de sa popularité mais aussi de nombre de liens et de la pertinence de son contenu] https://fr.wikipedia.org/wiki/PageRank/ .

Peer-to-peer (P2P, pair à pair) : modèle de réseau informatique proche du modèle client/serveur, c'est-à-dire utilisé de manière mutualisée, mais où chaque client est aussi un serveur. http://fr.wikipedia.org/wiki/Pair_à_pair/ . [Protocole équilibré de partage des capacités et pouvoirs entre clients et serveurs (ambivalence), désigne plus largement la simple transaction entre deux ordinateurs.]

Permalien (mot-valise formé par la contraction linguistique de « permanent » et « lien ») : type d'URL conçu pour référer un élément d'information (souvent une nouvelle ou une entrée de weblog) et pour rester inchangé de façon permanente, ou du moins, pour une certaine période de temps. [Se base sur le principe de maintenance des contenus et de leurs liaisons.] https://fr.wikipedia.org/wiki/Permalien/ .

PGP (Pretty Good Privacy, en français « assez bonne confidentialité ») : logiciels de cryptage dont le principe de base est le cadenas et sa clé. [Suite de logiciels permettant entre autres l'utilisation du cryptage et de la gestion des différentes adresses privées/publiques] https://fr.wikipedia.org/wiki/OpenPGP/ .

Phishing (hameçonnage, filoutage en français) : technique utilisée par des fraudeurs pour obtenir des renseignements personnels afin de perpétrer une usurpation d'identité.
https://fr.wikipedia.org/wiki/Hameçonnage/ .

Ping : ping est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP. La commande mesure également le temps mis pour recevoir une réponse, appelé round-trip time (temps aller-retour). https://fr.wikipedia.org/wiki/Ping_(logiciel)/ .

PirateBox : dispositif électronique souvent composé d'un routeur et d'un dispositif de stockage d'information, créant un réseau sans fil qui permet aux utilisateurs qui y sont connectés d'échanger des fichiers anonymement et de manière locale. https://fr.wikipedia.org/wiki/PirateBox/ .

Prism : programme de surveillance électronique de la NSA. « En juin 2013, le quotidien britannique The Guardian affirme, à la suite des révélations d'Edward Snowden, que la NSA dispose d'un accès direct aux données hébergées par les géants américains des nouvelles technologies, parmi lesquels Google, Facebook, YouTube, Microsoft, Yahoo!, Skype, AOL et Apple. Barack Obama le présente comme un outil de lutte antiterroriste. » http://fr.wikipedia.org/wiki/PRISM_(programme_de_surveillance/ .

Privacy by design : inspiré de la protection intégrée de la vie privée (PIVP) permettant aux technologies d'évoluer sans porter atteinte à la vie privée intégrée dans l'ergonomie de leur application numérique. http://www.journaldunet.com/solutions/expert/59334/privacy-by-design---ma-lecture-des-sept-principes-fondamentaux.shtml .

Proxy : serveur mandataire permet de se connecter à un contenu (Internet) via un ordinateur intermédiaire (sert pour se connecter avec ses configurations et donc avec ses moyens/restrictions).

Qubit : la plus petite unité de stockage d'information quantique. C'est l'analogue quantique du bit. https://fr.wikipedia.org/wiki/Qubit . [Les qubit sont utilisés par un certain type d'ordinateur surpuissant, capable de résoudre des problèmes complexes. Le principe d'état intriqué de ces éléments constituant la puissance de calcul d'un processeur (bit) leur permet d'être dans deux états simultanément (et non pas binaires comme le sont les bits soit égales à 1 ou à 0).]

Ransomware (rançongiciel ou logiciel de rançon) : logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. https://fr.wikipedia.org/wiki/Ransomware/ . [Plus largement, un logiciel de rançon peut rendre inaccessible ou faire peur pour réclamer une rançon sans pour autant crypter les données des utilisateurs attaqués.]

Ready-made (anglicisme pour objet manufacturé) : produit manufacturé du quotidien promu œuvre artistique en héritage de la pensée de Marcel Duchamp. La pratique du ready-made artistique prend en compte le contexte d'un objet, qui, désigné comme œuvre, est intégré au champ artistique comme geste de déplacement ou choix artistique.

Un ready-made opère un changement d'usage et donc de de compréhension d'un objet (numérique ou non) par son changement des modalités de sa compréhension, hors de son champ d'origine. Un décalage critique ou du moins distancié peut ainsi, dans cette mise en scène, s'opérer à son sujet (et sur le regardeur qui ainsi, dans sa nouvelle situation, le re-découvre et se re-découvre lui-même en le regardant).

Régime de vérité : axe de recherche développé par Michel Foucault dans les années 1980. Le « régime de vérité » permet d'isoler la part libre et réfléchie prise par le sujet dans son activité propre.

Snuff movie : film mettant en scène la torture, le meurtre, le suicide ou le viol d'une ou plusieurs personnes, la victime est censée ne pas être un acteur mais une personne véritablement tuée ou torturée. https://fr.wikipedia.org/wiki/Snuff_movie/ .

Spam (acronyme de spiced ham, jambon épicé, terme francophone : « pourriel », contraction de « poubelle » et de « courriel ») : à l'origine inspiré par un sketch du Monty Python's Flying Circus où le terme est répété à l'infini ; ce courrier indésirable provenant d'utilisateurs inconnus ou de robots, destinés à des fins commerciales ou malhonnêtes. Les spammeurs récupèrent les adresses électroniques par l'intermédiaire de virus, en aspirant les adresses sur les pages web ou les forums sur Internet ou encore via des bases peu sécurisées ou, plus simplement par échange de base de données de clients. Ce double usage entretenant la confusion. http://www.altospam.com/actualite/2007/03/le-spam-origine-et-definition-d'un-acronyme/ .

Stalking (traque furtive) : une forme de harcèlement névrotique, terme communément utilisé pour faire référence à une attention obsessionnelle et non désirée accordée à un individu ou à un groupe de personnes. Courrier indésirable provenant d'utilisateurs inconnus ou de robots, destinés à saturer le réseau Internet. https://fr.wikipedia.org/wiki/Traque_furtive/ . [Employé ici pour désigner une sur-attention, une veille attentive pour suivre une activité sans la perdre.]

Streaming (terme anglais, de stream, « courant », « flux », « flot ») : flux direct, flux, lecture en continu, lecture en transit ou diffusion en mode continu, désigne un principe utilisé principalement pour l'envoi de contenu en « direct » (ou en léger différé). https://fr.wikipedia.org/wiki/Streaming/ .

Swarm intelligence (intelligence en essaim) : programmes informatiques à intelligence artificielle distribuée ; « propriété de systèmes de robots non intelligents qui montrent collectivement un comportement intelligent » selon Gerardo Beni, Proceedings of the Seventh Annual Meeting of the Robotics Society of Japan, 1989 ; propos énoncés dans le contexte de systèmes artificiels qui doivent leur existence à un concept similaire de la nature. https://fr.wikipedia.org/wiki/Intelligence_distribuée/ .

TCP/IP (Transmission Control Protocol/Internet Protocol) : ensemble de protocoles permettant le transport de données sur l'internet. http://www.etudes-francaises.net/entretiens/21glossaire.htm .

The Cloud : cf. cloud computing.

TLD (Top-Level Domain, domaine de premier niveau ou un domaine de tête) : domaine correspondant au niveau le plus élevé dans la structure d'adressage de l'Internet. Il est situé à la fin de tout nom de domaine ; identifié soit par la représentation codée d'un nom de pays, telle que « .fr », soit par une abréviation telle que « .com » ou « .org ». https://domaine.blogspot.com/2009/12/2-ne-dites-plus-top-level-domain-mais.html .

[Si l'Icann distribue les TLD, il existe d'autres systèmes de DNS permettant d'accéder à des sites ayant leurs propres TLD tels .pirate, .geek, .bit, etc. Le TLD .onion est réservé et ne peut pas être enregistré comme nom de domaine en dehors de Tor. D'autres TLD sont exclusivement réservés, par exemple à l'armée américaine.]

Tor (The Onion Router, le routeur oignon en français) : l'appellation fait référence à la structure du réseau Tor, qui consiste en plusieurs couches successives de chiffrage, destinées à protéger les données. Le logiciel qui prend les données qui entrent et sortent via une connexion Internet qui les fait passer à travers un circuit de serveurs – appelés nœuds ou hub – mis à disposition par des individus volontaires (estimé à 4 000 machines réparties dans le monde entier). Ce qui permet d'anonymiser l'origine de connexions TCP. À l'épreuve de tout pistage, c'est un outil de contournement de la censure sur Internet.
http://torstatus.blutmagie.de .

Torrent (ou fichier d'extension .torrent) : désigne un type de fichier utilisé par le protocole d'échange « pair à pair » BitTorrent. Le torrent est un fichier qui pointe à l'endroit où se trouvent les parties du fichier réel sur internet. Il contient également l'adresse IP d'un tracker qui coordonne les échanges entre pairs.
http://en.wikipedia.org/wiki/Torrent_file/ .

Trading (> trader, « marchand ») : désigne spécifiquement les opérations d'achats et de ventes effectuées sur les marchés financiers (valeurs mobilières, devises et produits dérivés). Les traders sont les opérateurs salariés d'une institution financière ou boursière qui officient depuis la salle des marchés ; certains sont indépendants et le pratiquent par Internet. Le trading définit également la discipline du négoce désormais enseignée à travers des formations dispensées au sein d'écoles de commerce, incluant la gestion des risques financiers, le suivi des opérations de marché, ainsi que la prévention des délits financiers.
http://www.larousse.fr/dictionnaires/francais/trader/10910347/ .

Troll : caractérise ce qui vise à générer des polémiques. Le troll est à distinguer du flaming qui consiste en l'envoi de messages délibérément hostiles et insultants avec l'intention de créer un conflit. L'origine de ce nom, bientôt trentenaire, connaît plusieurs versions dont la plus probable, est l'usage du verbe anglo-américain trolling dans son sens figuré : chercher à provoquer des réactions.
https://fr.wikipedia.org/wiki/Troll_(Internet)#Origine_du_terme/ .

Underground : la culture underground (ou « souterraine ») est, avant l'apparition d'Internet, un complexe socioculturel de productions culturelles, artistiques à caractère expérimental, situées en marge des courants dominants et diffusées par des circuits indépendants des circuits commerciaux ordinaires.
http://fr.wikipedia.org/wiki/Culture_underground/ .

URL (Uniform Ressource Locator, littéralement « localisateur uniforme de ressource », plus couramment appelé « adresse web ») : simple ligne de texte qui permet de retrouver une ressource (texte, image, musique…). Adresse servant à désigner une ressource présente sur le web.
http://fr.wikipedia.org/wiki/Uniform_Resource_Locator/ .

VPN (Virtual Private Network, ou « réseau privé virtuel ») : permet d'aller d'un réseau privé à un autre réseau privé en traversant internet dans un tunnel sécurisé. [Dispositif permettant de changer d'adresse IP en utilisant les ressources d'un ordinateur distant (qui retransmet le résultat des requêtes demandées)]
http://fr.wikipedia.org/wiki/Réseau_privé_virtuel/ .

Wallet (« portefeuille » en français, et e-wallet pour « portefeuille électronique ») : un wallet sur le darknet désigne généralement un portefeuille numérique qui contient de la crypto-monnaie (monnaie basée sur de la cryptographie) tels des bitcoins (monnaie numérique échangée via des index de transaction sécurisés, les blockchains). Un wallet contient une adresse de réception et permet d'envoyer à d'autres wallets de la monnaie par cette adresse. Il existe différents wallets plus ou moins sécurisés dans leur conception.

Web (ellipse de World Wide Web, ou toile d'araignée mondiale en français) : symbolise les hyperliens entre les ressources du web.

Wifi : un réseau wifi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux. Le terme « wifi » suggère la contraction de « Wireless Fidelity », par analogie au terme « hifi » pour « High Fidelity ». https://fr.wikipedia.org/wiki/wifi/ .