Table des matières

Déclaration ii
Remerciements iii
Résumé iv
Table des matières v
Liste des tableaux vii
Liste des figures viii

Introduction 1
Motivation 1
Objectifs 1
Définition 1
Le Surface Web 1
L'indexation des sites Web 2
Le Deep Web 3
Le Dark Web et les Dark Nets 6
Pourquoi utiliser le Dark Net ? 7
The Onion Router et les autres accès au Dark Net 9
Retroshare 9
La cryptographie asymétrique 10
OpenSSL standard 11
Tor 11
Traçabilité 14
I2P 14
Accès et utilisation 15
Approche technique d'accès 15
Utiliser une VM 17
Approche technique d'utilisation 18
Simulation 19
Tentative sous l'OS Tails 19
Tentative sous machine virtuelle Windows 24
Légalité 25
Protection de la personnalité 25
Zone grise 26
La criminalité 26
Les agences de surveillance 27
National Security Agency 27
European Union Agency for Network and Information Security 27
Régulations actuelles 27
Le Deep Web à travers le monde 29
Comment contrôler le Deep Web 30
Techniques 30
Sanctions 32
Les cryptomarchés 33
Description 34
Silk Road 35
Autres cryptomarchés 36

Systèmes de paiements 37
Bitcoin 37
Fonctionnement 38
Wallet 39
Comment payer de manière anonyme 39
Le transport 40
L'impact du Dark Web sur notre économie 41
Les marchés 41
Les drogues 41
Les armes 43
Les médicaments 43
La pédopornographie 44
Les Hitmans 45
La falsification de document 45
Les Malwares 45
La contrefaçon et les articles « tombés du camion » 46
Le terrorisme 46
Le pouvoir de l'Open Source 47
Conclusion 48
Bibliographie 50

Liste des tableaux

Tableau 1 : informations laissées après notre passage sur internet..... 13
Tableau 2 : Comparaison du niveau de sécurité par rapport aux différents OS..... 24

Liste des figures

Figure 1 : Algorithmes créés par Google pour indexer les sites Web..... 2
Figure 2 : Représentation du Web par un iceberg..... 3
Figure 3 : Captcha identification..... 4
Figure 4 : Carte mondiale représentant les ennemis d'internet..... 8
Figure 5 : Logo Retroshare..... 9
Figure 6 : Illustration de la cryptographie asymétrique..... 10
Figure 7 : Logo de Tor The Onion Router 11
Figure 8 : Configuration de Tor..... 15
Figure 9 : Tor joint le réseau en mettant à disposition votre adresse IP..... 15
Figure 10 : Tor circuit de l'adresse IP..... 16
Figure 11 : Adresse IP disponible par le fournisseur internet..... 16
Figure 12 : Autoriser le JavaScript sur Tor..... 18
Figure 13 : Les extensions du navigateur Tor..... 18
Figure 14 : Tails OS, bureau avec le Finder et centre de contrôle..... 20
Figure 15 : Centre d'activité de l'OS Tails..... 20
Figure 16 : Moteur de recherche par défaut de Tor..... 21
Figure 17 : Recherche du site Facebook sur DuckDuckGo..... 21
Figure 18 : Les Hidden Wiki, disponibles depuis le Surface Web..... 21
Figure 19 : Dark Web proposant du Cannabis ou des produits dérivés..... 22
Figure 20 : Grams, la Search Engin spécialisée dans les drogues..... 22
Figure 21 : recherche « weed switzerland » sur Grams..... 23
Figure 22 : Analyse des cryptomarchés de la drogue par Grams..... 23
Figure 23 : Carte du monde indiquant les plus gros utilisateurs de Tor..... 30
Figure 24 : Les Hidden Wiki..... 33
Figure 25 : Déploiement d'une attaque DDoS..... 33
Figure 26 : Image d'archive de la première version de Silk Road..... 34
Figure 27 : Évolution du Bitcoin depuis sa création..... 38
Figure 28 : Illustration du Bitcoin mixer..... 39
Figure 29 : Illustration du système Escrow..... 40

Introduction

Motivation

J'ai choisi de réaliser mon travail de bachelor sur le Deeb Web, car c'est un thème d'actualité et souvent mal compris, ou mal connu, du grand public. Beaucoup de confusion entoure ce thème pouvant entraîner une crainte chez les utilisateurs sans même savoir que ces derniers utilisent peut-être le Deep Web au quotidien sans véritablement s'en rendre compte.
De plus, le Deep Web possède aussi des aspects positifs souvent négligés ou ignorés des journalistes ou des sites d'actualités qui enquêtent sur ce domaine.
Le choix de ce thème de bachelor me permet donc de mieux comprendre le côté moins connu du net et d'émettre différentes conclusions relatives à cette thématique passionnante.

Objectifs

Ce travail de recherche offre une description complète et exacte du Deep Web, explique comment s'y rendre et comment l'exploiter. J'aborde ensuite les parties plus sombres du Deep Web, plus communément appelées le Dark Web. Il est aussi important pour moi de bien comprendre comment la police et la justice luttent contre le Dark Web.
Le but de ces recherches est véritablement de faire une analyse complète de la situation dans un domaine où l'on voit circuler beaucoup d'informations incomplètes ou erronées.

Définition

Le Surface Web

Avant même de parler du Deep Web, il est important de comprendre le fonctionnement d'internet en général.
Internet est un réseau de réseaux connectés à travers le monde via des protocoles de connexions tel que TCP IP. Sur ce réseau de réseaux, nous y trouvons plusieurs applications que nous connaissons bien telles que l'envoi ou réception d'email, via le « small message transfer protocol », le transfert de fichier, qui lui utilise le « file transfer protocol » et bien évidemment le World Wild Web ou, en terme simplifié, le Web. Toutes ces applications utilisent internet comme un support ou un moyen de transport grâce à des connexions entre tous ces différents réseaux.
Les informations sont stockées de plusieurs manières, par exemple sur des serveurs comme chez Google. Les serveurs sont ensuite reliés entre eux par le principe de l'hyper-text.
Cette partie d'internet, bien connue de tous, est appelée le Surface Web. Ce sont tous les sites indexés et stockés dans les serveurs par les moteurs de recherche accessibles via des navigateurs tels que Google Chrome, Safari, etc.

L'indexation des sites Web

Afin de rendre possible le lien entre un moteur de recherche muni du texte « économie du monde » et l'apparition d'une liste de sites comme www.lemonde.fr ou www.monde-economique.ch, il est nécessaire que les pages concernées soient indexées sur des sites qui sont eux-mêmes référencés. Ceci permet de « transporter » la demande initiale sur une catégorie existante, la catégorie économique par exemple, et de voir apparaître des pages indexées à ladite catégorie.

Dans le but d'indexer un maximum de page Web et de rendre les recherches sur un navigateur plus vaste, des robots d'indexation travaillent en permanence. Google a nommé ses robots « GoogleBots ». Leurs tâches sont simples ; ces robots vont se rendre sur un site Web, ensuite ils vont indexer les pages du site en essayant de « comprendre » (classifier) le site et son contenu puis sauvegarder ces informations dans une base de données prévue à cet effet.

Tout d'abord, des robots d'exploration vont régulièrement parcourir les différents sites Web identifiables sur internet, les scanner et naviguer entre eux grâce aux liens hyper-text internes et externes afin d'agrandir leur connaissance.

Ensuite, entrent en jeu les robots d'indexation qui vont récolter les données des pages scannées par les robots d'exploitation. Les données traitées sont les URL, les titres et les mots clés qui seront également classés dans la base de données.

Pour finir, l'utilisateur tape sa recherche sur un moteur de recherche qui va ensuite localiser les informations dans la base de données en suivant un algorithme.

Il est à préciser que certains sites ne peuvent pas être indexés par les robots d'indexation, nous reviendrons d'ailleurs sur ce point ultérieurement.

Il est encore important de savoir que, pour qu'un site soit indexé et référencé, ses pages doivent respecter certaines normes comme le format, le contenu et le droit d'accès au robot d'indexation. Il est tout à fait possible qu'un site possède certaines pages qui respectent ces différentes normes, mais d'autres ne les respectent pas (pages qui ne seront donc pas indexées).

En résumé, s'il est possible d'indexer un site, il sera identifiable par un moteur de recherche, et donc se situera dans la Surface Web.

Figure 1 : Algorithmes créés par Google pour indexer les sites Web

(https://doingenia.com/blog/algorithmes-google/)

Le Deep Web

À l'inverse du Surface Web, le Deep Web représente tous les sites non indexés par les moteurs de recherche, ce qui représente 96 % des pages internet disponibles. Je tiens à préciser que ce pourcentage peut varier en fonction des études, des chercheurs et des enquêtes. Il est difficile d'être précis vu le nombre de pages disponibles sur internet. Ce pourcentage peut varier de 5 à 20 %, mais l'information importante à retenir est que le Deep Web est plus important en nombre que le Web standard. L'impressionnant nombre de pages et leur proportion très élevée en faveur du Deep Web font ressembler le Web dans son ensemble à un iceberg.

Figure 2 : Représentation du Web par un iceberg

La question à laquelle il est important de répondre est pourquoi certaines pages ne sont pas indexables ?

De fait, il existe plusieurs raisons expliquant pourquoi une page Web ne peut pas être indexée par les robots d'indexation, mais les plus courantes sont :

- Lorsque la page ne possède pas de backlink

  Une page Web sans lien hyper-text interne ou externe ne peut pas être atteinte par un robot d'indexation, donc impossible à indexer.

- Lorsque le contenu de la page ne le permet pas

  Il est possible que certains langages de programmation, comme JavaScript par exemple, empêchent la compréhension de certaines pages et rendent donc l'indexation impossible.

- Si le format de la page Web est non indexable

  Il faut noter qu'initialement les robots d'indexation ne comprenaient que le langage HTML, ce qui rendait difficile l'indexation d'autres formats par exemple les fichiers PDF. Actuellement les robots sont beaucoup plus performants et comprennent de plus en plus de formats.

- Lorsque le contenu de la page dépasse un certain volume

  Sur certains sites, avec de très grands volumes de données, par exemple les sites regroupant des archives, la totalité des pages n'est pas indexée afin de ne pas surcharger les serveurs. Par exempleGoogle s'arrête d'indexer à partir de 500 kb.

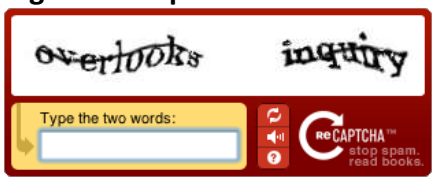
- Si la page est une Web Private Page

  Si l'auteur de la page Web désire qu'elle soit privée, et donc non indexable, il utilisera robot.txt dans le code. Ceci bloque les robots d'indexation et permet à un contenu de page de rester privé. Robots.txt permet également de protéger un copyright et d'éviter de retrouver des images privées d'un site sur Google Images. Ce fichier, placé dans le code du site, permet aussi de limiter l'accès au site et donc de limiter le trafic.
  Sur le même site, certaines pages peuvent donc être protégées par Robot.txt, et d'autres non. Il est à noter que pour avoir accès à une page privée, il suffit de connaître l'URL de la page (qui peut s'obtenir par l'administrateur du site lui-même ou via certains forums).

- Si la page ne permet qu'un accès limité

  Aussi connus sous le nom du Owner Web, ce sont des sites qui demandent une authentification via un login password ouvrant une connexion directement sur le site. Certains de ces sites sont payants et lors de votre inscription vous devez compléter un Captcha, prouvant par un enchaînement de caractères ou sous la forme d'une image non lisible pour une machine que vous n'êtes pas un robot d'indexation.

Figure 3 : Captcha identification



(http://www.captcha.net)

- L'IOT

  Cet acronyme désigne l'Internet Of Things (en français l'Internet Des Objets). L'IOT est le regroupement de tous les objets connectés par exemple AppleWatch, iPhone, PlayStation 4. Les pages Web de ces objets ne sont pas indexées pour des raisons logiques, car il n'y a aucun intérêt, malgré leurs URL, à le faire. En 2018, nous estimons que le nombre d'objets connectés sera supérieur à 450 millions.

  Considéré comme la 3e évolution d'internet, le Web 3.0 (IOT) représente l'échange de données entre les dispositifs du monde réel et les réseaux internet. Il existe des moteurs de recherche permettant de faire des recherches sur les IOT assez facilement. Cela peut permettre, et c'est important de le signaler, l'accès, par exemple, à certaines caméras de surveillance peu protégées ou à localiser certains véhicules connectés.

- Si le nom de domaine de la page n'est pas considéré comme un standard

  L'ICANN, l'Internet Corporation for Assigned Names and Numbers, est une compagnie américaine basée à Los Angeles qui se charge de la coordination des systèmes de noms de domaines assignés au DNS. Les noms de domaines les plus connus sont les. ch. com. org, etc. En tapant, par exemple, sur notre recherche le site « 20minutes.ch », notre demande sera envoyée au serveur DNS correspondant qui traduira ensuite la demande et nous redirigera vers le site souhaité. Si le nom de domaine n'est pas connu par le serveur DNS, il faut passer par un DNS spécial, d'où une indexation impossible de ces pages. Le domaine non « standard » qui nous intéresse le plus est »onion', accessible via le navigateur TOR (ce point sera traité ultérieurement, cette facette internet étant la moins facile d'accès, située sur le Dark Net, et permettant par la suite de nous trouver dans une couche plus profonde encore, le Dark Web).

- Les pages dynamiques

  Bien évidemment, les pages dynamiques ne sont pas indexables, car elles peuvent varier entre les demandes d'utilisateurs. Par exemple, il est impossible pour un robot d'indexer toutes les pages Web proposant des services de déplacements (comme EasyJet). En effet, dans ce cas, nous devons d'abord aller sur la page officielle du site et, en fonction de nos critères de recherches, le site nous proposera, par exemple, les vols correspondants à nos filtres.

Toutes ces pages non indexées par aucun moteur de recherche se retrouvent ainsi dans le Deep Web et l'on peut aisément constater qu'un utilisateur lambda d'internet fait des passages fréquents sur le Deep Web sans même s'en rendre compte.
Le Deep Web est donc souvent associé à une « zone criminelle » ou « peu sûre » par de nombreux utilisateurs simplement parce qu'il est peu expliqué ou très mal compris.
En effet, Google drive, votre boîte mail, le gestionnaire de votre commerce en ligne, tout ceci n'est pas indexable pour l'une des raisons citées plus haut. De fait, bien souvent sans même le savoir, nous sommes sur le Deep Web en toute légalité en utilisant nos outils de tous les jours. Cela explique aussi pourquoi la Surface Web est si petite comparée à celle du Deep Web.

Cette confusion entre le Deep Web et le Dark Web nuit donc à la réputation du premier. Le Deep Web n'est, en fait, simplement qu'une partie du Web non compréhensible pour certains moteurs de recherche.

Le Dark Web et les Dark Nets

Tout comme le Deep Web, le Dark Web est non indexable, mais, cette fois-ci, pour une seule véritable raison : le nom de domaine. En effet, par un nom de domaine non répertorié par l'ICANN, les sites possédants un nom tel que, par exemple « onion », ne sont pas accessibles aux navigateurs standard, car ils n'y sont pas référencés. Ceci principalement pour des raisons de discrétion. Le Dark Web n'est donc rien d'autre qu'une sous-division du Deep Web, une partie encore plus immergée de l'iceberg. Sur les 94 % correspondant au Deep Web seulement environ 4 % font partie du Dark Web. La différence importante à signaler est que le Dark Web utilise le, ou les, Dark Nets comme support, alors que le Web, comme nous l'avons mentionné plus haut, utilise l'internet. Les sites ayant comme nom de domaine » onion' sont donc des Dark Web.

Les Dark Nets, de l'anglais network, sont des sous-réseaux qui ne communiquent pas entre eux de la même manière qu'internet. C'est un ensemble de réseaux privés et anonymes qui utilisent des protocoles spéciaux intégrant des options de confidentialité et d'anonymat. À l'inverse du Web, qui utilise une architecture centralisée, le Dark Net lui utilise une architecture appelée Peer-2-Peer (P2P). Il y a donc plusieurs Dark Nets et ils peuvent varier en fonction de leurs infrastructures. Par exemple, il y a des réseaux P2P, des mixnets ou les 2 en même temps. Contrairement à un réseau centralisé, le P2P fonctionne sans serveur principal. En effet, le P2P se veut comme un échange de données entre les utilisateurs. Chacun d'entre eux partage l'information stockée sur son ordinateur sur le réseau. Ce type de connexion est chiffré et anonyme et, sans en posséder l'accès, il est quasiment impossible de s'y connecter. Un des premiers réseaux possédant un tel fonctionnement fut Freenet. En 2008, Freenet a élargi sa communauté en permettant l'accès à des personnes extérieures au cercle « d'amis », tout en restant chiffré et anonyme. Les Dark Nets permettant l'échange de données sont nombreux et d'autres Dark Nets permettent eux la construction d'écosystèmes tout en restant anonyme ; par exemple Tor, The Onion Router, sur lequel nous allons revenir par la suite. Par écosystème, nous parlons donc d'un système d'email, de chat, d'internet relais, de blog, etc.

Le mot Dark Net est apparu pour désigner tous les réseaux qui étaient isolés d'ARPANET pour des raisons de sécurité. ARPANET est l'ancêtre d'internet, créé par une agence américaine basée en Virginie, la DARPA (Defense Advanced Research Project Agency). La DARPA est une agence gouvernementale du Département US chargée de la recherche et du développement des nouvelles technologies pour des usages militaires.

De nos jours, ces réseaux anonymes permettent aux utilisateurs des Dark Nets de communiquer et/ou d'échanger des données ou des informations sans barrière et, surtout, sans être surveillé par un gouvernement ou toute autre agence de sécurité sur internet (y compris les fournisseurs internet).
Le problème central du Dark Web et des Dark Nets est qu'avec aucun véritable contrôle, on y trouve de tout et bien entendu aussi des activités illégales.

De nombreuses enquêtes, analyses, des chercheurs ainsi que plusieurs organes de police en Europe ou ailleurs ont essayé de quantifier/définir les activées illégales sur le Dark Web sans vraiment aboutir à un résultat exhaustif et vraiment relevant.

Pourquoi utiliser le Dark Net ?

Suite à la définition donnée des Dark Nets, nous pouvons en conclure qu'on n'y trouve donc pas que des activités illégales. En effet, beaucoup d'utilisateurs d'internet préfèrent le Dark Net à son cousin l'internet, mais pourquoi ?

Il faut savoir que le réseau d'internet, sans comprendre votre fournisseur d'accès, est la plupart du temps gratuit. Par exemple des recherches Google, ou un compte sur Facebook ne coûtent rien, et c'est là où réside une partie du problème. Car la plupart du temps, si l'offre est gratuite, c'est que, indirectement, nous sommes nous-mêmes le « produit ».

De nombreux utilisateurs lambda l'ont bien compris et refusent, pour des questions de confidentialité et de respect de la sphère privée, de se rendre sur des sites où sont mises à disposition gratuitement des données personnelles en faveur de tiers, souvent de grandes compagnies. En effet, ces données sont souvent ensuite revendues et utilisées pour analyser et prévoir le comportement de leurs propriétaires et même inciter leurs choix. Tout est marketing, et le Net n'y échappe pas. L'intérêt commercial, le profit d'une certaine manière, reste, dans de nombreux cas, un objectif principal et ceci avant les libertés individuelles les plus élémentaires bien souvent. Entre les données échangées sur les réseaux, les fournisseurs d'accès à internet, qui enregistrent les déplacements sur le Web, et certaines agences de sécurité du Web, comme la NSA, la surveillance est permanente. Certains affirment même que le Dark Net permettrait d'éviter cette surveillance globale des internautes dans le monde.

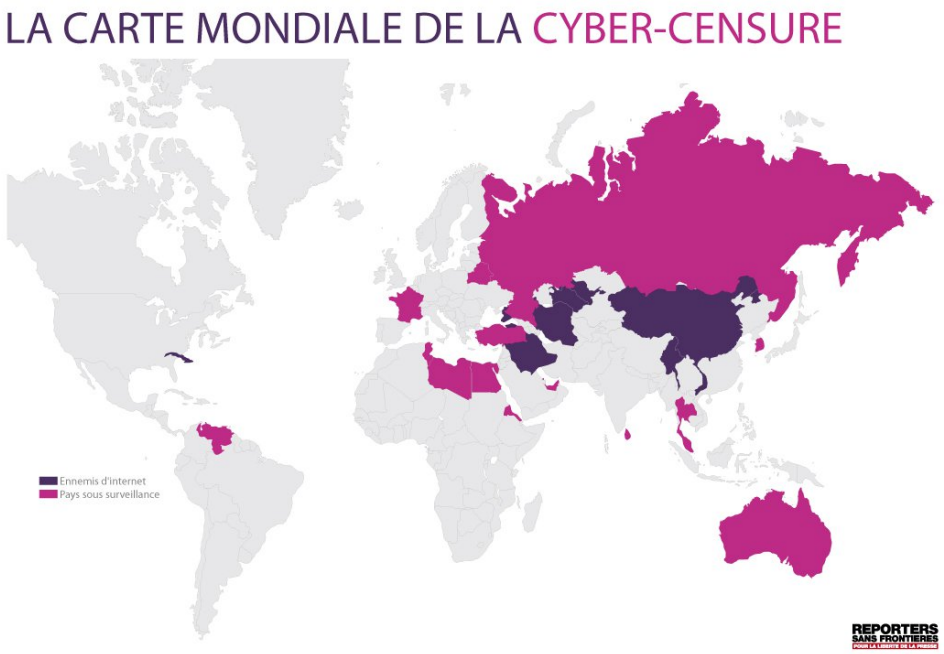
Grâce à son système d'accès et à son architecture, Certains Dark Nets rendent les déplacements anonymes et non traçables. Il faut souligner qu'avec une adresse IP générée par un fournisseur internet, nous sommes constamment géolocalisables ; de manière régulière et précise.

Un autre point important à souligner est : Qui utilise le Dark Net ? Car de toute évidence l'internaute lambda n'est pas le seul à s'y rendre. Un des Dark Net le plus connu a été conçu par l'armée américaine, qui l'utilise toujours. Et ce cas est loin d'être isolé. En effet, le département de la sécurité nationale d'un pays a intérêt d'être le plus discret possible par rapport aux réseaux qu'ils utilisent, ceci pour d'évidentes raisons de sécurité, donc il utilisera le Dark Net à cet effet.

Un autre utilisateur bien connu du Dark Net est le monde de la presse (principalement ses journalistes d'investigation). Effectivement, la discrétion, et la non-traçabilité des utilisateurs permettent aux journalistes d'entrer en contact avec des personnes dans le monde entier sans prendre de risques inconsidérés (pour eux comme pour la personne contactée).
L'échange de preuves, de faits divers ou d'interviews peut se faire en toute discrétion.

De plus, certaines zones du globe sont difficiles d'accès, pour des raisons liées à la guerre ou à un régime politique fermé par exemple. Le Dark Net permet donc de faciliter ces échanges en les rendant plus sûrs, et surtout possibles, pour certaines personnes n'ayant pas la parole ou lorsque le net « standard » ne souhaite pas les montrer et les censurer.
Certains journalistes français ont même renommé le Dark Net en Libre Net. Car la cybercensure existe vraiment, ci-dessous une carte postée par Reporters sans Frontières montrant dans quel pays elle est la plus présente :

Figure 4 : Carte mondiale représentant les ennemis d'internet



(https://rsf.org/fr)

Dans le même type de catégorie d'utilisateurs que les journalistes d'investigation, nous avons aussi les « dénonciateurs ». Comme exemple mentionnons Edward Snowden qui, durant sa fuite, s'est caché derrière le Dark Net pour communiquer les informations confidentielles qu'il détenait.
Un autre « dénonciateur », actuellement réfugié à l'ambassade d'Équateur à Londres, est Julian Assange, le fondateur de wikileaks. Devant une menace d'extradition aux USA, où il est l'objet de plusieurs poursuites judiciaires, le créateur de ce site, hébergeant un grand nombre de dénonciations, utilise également le Dark Web. WikiLeaks est connu pour son grand nombre de partages de documents qui aurait fuité de manière anonyme. Ce site évoque des scandales de corruption, des cas d'espionnage, en masse ou visant une personne en particulier, et des violations des droits de l'homme dans de nombreux pays.
Le site mentionne clairement : « les principes généraux sur lesquels notre travail s'appuie sont la protection de la liberté d'expression et de sa diffusion par les médias, l'amélioration de notre histoire commune et le droit de chaque personne à créer l'histoire.
Ces principes découlent de la Déclaration universelle des droits de l'homme. En particulier, l'article 19 inspirant le travail des journalistes et autres "volontaires" ».
Malgré ceci, le fondateur de WikiLeaks, ainsi que beaucoup de ses activistes, reçoit de très nombreuses menaces et intimidations du plus haut niveau.

Ces « dénonciateurs » n'auraient jamais pu poster ce type de documents sur la Surface Web sans se faire directement censurer par le ou les gouvernements gardant le contrôle de leur Web respectif afin d'en contrôler le contenu et étouffer les « affaires gênantes' les concernant.

The Onion Router et les autres accès au Dark Net

Il existe plusieurs types d'accès permettant de se rendre sur le Dark Net. Le premier type est celui permettant l'échange de données comme GnuNet ou Retroshare.
Grâce à un accès sur les Dark Nets, ce type de réseaux, aussi appelé Friends-to-Friends, permet l'échange de fichiers dans une communauté bien définie, ou en train de l'être. Leur anonymat ainsi que la non-traçabilité permettent à leurs utilisateurs des échanges de nombreuses données variées sans avoir à craindre de « représailles ».

Retroshare

Retroshare est vu comme un réseau social sécurisé permettant la communication et l'échange avec des « amis ». Il fournit :

- Une messagerie instantanée cryptée
- Un système de partage de fichiers sécurisés
- Des forums décentralisés

Figure 5 : Logo Retroshare

(http://retroshare.net/index.html)

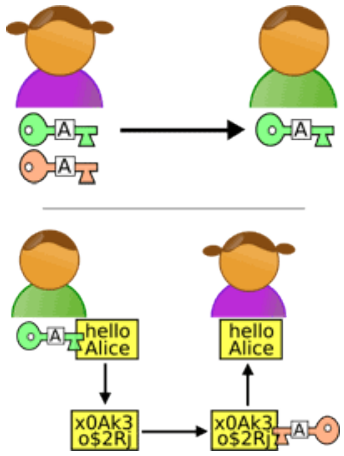
Le point fort est la sécurité de ce réseau, car les fichiers ne sont partagés qu'avec des « amis », « amis » que vous avez vous-même validés. De plus, il n'y a pas de cloud de stockage et on peut éviter l'utilisation de systèmes de communication standard tels que Facebook, Skype ou Google pour entrer en contact avec ces « amis ».

Après l'installation de Retroshare sur votre machine (Windows, Macintosh ou Linux), une paire de clés d'authentification « utilisateur » sera distribuée. Ces clés sont des chiffrements GPG (Gnu Privacy Guard) qui utilisent la cryptographie asymétrique RSA 2048 bits.

La cryptographie asymétrique

Aussi appelée le « chiffrement de la clé publique et privée », la cryptographie asymétrique est un système de cryptage qui se déroule en 3 étapes assurant l'envoi d'un message chiffré et permettant l'authentification de l'expéditeur.
Dans un premier temps, l'utilisateur A génère une clé publique et une clé privée. La clé publique est alors envoyée à l'utilisateur B. Ce dernier va alors crypter un message avec la clé publique de l'utilisateur A. L'utilisateur A va ensuite décrypter le message de l'utilisateur B avec sa clé privée.

Figure 6 : Illustration de la cryptographie asymétrique



Par cette technologie, la personne assure son niveau de confiance sur le réseau et peut donc partager une clé avec une personne tierce pour créer un lien avec elle. C'est donc, finalement, un service du réseau qui procède à l'échange de clés publiques entre 2 « amis ». Les adresses IP seront récupérées par un DHT (Distributed Hash Table) mis en œuvre par bitTorrent permettant la proposition « d'amis » en commun. Le DHT agit comme un intermédiaire neutre, que l'on consulte pour mettre en place des connexions.

Retroshare propose un système de clés GXS, avec lequel vous pouvez créer plusieurs « sous compte », originaires de votre compte, afin de multiplier vos « cyberidentités » en fonction du service utilisé sur Retroshare. En d'autres termes, vous pouvez avoir une identité pour le système de courriel et une autre pour communiquer sur les forums.
Cependant, ces clés GXS restent indépendantes des clés RSA parentales des utilisateurs.
Un réseau Friends-to-Friends est une extension du système Peer-to-Peer, bien connu de cette communauté. En effet, le P2P est un réseau où nous pouvons nous connecter à d'autres paires de manière totalement aléatoire dans le monde, alors que le F2F ne propose des connexions qu'avec des membres de la communauté que vous avez approuvés.

Il n'y a pas de nombre d'amis' minimums obligatoire, cependant il est conseillé de créer un réseau d'au moins 5 personnes pour pouvoir utiliser Retroshare de manière pleinement intéressante (mais le réseau tournera même avec deux uniques utilisateurs).

Vos communications sont cryptées en utilisant des techniques OpenSSL standard et vos fichiers sont échangés par la connexion entre 2 « amis », soit un système de tunnel anonyme qui permet à 2 utilisateurs de passer leurs fichiers via une chaîne « d'amis ». L'implémentation de cet algorithme s'inspire du Turlte Hopping où les fichiers sont uniquement représentés sous leurs formes « hachées » dans un système de liens permettant d'inclure ou d'exclure les références des fichiers passés à travers le tunnel. Vos « amis » participant à ce tunnel anonyme ne pourront donc pas lire en « clair » vos fichiers partagés.

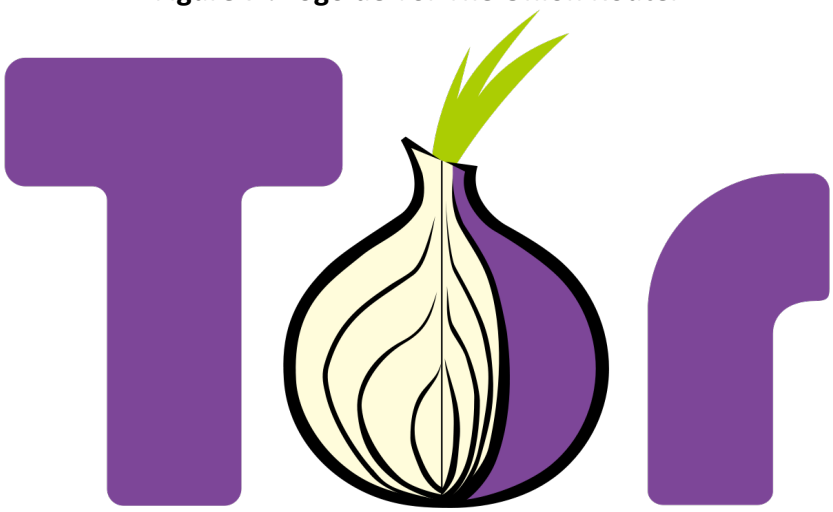
OpenSSL standard

Open SSL standard est un système de chiffrement se composant d'une bibliothèque d'algorithme de cryptage et du protocole de communication Transport Layer Security. Ce protocole de sécurité des échanges sur internet permet l'authentification du serveur ou du pair par un cryptage des données ainsi que celle du client ou de l'autre pair.

Tor

Le deuxième type d'accès permettant de se rendre sur le Dark Net est Tor, The Onion Router. Le terme « oignon » s'explique par le fait qu'il est organisé en couches, un peu comme un oignon. Le réseau Tor a été inventé par la marine US.

Figure 7 : Logo de Tor The Onion Router



(https://www.torproject.org)

Tor est un réseau superposé proposant des recherches directement dans le Dark Web, ou le Web, dans l'anonymat le plus complet. En effet, avec le réseau Tor, vous allez atteindre votre destination en passant par plusieurs points dans le monde.
Il permet l'accès à tous les sites présents sur l'internet, même ceux qui ne sont pas référencés par les moteurs de recherche, volontairement ou pas.

Tor va donc se charger de vous rendre anonyme sur les réseaux. Cependant cela a un prix : la performance. La première chose que l'on remarque quand on utilise le navigateur Tor, c'est une vitesse de chargement très lente.

En effet, au moment de l'envoi de votre requête, par exemple sur le site « unsiteauhasard.ch », en direction du serveur du site « unsiteauhasard.ch », Tor va se charger de séparer votre requête en plusieurs parties. Il prendra la peine d'effacer une partie des paquets de l'en-tête de la requête comme de la source, l'heure et la date.

Ensuite, il se chargera de crypter chaque paquet, puis les enverra à un nœud présent sur le réseau. Ce nœud va décrypter le minimum d'informations possibles afin d'obtenir seulement les éléments nécessaires concernant l'étape suivante du paquet, puis recrypter le tout avant de l'envoyer au nœud suivant. Voilà d'où vient la comparaison avec l'oignon.
Cette étape de décryptage et recryptage peut se répéter une dizaine de fois.
Ce paramètre, Relay, peut être réglé dans le code de Tor, tout comme le pays de destination.
Les nœuds, appelés onion router, sont des serveurs distribués, en d'autres termes des ordinateurs d'autres utilisateurs qui assurent une protection contre les agences de surveillance, des fournisseurs d'accès et contre les onion routers eux-mêmes.

De cette manière, Tor protège vos informations par exemple votre adresse IP, votre géolocalisation, les données transférées et la destination de vos requêtes. Ceci permet d'éviter que de potentiels hackers, agences de surveillance ou fournisseurs d'accès à internet « volent » ces informations ou contre un administrateur du système qui lui peut les communiquer à un gouvernement ou à la police. Cette protection est assurée par le cryptage répété des informations qui passent par plusieurs relais avant d'arriver à destination.
Cependant, le passage d'informations entre le dernier relais et le serveur du site souhaité est en « clair » si le site est en HTTP, mais chiffré si le site est en HTTPS.

Voici la différence des informations que nous laissons derrière notre passage sur internet :

Tableau 1 : informations laissées après notre passage sur internet

<table>
<tr><th></th><th>Navigateur standard</th><th>Tor + HTTP</th><th>Tor + HTTPS</th></tr>
<tr><td>Hacker</td><td rowspan="3">• Site de destination
• Informations personnelles
• Données
• Location</td><td rowspan="3">• Location
• Tor</td><td rowspan="4">• Location
• Tor</td></tr>
<tr><td>Fournisseur d’accès internet côté client</td></tr>
<tr><td>Agence de surveillance cotée client</td></tr>
<tr><td>Tor relais</td><td>Inexistant</td></tr>
<tr><td>Tor dernier relais</td><td>Inexistant</td><td rowspan="4">• Site de destination
• Informations personnelles
• Données
• Tor</td></tr>
<tr><td>Agence de surveillance cotée serveur</td><td rowspan="3">• Site de destination
• Informations personnelles
• Données
• Location</td></tr>
<tr><td>Fournisseur d’accès internet côté serveur</td></tr>
<tr><td>Administrateur du serveur</td><td>• Site de destination
• Informations personnelles
• Données
• Tor</td></tr>
</table>

(https://blog.nicolargo.com/2012/04/introduction-et-premiere-utilisation-de-tor.html)

Tor, accompagné du protocole HTTPS, permet un anonymat de manière efficace sur :

- Notre site internet de destinations, là où nous cherchons à nous rendre
- Nos Informations personnelles, comme notre username et notre password
- Nos données, ce qui signifie nos données échangées sur le réseau

La localisation qui peut être retrouvée dans ces paquets est celle du dernier nœud se trouvant sur la chaîne de Tor relais (cependant la personne qui intercepte un paquet saura que Tor est utilisé), donc que l’on se trouve sur le Dark Net.

Traçabilité

La capacité de Tor à nous rendre non traçables est due à ses nœuds qui sont, en fait, d'autres utilisateurs du réseau qui permettent de se retrouver à d'autres endroits du globe lors de l'accès au serveur du site que vous souhaitez atteindre. Maintenant, il faut imaginer que l'on se rende sur le site « lematin.ch » depuis Genève, mais en passant par les USA, puis l'Angleterre et, finalement, revenir aux USA. Si quelqu'un devait maintenant intercepter un des paquets de la requête, par exemple l'administrateur du site, et qu'il décrypterait ce paquet et trouvait l'adresse IP, il verrait d'abord celle des États Unis d'Amérique puis il s'apercevrait qu'il s'agirait d'un Tor Relay. Il devrait donc décrypter une seconde couche du paquet pour se diriger vers un autre Tor Relay et ainsi de suite. On peut donc imaginer la complexité d'une telle procédure. Complexe, mais pas impossible pour autant. C'est pour cela qu'il existe des moyens pour devenir encore plus difficile à « tracer ». Un de ces moyens est l'utilisation d'un VPN (à noter que le VPN va également ralentir votre vitesse de connexion, ceci combiné à Tor la différence se fait ressentir). Le VPN est traité ci-dessous.
Le seul moyen donc de retracer tous les liens entre les nœuds relais est de placer une entité globalisée passive avec la capacité de comparer tout le trafic sur le réseau Tor en enregistrant le timing et la taille de tous les paquets. Si cela devait se mettre en place, il serait, statistiquement parlant, possible de retracer les paquets jusqu'à leur réel expéditeur.
Nous comprenons donc mieux à présent pourquoi une communauté grandissante est nécessaire pour ce genre de projet qu'est Tor.

VPN

Un Virtual Private Network offre la possibilité de vous connecter, toujours de manière sécurisée, sur un autre lieu dans le monde où se trouve un serveur VPN. C'est depuis ce point que seront envoyées vos requêtes dans le réseau Tor. De plus, c'est l'adresse du VPN qui sera mise à disposition du réseau Tor ainsi qu'aux autres utilisateurs concernés.
De ce fait, vous possédez un extra Tor Relay pour votre connexion.
Si votre objectif est de faire des achats sur le Dark Web, vous avez donc meilleur temps d'utiliser un VPN

I2P

The Invisible Internet Project est un autre accès au Dark Net fonctionnant de la même manière que Tor. En effet, I2P va crypter vos données et les envoyer à un autre utilisateur du réseau, qui en fera de même et ceci jusqu'à parvenir au site de destination.
Seules deux différences concrètes sont à notifier. La première concerne le dernier Tor relais. Le système de I2P fonctionne avec des classes de routeurs appelées FloodFill. Ces routeurs remplacent le dernier Tor Relay et c'est lui qui communique avec les serveurs des sites visités. Les FloodFill gardent en mémoire quels tunnels (la chaîne de Tor Relay dans le système I2P) communiquent avec quels serveurs.
La deuxième différence est en rapport à leur notoriété. Tor étant nettement plus connu, son nombre de nœuds est donc beaucoup plus important et, par conséquent, plus difficile à retracer.

Accès et utilisation

Afin de profiter pleinement de l'anonymat qu'offre Tor, je vais vous présenter quelques notions importantes à mettre en pratique sur les Dark Nets afin de préserver sa sécurité quant à votre identité.

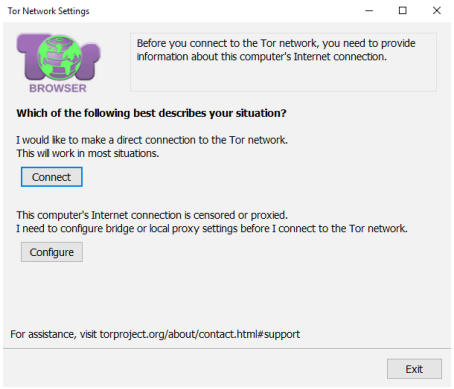
Approche technique d'accès

Il y a plusieurs manières d'utiliser le réseau Tor, et cela dépend de votre OS. Certaines de ces procédures sont plus sécurisées que d'autres.
Commençons par les 3 OS les plus repandus :

- Windows
- Mac OS
- Linux, ou OS avec un cœur Linux

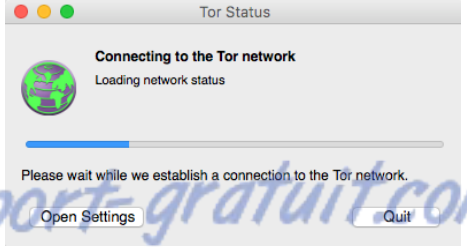
Avec l'un de ces OS, il suffit d'installer Tor Browser depuis le site thetorproject.org. Au moment de l'installation, une question vous sera posée à propos de la situation qui vous convient le mieux. Cette situation concerne votre accès à internet.
La première réponse vous propose un accès direct au réseau Tor, cela est possible si vous n'avez aucune restriction ou censure de l'internet dans votre pays ou une redirection de proxy. Si cela est votre cas, vous devez configurer un bridge, un VPN ou un proxy, vous localisant à l'extérieur de la zone censurée d'internet. Il est important de garder sa version Tor à jour, car régulièrement des mises à jour sont effectuées.

Figure 8 : Configuration de Tor



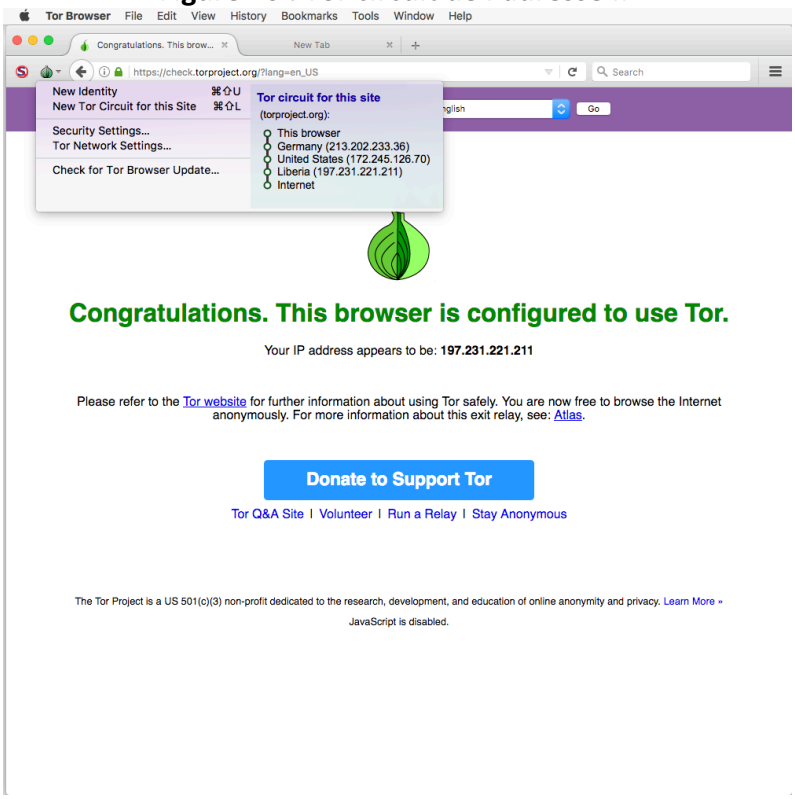
Quand le browser est installé, à l'ouverture de l'application, votre ordinateur va se connecter au réseau Tor, et donc partager votre adresse IP aux utilisateurs pour vous permettre de faire de même avec leurs propres adresses.

Figure 9 : Tor joint le réseau en mettant à disposition votre adresse IP



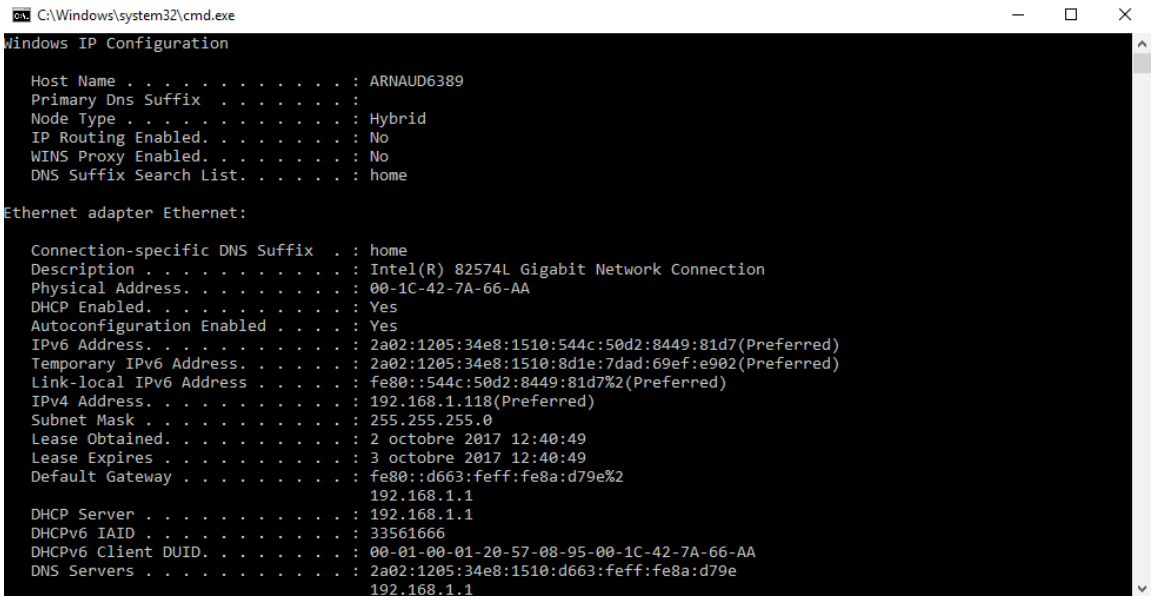
La page d'accueil du programme s'ouvre et vous indique que vous pouvez naviguer sur internet de manière anonyme. Vous pouvez aussi faire un test des réglages de Tor, qui vous indiquera l'adresse IP que vous possédez.

Figure 10 : Tor circuit de l'adresse IP



J'ai fait le test moi-même, et mon adresse IP n'était pas celle fournie par mon fournisseur d'accès à internet. En effet le site m'assure que je suis sur le réseau Tor et me montre une adresse IP libérienne, en passant par l'Allemagne et les USA.

Figure 11 : Adresse IP disponible par le fournisseur internet



Il existe aussi d'autres types d'OS beaucoup moins connus, mais beaucoup plus sécurisés. J'ai choisi de vous parler de l'OS Qubes ; il a, depuis peu, pris la place de Tails OS, un autre OS ou la sécurité est prioritaire. C'est également l'OS que Edward Snowden a choisi d'utiliser pour un niveau de sécurité, de son point de vue, jugé imbattable. Un grand nombre d'activistes dans le monde conseillent d'utiliser Qubes. Des articles de presse sont apparus dans The Economist, Motherboard et WIRED à propos de cet OS.
Qubes fonctionne avec le Xen Project, incluant le Xen Hypervisor. Ce dernier fonctionne à l'aide des principaux fournisseurs d'hébergements dans le but d'isoler les sites les uns des autres, tout comme pour les services. Le système mettant en parallèle 2 machines virtuelles, comme le fait Whonix OS, car il y est intégré. L'une des machines permet les communications sur internet via le réseau Tor et l'autre supporte les applications de l'utilisateur. Ce système peut être lancé depuis un DVD ou une clé USB, mais pas depuis une Virtual Machine.
Il existe une dernière manière de se rendre sur le Dark Net. Cette façon de faire est aussi la plus compliquée, mais reste une des plus répandues. Elle permet un système de maintenance différent entre la machine qui est utilisée comme nœud et celle qui permet de naviguer sur le réseau. En premier lieu, vous devez, à l'aide des lignes de commande du Terminal, inscrire votre machine au réseau Tor. À ce moment-là, vous pouvez déjà utiliser un VPN. Ensuite vous devez télécharger un programme multiplateforme vous permettant d'utiliser Tor auprès d'une configuration adéquate. Un exemple de ce genre de software est Vidalia, qui est aussi le nom d'une variété d'oignon. Ensuite, vous utilisez Vidalia « comme navigateur », car il se charge de supporter et de mettre en fonction la navigation sur le réseau Tor.

Utiliser une VM

L'utilisation de la Virtual Machine, qui exécuterait, par exemple Windows 10, est l'une des manières les plus simples et les plus sécurisées de se rendre sur Tor et le Deep Web. La Virtual Machine vous protégera des virus et autres programmes de cyberespionnages, car, en cas de contamination, elle est immédiatement détruite depuis la machine physique et ensuite réinstallée.
Si votre objectif est de naviguer sur internet de manière anonyme, une VM et Tor sont suffisants, la VM est même optionnelle.

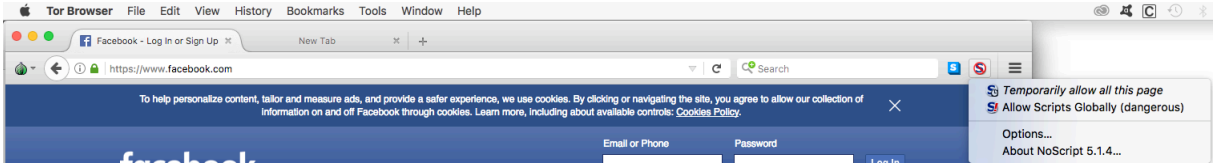
Un autre moyen de rendre Tor encore plus sécurisé est d'en parler autour de nous. Si de plus en plus de personnes l'utilisent, les nœuds sur le réseau seront plus nombreux et permettront plus d'anonymats.

Approche technique d'utilisation

Afin de rendre votre utilisation Tor la plus sécurisée et la plus agréable possible, certains réglages et un changement de comportement sur internet sont à prendre en compte.

Le premier réglage à faire, mais optionnel, est de désactiver le contenu JavaScript, car avec son cryptage et décryptage constant, le réseau Tor est particulièrement lent et, malheureusement, le contenu JavaScript n'aide pas en termes de performance. Les sites du Surface Web qui contiennent du JavaScript seront affectés et perdront les animations de ce langage. D'ailleurs les sites du Deep Web et du Dark Web ne sont pas souvent écrits en JavaScript pour cette raison et paraissent donc plus anciens.

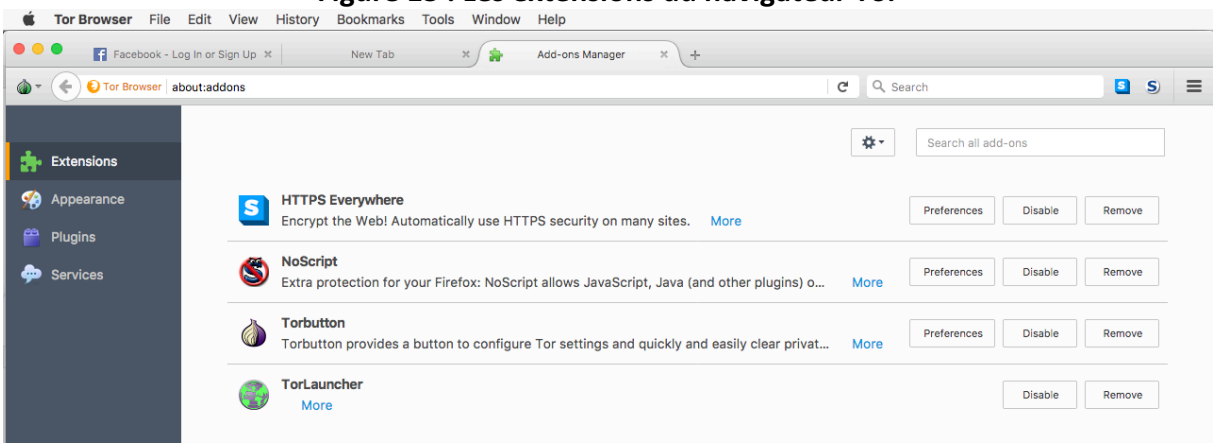
Figure 12 : Autoriser le JavaScript sur Tor



Il est déconseillé de faire du partage de torrent en utilisant le réseau Tor. La première raison est due au fait que pendant l'envoi de paquets à travers le réseau Tor vous allez régulièrement envoyer votre réelle adresse IP dans la requête GET du torrent en téléchargement ou en partage, car tel est le fonctionnement des torrents. Il faut rappeler que Tor ne fonctionnement pas de manière P2P.
La deuxième raison est que vous allez ralentir le trafic de toute la communauté.

Tor vient déjà avec des extensions, qu'il ne faut pas désactiver, par exemple HttpEverywhere et NoScript. Il est conseillé de ne pas ajouter d'autres extensions.

Figure 13 : Les extensions du navigateur Tor



Bien évidemment il est conseillé d'utiliser uniquement des sites en HTTPS, pour les raisons citées auparavant et pour rendre la connexion au réseau Tor plus sûre pour toute la communauté. De plus, par une connexion HTTPS, vous êtes protégés des nœuds malicieux qui pourraient lire vos données.

Il est sérieusement recommandé de ne pas ouvrir de documents, comme. texte. doc ou même PDF, télécharger depuis Tor, quand que vous êtes connectés au réseau. Ces documents peuvent contenir des ressources provenant d'internet et pourraient créer un lien avec ce dernier et afficher ainsi votre vraie adresse IP. Pour cette même raison, il est conseillé d'utiliser une machine virtuelle avec le réseau désactivé ou TailsOS ou autre OS sécurisé.

Afin de contrôler votre niveau d'anonymat, vous pouvez sélectionner les nœuds que vous voulez privilégier ou bannir de votre chaîne de nœuds, vous permettant d'atteindre le serveur du site de destination. Il est possible dans le code de Tor de régler ce paramètre, tout comme votre pays de destination :
Dans le fichier de l'application Tor, ouvrir avec un éditeur de texte le fichier « torrc ». À la fin de cette page de code, vous pouvez rajouter la ligne.

```
ExitNodes {pl} StrictNodes 1
```

Celle-ci utilisera un nœud polonais comme dernier nœud.
D'autres réglages de ce type sont possibles, vous pouvez les découvrir dans le manuel de Tor.

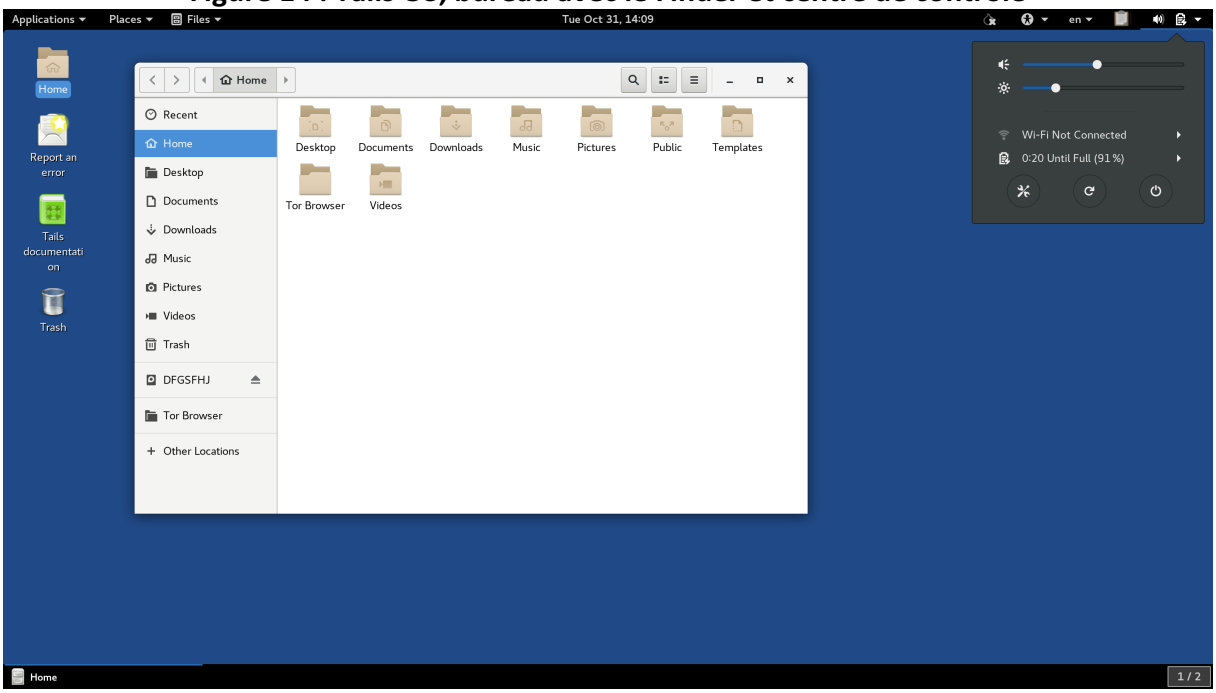
Simulation

Afin de pouvoir expliquer et de pouvoir présenter ma propre expérience sur le réseau Tor, je me suis plongé dans le Deep Web. Pour cela, j'ai décidé de le faire depuis deux OS différents. Le 1er sera sur l'OS Tails, car beaucoup plus simple à l'installation depuis une machine MacBook Pro que Qubes, mais toujours aussi sécurisé.
Au moment du démarrage de mon MacBook, je sélectionnerai l'OS de Tails pour booter mon ordinateur.
La deuxième entrée dans le réseau se fera depuis une VM Windows 10. Bien évidemment aucune transaction ne sera faite sur le Dark Net pour des questions juridiques. Je reviendrai sur ce sujet. Mais je naviguerai dans le Dark Net dans le but de vous expliquer mon expérience personnelle.

Tentative sous l'OS Tails

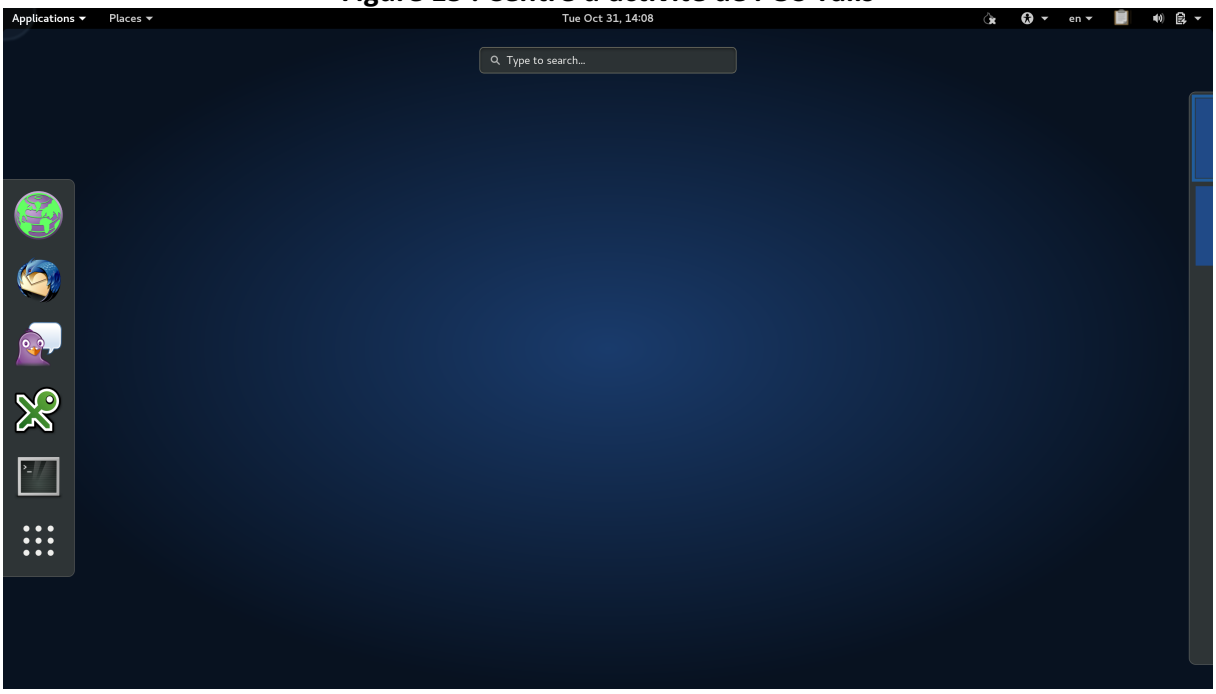
Pour commencer, j'ai dû installer un Tails intermédiaire sur une clé UBS depuis les lignes de commande de mon Terminal MacBook. Quand cette installation fut finie, j'ai dû booter mon ordinateur depuis la clé USB rendue « bootable » durant l'installation du Tails intermédiaire.
Ensuite, depuis ce Tails, j'ai installé le Tails définitif et l'ai rendu « bootable » sur la seconde clé USB. Pour finir, je me retrouve donc avec une clé USB contenant la version définitive pour utiliser Tails et une seconde clé que je peux formater. Cette installation très spéciale permet de segmenter Tails en 2 machines, une permettant d'être reliée au réseau Tor, et l'autre contenant les applications « utilisateur ».

Figure 14 : Tails OS, bureau avec le Finder et centre de contrôle



Voici à quoi ressemble le bureau de Tails, avec le Finder ouvert et le point de contrôle général. L'esthétique n'est pas le point mis en avant avec ce type de système d'exploitation, mais la sécurité.

Figure 15 : Centre d'activité de l'OS Tails



En déplaçant la souris vers le haut, nous avons accès au menu de recherche, aux applications favorites, nous y trouvons TorBrowser, et il permet d'organiser les fenêtres ouvertes sur la session.

Sans posséder l'adresse exacte du site, il est impossible de trouver un Dark Web, même avec le moteur de recherche par défaut de Tor, DuckDuckGo Search Engin, qui permet d'atteindre les sites du Surface Web sans problème.

Figure 16 : Moteur de recherche par défaut de Tor

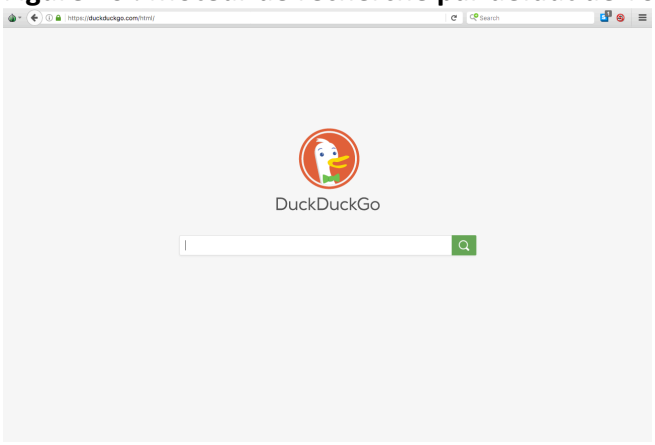
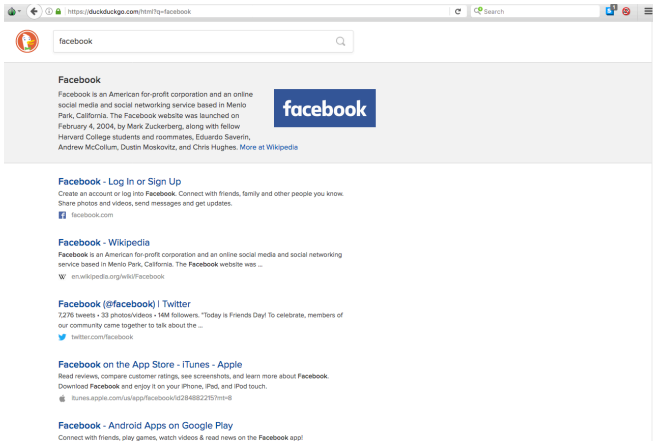
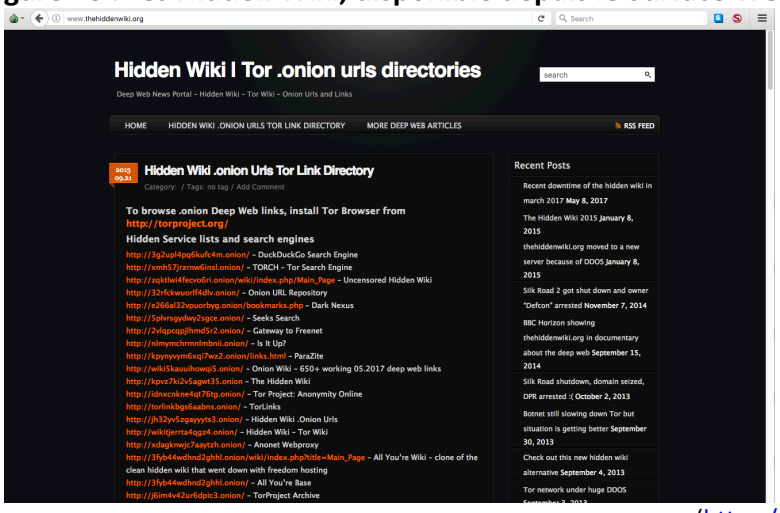


Figure 17 : Recherche du site Facebook sur DuckDuckGo



Facebook est facilement atteignable comme la plupart des autres sites répertoriés. Un moyen facile d'atteindre le Dark Web est grâce au Hidden Wiki.

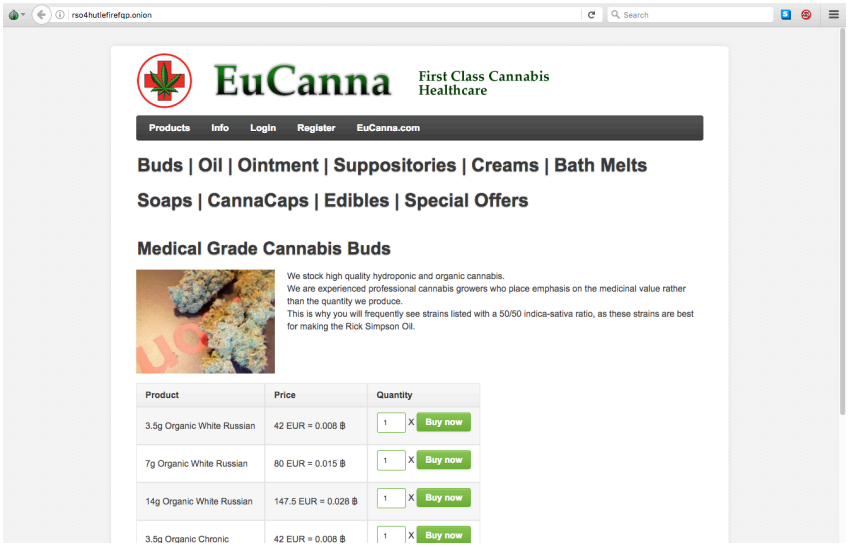
Figure 18 : Les Hidden Wiki, disponible depuis le Surface Web



(https://thehiddenwiki.org)

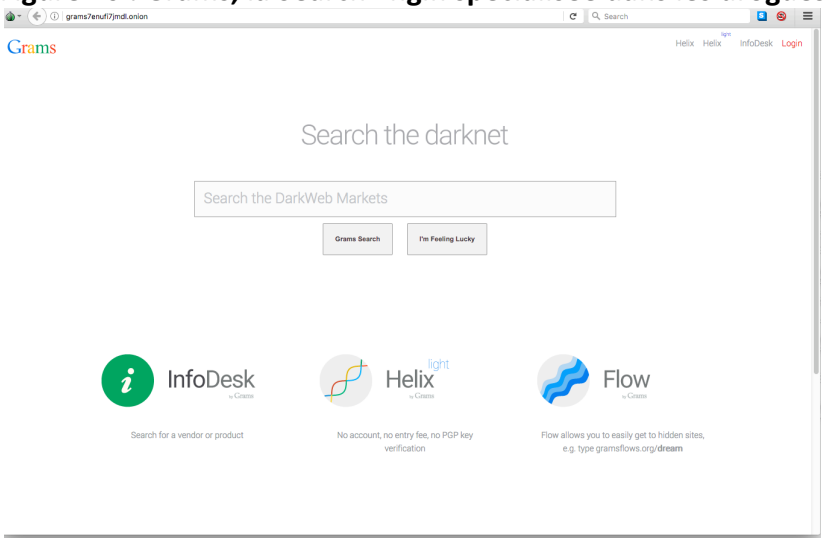
Classé par type de marché, il est facile de trouver ce que l'on cherche.
La première section concerne les Search Engins, en d'autres termes les moteurs de recherches spécialisés dans un domaine spécial. Nous trouvons ensuite des sites pour acheter/vendre des Bitcoins ou des sites Escow/Tumbler. Puis viennent les cryptomarchés.
Durant cette simulation, nous allons nous rendre sur un Dark Web spécialisé dans la vente de Cannabis, le produit le plus répendu sur les cryptomarchés, trouvable sur dans les Hidden Wiki, EuCanna.onion.

Figure 19 : Dark Web proposant du Cannabis ou des produits dérivés



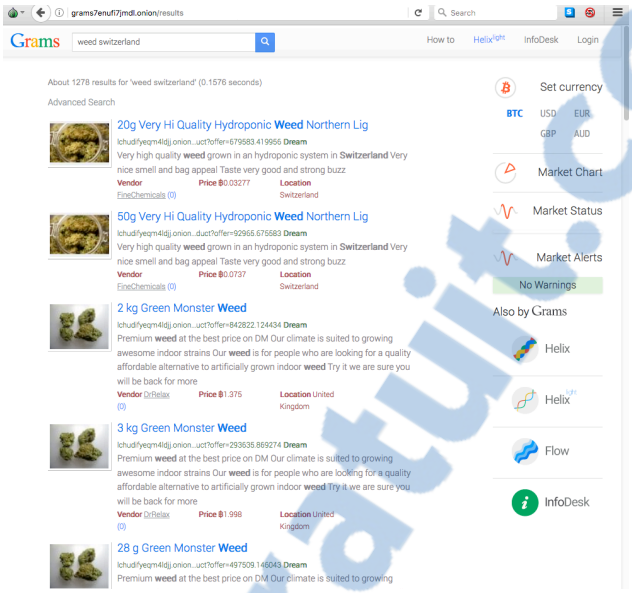
On y voit tout de suite ce que nous sommes venus chercher. Le site propose différents produits à base de Cannabis. Les prix sont affichés en Euro et en Bitcoin. En cliquant sur « Buy Now », nous sommes redirigés vers une page de login. Sans possession d'un compte sur le site, il est impossible de réaliser une transaction. Une fois connectés, nous rentrons en contact avec le vendeur via un système de messagerie. Nous nous arrêterons à cette étape pour continuer sur un autre moyen de trouver ce que l'on cherche grâce à des Search Engins. Ils en existent des spécialisés dans la drogue, l'un des plus connus est Grams.

Figure 20 : Grams, la Search Engin spécialisée dans les drogues



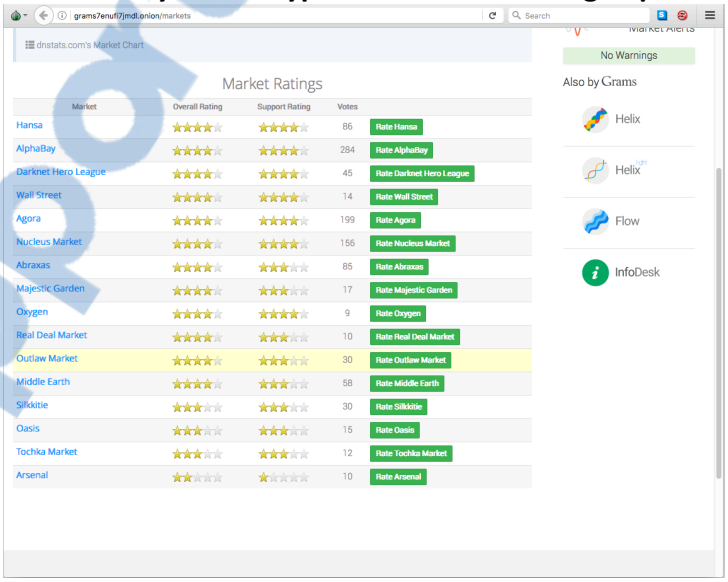
Grams a développé son propre Bitcoin Tumbler, Helix by Grams, accessible depuis la page d'accueil. En tapant dans la barre de recherche « weed switzerland », voici le résultat :

Figure 21 : Recherche « weed switzerland » sur Grams



On y voit de nouveau le produit recherché avec son prix, son vendeur et sa location. Sans compte sur ces Dark Webs, ces pages ne nous sont d'aucune utilité.
Grams propose un Market Chart nous offrant la possibilité de noter les différents cryptomarchés.

Figure 22 : Analyse des cryptomarchés de la drogue par Grams



Il n'est pas compliqué de trouver l'adresse d'un cryptomarché, de s'y rendre et de s'y inscrire. L'accès à tous ces produits illégaux est si facile, sans même bouger de chez soi, juste avec une connexion internet.

Tentative sous machine virtuelle Windows

Cette tentative est beaucoup plus simple en termes d'accès. En effet, possédant déjà une machine virtuelle Windows sur mon ordinateur, j'ai juste eu à installer Tor browser et me rendre sur le Dark Web. La différence est qu'avec Windows, les connexions non sécurisées ne sont pas bloquées, comparées à Tails, et que nous utilisons une machine comme accès au Dark Net qui est la même machine également offerte comme relais à la communauté. De plus, nous devons désactiver toutes les applications ayant un accès à internet.

Tableau 2 : Comparaison du niveau de sécurité par rapport aux différents OS

	Configuration normale	Virtual Machine	Tails OS
Malware et virus	Endommage la machine	Sans risque	
HTTP	Accessible		Inaccessible
Segmenter la machine personnelle et celle sur le réseau	À configurer		Natif
Application avec accès à internet	Dois être désactivée		Bloqué

Une configuration normale signifie un OS standard avec Tor browser comme accès au réseau Tor

La VM et Tails OS sont sans risque à propos dans Malware et virus, car la destruction de la VM se fait facilement sans endommager la machine physique.

L'avantage de Tails OS comparé aux autres méthodes est qu'il permet l'accès uniquement aux URL HTTPS, car toutes les applications de l'OS qui demandent une connexion internet sont configurées pour accéder à internet via Tor.

Légalité

La question qui revient le plus souvent quand on parle de Deep Web ou de Dark Net est « est-ce légal ? », la réponse est bien évidemment oui.

Le Deep Web est une partie inévitable du Web pour différentes raisons que nous avons déjà expliquées et particulièrement du moment où le site n'est pas référencé par les moteurs de recherche. Cela peut être dû à une mauvaise manipulation du code source du site. En effet, il suffit que l'équipe de développeurs soit débutante et que leur site ne puisse pas être indexé dans les bases de données. Ce qui ne rend pas ce site illégal pour autant. De plus, si cette « non-indexation » est souhaitée ou voulue, code lié au fichier robot.txt, ce site est toujours aussi légal que celui cité dans la première hypothèse.

En ce qui concerne les Dark Nets, leurs utilisations sont tout aussi légales. Et ceci est protégé par les droits de la sphère privée.

Protection de la personnalité

Le Code civil suisse et la Constitution de la Confédération suisse de 1999 possèdent plusieurs articles sur ce sujet. Des lois et de la jurisprudence du Tribunal fédéral permettent de concrétiser le sujet. Ces différentes sources sont présentes afin de protéger et contenir les atteintes à la personnalité.
Dans un premier temps, la Constitution fédérale règle, notamment, les droits fondamentaux (art. 7 ss Cst.). Nous avons par exemple la protection des enfants et des jeunes (Art. 11 Cst.) la protection de la sphère privée (art. 13 Cst.), la liberté d'opinions et d'informations, en plus de ces dispositions, la liberté des médias est également protégée, ce qui protège la volonté et la possibilité à quelconque individu d'avoir accès librement à un média, de s'y renseigner et de s'y fier.
Le Code civil suisse protège la personnalité contre des engagements excessifs (art. 27 CC) et contre des atteintes (art. 28 a et b CC). Le demandeur a notamment le droit de requérir le juge pour « interdire une atteinte illicite, si elle est imminente (ch. 1) ; de la faire cesser, si elle dure encore (ch. 2) ; d'en constater le caractère illicite si le trouble qu'elle a créé subsiste (ch. 3) ». Cette disposition est la plus employée lors d'atteintes à la personnalité causées par des manipulations du Web.
La Loi sur la protection des données du 19 juin 1992 (LPD ; 235.1) vise à « protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (art. 1 LPD). Cette loi fédérale est essentielle pour protéger les personnes, prévenir les différentes atteintes à la personnalité qui peuvent avoir lieu par le biais de la diffusion des données.

Ces lois (comme la Loi sur la protection des données personnelles LPD) et des dispositions (articles qui se trouvent dans les lois, CC par exemple ou Constitution) sont présentes pour protéger et contenir les atteintes aux droits de la personnalité.
Voici quelques exemples de différentes protections des droits de la protection de la personnalité :

- Le respect de la vie privée
- Le respect de l'honneur
- Le respect de l'intégrité corporelle
- La liberté de mouvement
- La protection du nom et des données personnelles

Toutes ces lois sont respectées lors de l'utilisation de Dark Nets, ce qui n'est pas toujours le cas comparé aux connexions sur un réseau standard, où nos informations sont lisibles par n'importe qui pouvant y avoir accès. Les grandes multinationales comme Google ou Apple ne se privent d'ailleurs pas de s'en servir. Par exemple, dans les documents présentant les changements ou les mises à jour de nos applications, c'est bien souvent au moment où nous acceptons les termes et conditions de ces mises à jour que nous autorisons, sans vraiment le savoir, ces compagnies à utiliser nos données. Nous ne pouvons rien faire contre cela, car sans ces mises à jour, les applications deviennent obsolètes et ne fonctionneront plus après un bref délai.

Le seul moyen de combattre cette surveillance et ce « vol » de données légales est d'emprunter les Dark Nets comme le réseau Tor. Et cette option est totalement légale !

Zone grise

En offrant à cette communauté une telle liberté sans surveillance, cela offre également la possibilité à n'importe quel trafic de naître. En effet, tout en étant légal, le Dark Net offre l'opportunité au Dark Web d'exister et d'y abriter des activités illégales. Sur l'ensemble du Deep Web, 4 % seraient du Dark Web, donc des activités illégales.
Ces activités sont connues de tous et d'après certains créateurs de Dark Net, c'est le prix à payer contre la surveillance de masse.
Dans le livre[1] The Internet and Business : À lawyer's Guide to the Emerging Legal Issues, publié par The Computer Law Association, il est dit qu'avec une protection optimale de son anonymat il est impossible de retrouver l'identité de quelqu'un sur le réseau.

La criminalité

Des études faites par différentes institutions comme l'Université de Portsmouth explique, bien qu'il ne puisse être prouvé complètement, que 10 % des cybercriminels seraient responsables de plus de 90 % des cybercrimes commis sur le Dark Web.

[1] http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html

Plusieurs types de crimes sont commis sur les Dark Webs. Les plus répandus sont les trafics en général et en particulier celui de la drogue. Un chapitre sera dédié à ce sujet ainsi qu'aux autres crimes du Dark Net.

Les agences de surveillance

National Security Agency

Il existe plusieurs agences de surveillance sur internet, mais la plus connue, et sûrement la plus efficace, est la NSA, la National Security Agency. La NSA est un organe du gouvernement du département de la Défense des États-Unis d'Amérique. Basée dans le Maryland, cette agence se charge d'analyser les échanges d'origine électromagnétique, de la surveillance des systèmes d'information américains et de traiter les données du gouvernement américain.

Cette agence de surveillance a le monopole complet de ce type d'activités et d'analyses sur plusieurs continents et se trouve sous les ordres et la gérance du gouvernement US. WikiLeaks a posté différents documents de la NSA l'impliquant dans des écoutes téléphoniques illégales de centaines de personnes dans le monde. Ces informations ont été prouvées par Edward Snowden qui a dû quitter son pays pour ne pas être interpellé par le gouvernement.
Comme nous l'avons vu dans le tableau expliquant lesquelles de nos données étaient lisibles pendant nos connexions internet, la NSA, par son niveau hiérarchique au sein du gouvernement américain, peut se permettre de récolter des informations sur n'importe quel réseau, depuis n'importe quel point d'accès. Voilà pourquoi des Dark Nets comme Tor permettent d'échapper à cette surveillance systématique.

European Union Agency for Network and Information Security

En Europe, il existe une agence semblable à la NSA, son acronyme, que vous connaissez sûrement si vous suivez ce genre de thématiques, est ENISA. Cette agence se charge de conseiller l'Union européenne en matière de sécurité informatique, de recueillir et d'analyser les données sur le net qui pourraient être dangereuses pour l'Union européenne. Mais la frontière est souvent mince entre analyser les éventuels dangers potentiels et la surveillance du trafic entier sur internet.

Régulations actuelles

Concernant les lois sur les cybernuisances, il en existe finalement très peu, car il est difficile de connaître l'identité d'un cybercriminel ou d'un groupe de cybercriminels. L'anonymat fourni par certains accès aux Dark Nets permet un cryptage de l'information d'une haute qualité.
De ce fait, au moment de la capture d'un cybercriminel, il est de suite privé de connexion vers l'extérieur. De plus, en fonction du criminel et des délits commis, cette privation peut même comprendre toute connexion physique avec un tiers.

Les peines encourues sont des privations de liberté très strictes et longues, dans le but de dissuader les cybercommerces ou les hackers.
La quantité d'argent qui y est blanchi est si grande que les peines de privation de liberté sont souvent même à vie.

Afin de finir cette analyse sur les crimes possibles rencontrés sur internet, il est difficile de ne pas parler des torrents. Ce système d'échange de données, films, séries TV, software et autres, partagées sur un réseau P2P est illégal si vous partagez un tel article, quel qu'il soit, de manière gratuite et que celui-ci est normalement payant. En d'autres termes, c'est légal si votre contenu partagé l'est aussi grâce aux copyrights qui protègent ces articles.
À préciser que vous êtes responsables juridiquement si vous êtes la personne qui propose le service ou celle qui le télécharge.
Vous serez alors dans l'obligation de payer une amende allant de 6'500 CHF jusqu'à 200'000 CHF, et vous risquez jusqu'à 10 ans d'emprisonnement. Ces peines et amendes varient en fonction des pays.

Le Streaming illégal est un autre crime commis sur internet, mais plus compliqué à traiter juridiquement que le torrent. Le streaming est la nouvelle tendance pour visionner des films ou des séries et a, maintenant, pris la place des torrents. En effet, le streaming est plus rapide que le torrent, car nous n'avons pas besoin de télécharger le fichier sur notre disque. C'est en fait notre navigateur qui enregistre le fichier de manière temporaire dans sa mémoire vive. Mais il ne faut pas oublier que visionner un film en streaming est techniquement et juridiquement illégal pour les mêmes raisons que les torrents. Certains sites de streaming, cependant, permettent un abonnement mensuel pour visionner des films ou autres supports, cette procédure est par contre légale.
Il faut noter que dans certains pays, comme l'Inde, le streaming est complètement légal. Comme dernier exemple, la dernière saison de Game of Thrones [2]a été visionnée par 90 millions de personnes autour du globe de manière illégale, ce qui est en fait l'article le plus piraté de l'histoire du Web à l'heure actuelle.

Ces 2 types de crimes sont commis sur le Surface Web, car dû à sa plus grande communauté, les crimes sont plus fréquents

[2] https://news.sky.com/story/police-cracking-down-on-illegal-streaming-as-game-of-thrones-piracy-grows-10988497

Le Deep Web à travers le monde

Le Deep Web est un sujet complexe et souvent mal compris du grand public pour des questions liées à des informations lacunaires, voire régulièrement erronées. De nombreuses fausses informations circulent dans la presse, lors d'émissions de télévision ou internet sans véritable fondement et avec de nombreuses inexactitudes. Beaucoup de confusions règnent donc dans des reportages ou enquêtes traitant du sujet. C'est pour cela que mon travail vise à expliquer l'intégralité de ces différents points de manière compréhensible pour démystifier ce sujet et sa réputation souvent sabotée par différents médias.

Comme déjà expliqué dans les chapitres précédents, le Deep Web et l'utilisation des Dark Nets sont légaux tant que les activités pratiquées le sont également. En effet, l'utilisation du Deep Web se fait souvent sans même que l'on ne s'en rende compte et le Dark Net, de par son anonymat, est le meilleur moyen d'éviter un « espionnage » de masse contrôlant le Surface Web. Il est à noter que sur le Surface Web nous constatons plus d'activités illégales que sur le Dark Net dû, simplement, à son nombre d'utilisateurs beaucoup plus grand. D'ailleurs tout le monde connaît un collègue ou un ami s'étant fait abuser par une fausse annonce sur internet. Le danger est donc partout et nulle part à la fois, tout dépend, finalement, de notre manière d'utiliser le Web.

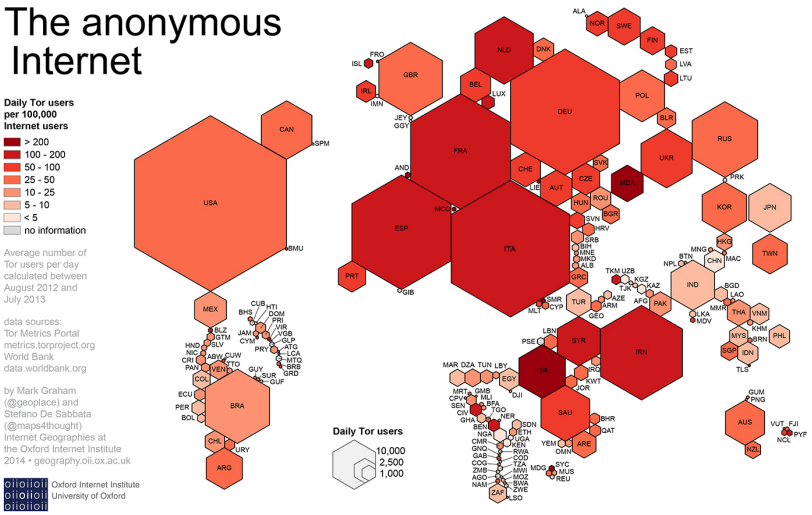
Comme nous avons pu le voir, de nombreuses personnes, ou groupes de personnes utilisent quotidiennement le Deep Web ou les Dark Nets ; nous avons évoqué les forces militaires de nombreux pays, certains professionnels spécifiques ou encore les lanceurs d'alertes. Mais ce ne sont de loin pas les seuls utilisateurs, car beaucoup d'entre eux sont également des personnes ordinaires comme vous et moi ! L'utilisateur lambda est présent souvent plus par inadvertance que par choix.

L'aspect marketing est très important, car il est présent partout sur les réseaux. Il faut savoir que l'analyse systématique des données des utilisateurs permet par la suite d'anticiper vos prochains achats ou vos prochaines envies, pouvant même vous pousser à acheter des articles dont vous n'avez pas besoin (pouvant parfois même être dangereux pour votre santé). Les analyses de vos données en disent long sur vous, votre mode de vie et votre manière de fonctionner. De plus, la confidentialité de ces données n'est généralement pas respectée ni vraiment réglementée, sur le Web.

Afin de ne plus subir ce marketing régulier, ces nombreuses publicités sont présentes partout, et de conserver vos données personnelles comme telles, beaucoup d'utilisateurs choisissent d'accéder au Dark Net pour leurs navigations sur internet qui, je le redis, est très souvent tout à fait légal. Se rendre sur le site 20minutes.ch via Google Chrome où Tor sont deux actions, en termes juridiques, parfaitement légales.

L'utilisateur lambda est beaucoup plus présent qu'on ne le pense. Partout dans le monde, de nombreuses personnes l'utilisent.
Voici une carte montrant les utilisateurs anonymes journaliers sur le Web

Figure 23 : Carte du monde indiquant les plus gros utilisateurs de Tor



Les USA sont les plus nombreux, ceci est probablement dû au fait qu'à l'origine ils sont les créateurs du projet TOR. En Europe, le navigateur Tor est aussi présent et régulièrement utilisé. Dans certaines régions d'Afrique ou d'Asie, la censure de l'internet est très présente et bloque l'accès à l'information. En revanche, grâce à Tor, ces régions peuvent y avoir accès. Le nombre d'utilisateurs n'est pas très élevé, dû au manque d'information sur « l'accès au Dark Net afin de contourner la censure » dans certaines régions. Le meilleur moyen de rendre Tor plus accessible est de le rendre plus sûr et vice et versa. Plus il y a de gens qui utilisent Tor plus vous êtes difficile à tracer. En rendant Tor plus accessible dans ces régions, la liberté de l'information trouvera un moyen d'augmenter.

Comment contrôler le Deep Web

La justice ne possède que très peu de lois concernant le monde de la cybercriminalité du fait qu'il est extrêmement complexe de démasquer la vraie identité des responsables. La plupart du temps, derrière un compte utilisateur relié à un accès aux réseaux, peuvent se cacher plusieurs utilisateurs. Cependant, en arrêtant une personne utilisant un compte, il est juridiquement possible de l'inculper des crimes commis par cette identité virtuelle.

Techniques

Il s'avère être toutefois compliqué pour la police de mettre la main sur l'identité d'une personne à l'intérieur des Dark Nets et, pour ce faire, la police a besoin d'être très active sur les Dark Nets en question. Avec l'aide de plusieurs spécialistes du domaine IT, la police a, cependant, plusieurs manières de procéder.

La première technique est de se rendre sur Tor et de se poster en tant que vendeur sur un cybermarché (nous parlerons plus en détail des cybermarchés dans le chapitre suivant). Pendant une durée fixée au préalable avec un juge, un policier se chargera de récolter les demandes d'achats, d'entrer en contact avec l'acheteur et de conclure un lieu de livraison ou l'acheteur, finalement, se fera arrêter. En effet, l'anonymat offert par Tor peut aussi devenir un avantage pour la police du fait qu'on ne connaît jamais vraiment son réel interlocuteur.

Une seconde technique est le « hack » d'une plateforme, d'un forum ou d'un chat sur un Dark Web. Pour ce faire, la police doit trouver une erreur dans la structure du site afin de trouver la location de l'administrateur. Ceci est certes une tâche complexe, mais pas impossible non plus. Le FBI a, par exemple, pu trouver une faille sur le site pédopornographique Playpen et mettre en place un malware, un programme-espion, qui révéla l'adresse IP des personnes « cliquant » sur le site. De fait, le site a pu tourner sous le contrôle de la police durant un mois.

Un autre moyen de démasquer un utilisateur du Dark Web peut se réaliser depuis la Surface Web. Cette méthode est appelée le « Creative Googling ». Elle consiste à chercher sur le Surface Web des personnes faisant la promotion d'un Dark Web. Un utilisateur régulier d'un cybermarché s'est fait repérer via sa vraie adresse IP sur le forum d'un site de bitcoins.

Un autre exemple concret nous montre qu'en Angleterre, deux départements de la sécurité du Web se sont associés afin de mettre en commun leurs informations concernant les crimes pédopornographiques. La création d'une entité passive fut nécessaire afin de récolter et analyser des informations sur le trafic d'un domaine très spécifique et d'une taille restreinte d'un crime commis sur le Dark Net. Ceci permet donc un espionnage massif des données, mais reste, par contre, une technique très compliquée à mettre en place.

À préciser que souvent, lors de la capture d'un cybercriminel, les policiers chargés de l'affaire vont aller dans les données du cybercriminel pour trouver des preuves supplémentaires permettant d'inculper d'autres utilisateurs.

Une dernière technique significative est la mise en place d'une collaboration avec les systèmes postaux d'un pays donné. En effet, avec l'aide de la poste il est facile de savoir qui a commandé tel ou tel produit et connaître également des adresses de destinataires. Nous reviendrons sur ce sujet dans le chapitre du transport.

Il y a heureusement plusieurs exemples de succès face à la cybercriminalité. Nous pouvons citer celui de la police australienne[3] qui a réussi à « hacker » un forum de pédopornographie et prendre la place de l'administrateur durant l'échange de photographies entre les différents utilisateurs du forum. De fait, elle a pu démasquer la plupart de ces derniers et les arrêter pour crimes sexuels sur enfants.

[3] https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web

Un autre exemple est celui de la police hollandaise[4] qui a « hacké » le site Web AlphaBay.onion, un des cybermarchés de la drogue les plus utilisés avant sa capture et fermeture. Au moment de la prise du site, la police a automatiquement bloqué le site durant quelques heures, puis l'a rouvert. La communauté du site s'est tout de suite interrogée sur la raison de cette fermeture et de nombreux utilisateurs ont cherché à savoir pourquoi (certaines de ces conversations sont visibles sur des forums du Surface Web). De fait, la police hollandaise avait fermé le site sur la plus courte durée possible afin d'y placer un programme-espion qui révéla par la suite la vraie adresse IP de l'utilisateur. Durant un mois, la police hollandaise a pu localiser les adresses de plus de 500 utilisateurs sur le territoire hollandais.

Sanctions

Les sanctions dépendent de plusieurs facteurs comme celui de l'utilisateur, du vendeur, de l'acheteur ou de l'administrateur du site, mais également de la quantité saisie/répertoriée. Si la police met la main sur un administrateur d'un Dark Web, celui-ci recevra une très forte amende et sera inculpé pour complicité de crime organisé et d'association à un réseau de malfaiteurs. Il sera jugé pour ses crimes et risquera au minimum une amende, mais également, en fonction de la gravité du crime, de la prison.

Pour un vendeur, tout dépendra de la marchandise ou du service vendus. Cela peut varier entre trafiquant de stupéfiant, receleur, contrebandier, etc. Un autre facteur aggravant est la « quantité » du/des produits trouvés chez les cybercriminels. Cela est toujours accompagné d'une forte amende et d'un risque d'une peine de privation de liberté.

Enfin pour un acheteur, il sera également amendé en fonction de la quantité achetée et du genre de marchandise concernée. La quantité permettra à la police d'en déduire s'il s'agit d'un simple utilisateur ou d'un trafiquant qui se fournit sur le Dark Web. Pour un utilisateur, la sanction peut aller également jusqu'à la privation de liberté dans certains cas et certains pays.

Il est possible que la police utilise un criminel, avec ou sans son consentement, afin de remonter des filières ou localiser les hauts responsables d'un trafic.

[4] https://thenextweb.com/insider/2017/07/20/police-fbi-drug-dark-web-market/

Les cryptomarchés

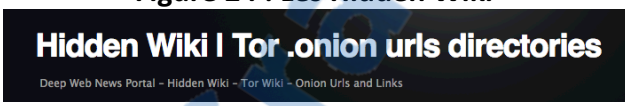
Les Dark Webs proposant des biens et/ou services illégaux sont de vraies plaques tournantes de trafics en tout genre.

Prenons l'exemple de la recherche d'un cryptomarché spécialisé dans la vente de drogue. Il existe deux moyens de le localiser. Le premier consiste à se renseigner via des forums ou auprès d'une communauté donnée. Ceci n'est pas aisé, car ces informations restent souvent confidentielles et ne sont pas divulguées si facilement.

Le second moyen et de se rendre sur les « Hidden Wiki ». Il s'agit d'une page Web accessible depuis le Surface Web et proposant des sites avec le nom de domaine « onion ». N'importe qui peut la mettre à jour à condition d'y être inscrit et d'en posséder les droits d'écriture. Cependant, votre navigateur ne vous permettra pas d'ouvrir les liens sans utiliser le navigateur Tor, ce que le site vous propose alors de télécharger.

Les « Hidden Wiki » sont un moyen efficace pour trouver des Search Engin, moteurs de recherche pour le Dark Web : Comme exemple nous avons « Grams », qui a d'ailleurs repris la même typographie que Google, qui est une Search Engin reconnue pour les cybermarchés de la drogue.

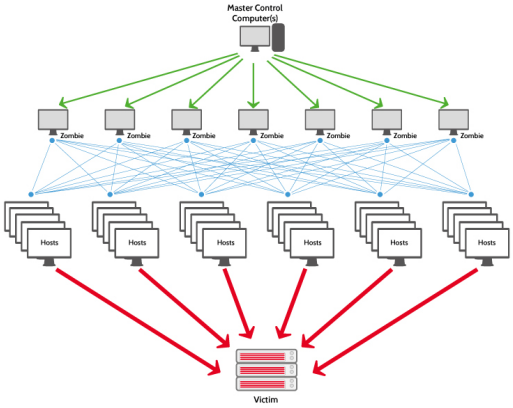
Figure 24 : Les Hidden Wiki



Il faut savoir encore que les cybermarchés ont des durées de vies plus ou moins courtes. En effet, beaucoup de ces Dark Web se font fermer, soit principalement par la police, soit par une cyberattaque d'un site concourant ou encore, dans certains cas, par des activistes. Ces hackers du bien sont appelés des « White Hat Hacker ». Certains d'entre eux ont réussi à faire fermer des sites pédopornographiques.

Le business de la pédopornographie est un réel problème pour la police, mais aussi pour la communauté des Dark Nets. En effet, le Dark Web contient un pourcentage très faible de ce type de sites, mais reste un crime absolument horrible pour l'ensemble des personnes en dehors de ce cercle. Là aussi, ces sites se font régulièrement fermer par des activistes procédant par des attaques DDoS. Ce procédé fonctionne lorsque l'attaquant se connecte à plusieurs postes sur le Dark Net et submerge de requêtes le serveur contenant les données jusqu'à le faire « crasher ». Il est à préciser que les sites qui se font « crasher » ou fermer peuvent être rouvert sous un nom de version différent, ou via l'ouverture d'un site similaire, seulement quelques heures ou jours après.

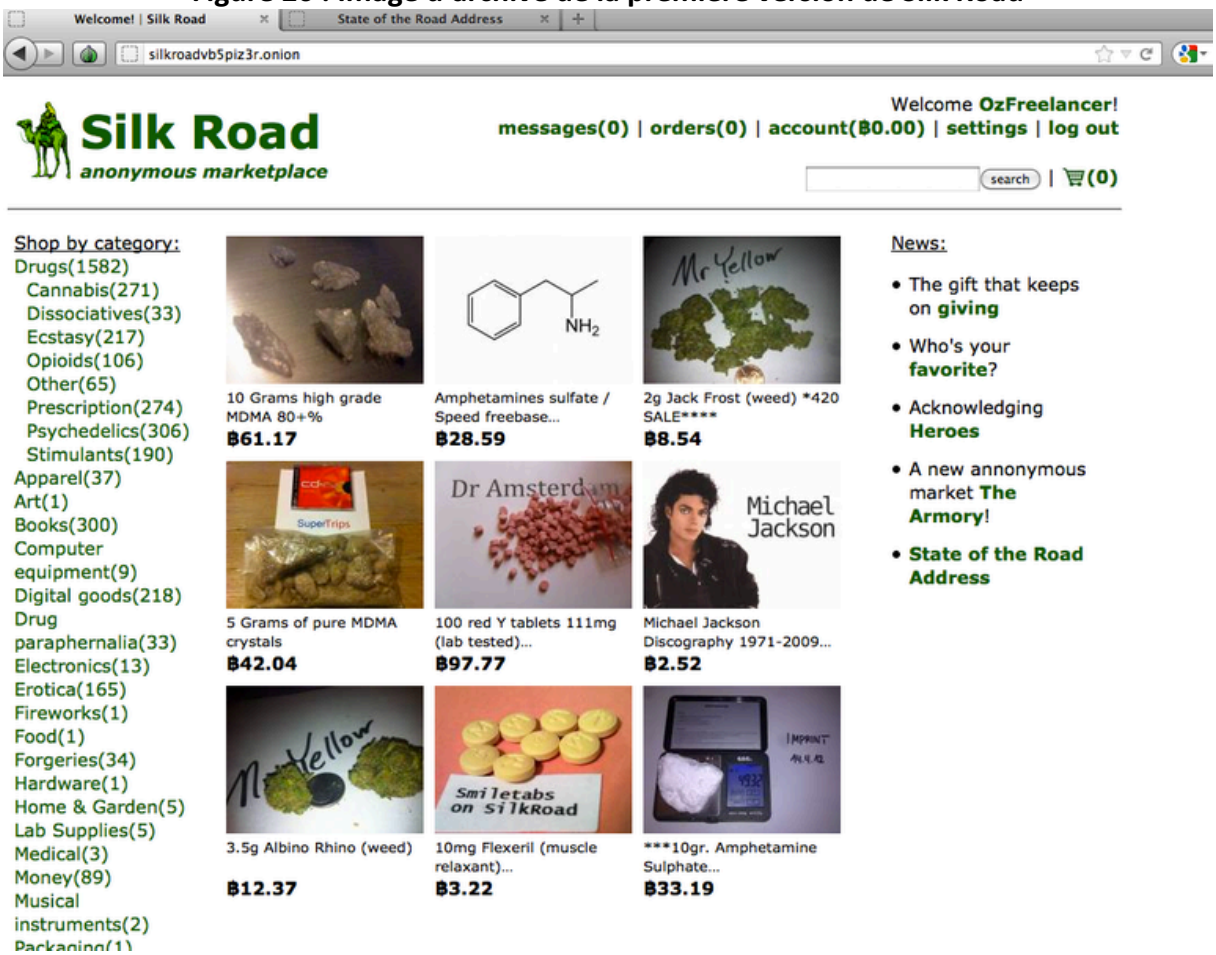
Figure 25 : Déploiement d'une attaque DDoS



Description

Un cryptomarché est un site du Dark Web où l'on peut acheter des biens et services qui peuvent être souvent illégaux. Visuellement ce type de marché ressemble fortement à un site par exemple Amazon. On y trouve des menus déroulants, une barre de recherche et des articles en promotion. Sur ces sites nous avons des vendeurs inscrits qui proposent leur marchandise. Les photographies des produits sont de bonne qualité et les produits souvent également. En effet, les cybermarchés sont accompagnés, comme les autres, d'un système de forum où les utilisateurs laissent des commentaires sur les vendeurs, la rapidité de la livraison et sur la qualité des produits. Il est même possible de noter les vendeurs avec un système composé d'étoiles. Ce qui veut dire que sur le Dark Web, tout se joue sur la confiance, car les possibilités de se plaindre en cas de litige n'existent quasiment pas ?

Figure 26 : Image d'archive de la première version de Silk Road



C'est pour cela que ce système de notations des vendeurs est pris très au sérieux. Il permet de définir si le vendeur est fiable, si ses produits ne sont pas dangereux et de bonne qualité. Cette notation crée donc la réputation du vendeur sur le site, sachant que l'offre est beaucoup plus importante que la demande, il est donc important d'avoir une réputation de vendeur de qualité si l'on ne veut pas perdre des clients. Avant d'acheter sur un cryptomarché, vous devez entrer en contact avec le vendeur, afin de créer un lien de confiance avec lui, mais aussi pour décider de l'adresse de réception du colis et un compte Bitcoin pour y verser l'argent.

Tous les utilisateurs ont un niveau dans le site, de 1, l'utilisateur débutant/nouveau, allant jusqu'à 10, le créateur. Cette évaluation offre un certain niveau de confiance dans la communauté et permet plus facilement la résolution de problèmes éventuels.
Certains vendeurs ont bien essayé d'utiliser des produits moins chers pour la conception de drogues de synthèse mettant en danger la vie des utilisateurs, mais ce type de comportements est tout de suite signalé par la communauté qui permettra à l'administrateur de l'exclure du site.
L'origine des produits est aussi un critère de sélection et est notifiée dans les descriptions générales de l'offre.
Les produits les plus vendus sur le Dark Web sont les drogues, et tout particulièrement :

- Le cannabis et ses dérivés
- Les stimulants, comme la cocaïne
- Les variantes de la MDMA, comme l'ecstasy

Des chercheurs ont estimé les ventes de 2016 sur le Dark Web concernant les drogues entre 15 à 20 millions US dollars par mois, dont plus de 5 millions aux USA. En Europe, les plus gros vendeurs sont l'Angleterre, l'Allemagne et la Hollande.

Silk Road

En 2011 Silk Road voit le jour et devient très vite le 1er cybermarché où se réunissent vendeurs et acheteurs dans le but de vendre/acheter des drogues. Silk Road a été renommé l'eBay de la drogue.
Son créateur est seulement connu sous son pseudonyme DPR ou « Dread Pirate Roberts » en hommage au personnage principal de la nouvelle de William Goldman « The Princess Bride ».

Silk Road a été créé avec une philosophie bien particulière. Son auteur anonyme n'a pu être interviewé que par certains journalistes par email. Il s'agit d'une Soft Platform, où tous les biens et services ne figurent pas. Par exemple, la pédopornographie et les hommes de main ne sont pas des articles disponibles sur ce site.
Le but de Silk Road était de fusionner Tor et son anonymat sur le réseau avec des transactions réalisées en bitcoin, sujet que nous traiterons par la suite.

Le créateur de Silk Road prouve donc qu'il est possible de créer un système économique viable sans faire recours à aucune banque, ni surveillance ou taxe gouvernementale. Il démontre, d'une certaine manière, qu'un système parallèle à notre économie, telle que nous la connaissons, est bel et bien possible et peut même s'autogérer.

La philosophie de Silk Road veut s'opposer aux codes, pour se concentrer sur les droits de l'Homme, et sur une certaine liberté. Bien conscient que tout cela est illégal, mais pour la vision de DPR, ceci n'est que « secondaire ».

Au fil des années, les personnes utilisant le compte de DPR augmentent, car la plateforme prend des proportions énormes et l'administration en devient difficile. Tous les autres utilisateurs sont des personnes de confiance du « créateur », souvent des activistes épousant la même cause.
En 2013, le FBI a exécuté une attaque DDoS sur le serveur de Silk Road et l'a fait crasher. À ce moment précis, la police a pris le contrôle du site et l'a complètement stoppé.

La police affirme avoir trouvé l'adresse IP réelle du serveur par une faille de sécurité dans le CAPTCHA permettant d'identifier si nous sommes un robot d'indexation. Cependant d'autres pensent qu'il s'agirait plutôt d'un hack illégal réalisé par la police sur le serveur PHP en y modifiant la requête afin d'y recevoir des informations sur l'utilisateur.

La police a réussi à remonter jusqu'à Ross Ulbricht, un homme accusé d'être le créateur et le propriétaire de Silk Road, et d'être l'utilisateur DPR. Cependant le compte de DPR était toujours actif après la capture de Ross Ulbricht.
Beaucoup de zones d'ombre planent sur cette affaire, d'autant plus que M. Ulbricht a reçu une peine de privation de liberté à vie pour avoir été accusé de blanchiment d'argent, d'être à la tête d'un organisme criminel, impliqué dans des trafics de narcotiques et responsable de la mort de 3 hommes sur contact. Alors que la police est accusée d'avoir « hacké » un serveur sans mandat afin d'attaquer le serveur de Silk Road. Ceci fut un réel choc aux USA où la population commence à douter sur ce que la police du Web est réellement capable de faire sans mandat pour trouver des preuves.

Quelque temps après, Silk Road a rouvert et s'appelle maintenant Silk Road 3, le concept est le même.

Autres cryptomarchés

Bien évidemment, il existe un grand nombre de cryptomarchés, les plus connus actuellement sont Silk Road 3, Dream Market, Ramp (Russian Anonymous Market Place), Valhalla, et j'en passe. Certains cryptomarchés demandent l'autorisation d'un administrateur afin de valider l'inscription d'un nouvel utilisateur. Dans chaque pays il y a ces marchés noirs connus. Il est vrai qu'il est souvent plus intéressant d'éviter les douanes pour de multiples raisons, de fait la possibilité de trouver un cybermarché dans son pays est un réel moyen de limiter les risques de se faire prendre par la police. Les douanes sont considérées comme des zones à risques pour les colis.

Systèmes de paiements

Après avoir démontré comment il est possible d'être en quelque sorte « invisible » sur internet nous allons maintenant expliquer comment il est possible de payer pour des biens ou des services illégaux sur internet sans que la police, y compris la police financière, puisse retracer les transactions. Pour ce faire, nous allons évoquer un élément central dans les systèmes de paiement : le Bitcoin. Ce dernier, combiné à Tor, rend les transactions invisibles. Cette cryptomonnaie est l'une des méthodes de paiement les plus sûres et les plus utilisées dans de très nombreuses transactions sur le Dark Web.

Bitcoin

Le Bitcoin est une cryptomonnaie, basée sur un système P2P, permettant de réaliser des achats sur internet. L'unité de cette monnaie est le « Bitcoin » et la quantité en est limitée, 21 millions Bitcoin pour être précis. Cette monnaie est divisible jusqu'à huit décimales. La technologie de la Blockchain y est incorporée. En effet, toutes les transactions faites en Bitcoin sont enregistrées par les nœuds du système, y compris les autres utilisateurs, dans un dossier public. Grâce à cette méthode, il est impossible de falsifier une transaction ou le montant de nos transactions en Bitcoins.

Le point fort de cette monnaie est son « indépendance ». Du fait qu'elle est décentralisée, sans aucune autorisation bancaire et sans administrateur unique, c'est l'ensemble des utilisateurs qui la rend sûre. Chaque transaction est en quelque sorte validée par la communauté des utilisateurs avant d'être traitée comme telle.
Le Bitcoin, comme le Deep Web, souffre de la liberté qu'il offre. En effet, par la discrétion qu'offre le Bitcoin, comme moyen de paiement, beaucoup de transactions concernant des biens et services illégaux sont réalisées à l'aide de cette cryptomonnaie, et la plupart du temps également sur le Dark Web bien entendu. Certains politiciens accusent donc le Bitcoin de favoriser le blanchiment d'argent.

Paradoxalement, le Bitcoin est un système de paiements de plus en plus accepté dans certains pays et totalement illégal dans d'autres. Par exemple, on peut s'en procurer à la gare de Cornavin en Suisse à Genève alors que cette monnaie est totalement illégale en Russie ou en Thaïlande. En France et aux USA, le débat est, à ce jour, toujours ouvert.
Sur internet il est par contre totalement légal de payer avec des Bitcoins si le vendeur et l'acheteur s'accordent sur ce mode de paiement.

Le Bitcoin n'est pas une monnaie alternative, mais une cryptomonnaie. Cela signifie que le Bitcoin n'est relié au cours d'aucune autre monnaie. Il n'est donc pas soumis au contrôle d'un quelconque système bancaire ou régulateur des changes. Son taux est flottant et varie en fonction du marché des changes, il s'agit du deuxième plus gros marché financier après celui des taux d'intérêt.
Les transactions sont enregistrées dans des fichiers et analysées environ toutes les 10 minutes par des ordinateurs sur la base des nœuds participant au fonctionnement de cette monnaie.
La monnaie est cryptée afin d'éviter les falsifications de Bitcoin. La création de cette monnaie virtuelle se fait à l'aide d'un code émis par un algorithme.

Figure 27 : Évolution du Bitcoin depuis sa création

Il est difficile de prévoir le futur du Bitcoin. En effet, contrairement aux monnaies traditionnelles, celui-ci ne risque pas de souffrir de l'inflation. Cependant, la quantité de Bitcoins étant déjà fixée par le programme, il est vulnérable à la déflation. De plus, sa très forte volatilité peut causer un problème. Ce dernier est présenté par son créateur comme une expérience économique ouvrant la question sur la possibilité de réinstaller un nouveau système de libre arbitre monétaire.

Fonctionnement

Pour utiliser le Bitcoin, il suffit de télécharger, sur le support de notre choix, une application permettant de gérer des Bitcoins. Une fois sur le réseau, nous pouvons créer un ou plusieurs comptes qui nous permettront de verser nos Bitcoins à d'autres utilisateurs. Ces fonctionnalités sont réalisées par des Wallet. Les transactions sont réalisées par la Blockchain permettant d'assurer leur validité. Les fichiers regroupant toutes les transactions sont lisibles par tous les utilisateurs, mais sans pouvoir y apporter des modifications.

Wallet

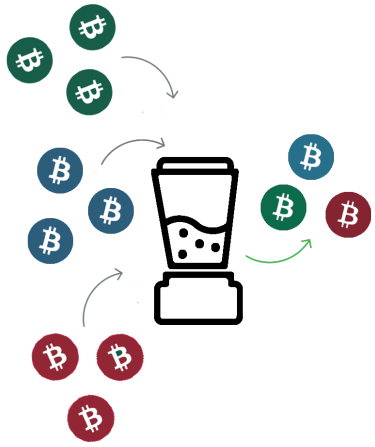
Les Wallets sont des applications qui regroupent toutes nos informations personnelles comme nos différents comptes de Bitcoin. Ces applications sont disponibles sur tout type de support et permettent de consulter nos comptes et réaliser des transactions (verser et recevoir donc des Bitcoins). L'accès aux comptes Bitcoin du Wallet se fait grâce à la vérification d'une clé publique par une clé privée.
La procédure pour la mise en place de ceci est simple.
Il nous faut nous inscrire sur un site permettant l'obtention d'un Wallet, comme sur coinbase.com par exemple, puis acheter des Bitcoins sur ce même site ou un autre proposant cette monnaie. Par exemple, à la gare Cornavin à Genève il existe la possibilité d'acheter des Bitcoins via les bornes à billet de train qui nous impriment 1 QR code qu'il faut ensuite scanner avec notre Wallet.
Pour vendre des Bitcoins, le procédé est exactement similaire, via un même site d'achat il est possible de les vendre également. L'argent est directement versé sur un compte PayPal.

Comment payer de manière anonyme

Quand nous sommes en possession de Bitcoin et que nous exécutons une transaction depuis notre Wallet en faveur d'un autre utilisateur la transaction est inscrite dans un fichier qui est partagé sur le réseau, tel est le fonctionnement de la Blockchain. Dans le but de rendre cette transaction anonyme, il existe plusieurs moyens très efficaces.

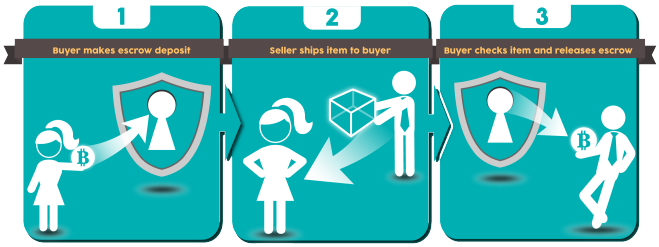
Le premier moyen est appelé Bitcoin Tumbler, ou Bitcoin Mixer. Cela fonctionne comme un « pot commun ». Plusieurs utilisateurs versent une certaine somme d'argent dans ce mixer et seul l'administrateur connaît les dépositaires et combien ils ont versé de Bitcoins. Au moment de payer, vous devez donc verser vos Bitcoins sur un site tel que Bitmixer.io ou Helix by Grams en spécifiant précisément à qui ils sont adressés. Le Mixer va donc prendre la somme de Bitcoins du pot commun pour réaliser la transaction sans vérifier à qui ils appartiennent. C'est là, précisément, où réside donc l'anonymat de la transaction pour l'émetteur. Du côté du destinataire, les Bitcoins qu'il recevra proviendront donc là aussi de différentes personnes émettrices rendant ainsi impossible l'identification du réel acheteur ? Le prix de ce « service » varie en fonction du montant de l'argent déposé dans le pot commun.

Figure 28 : Illustration du Bitcoin mixer



Un second moyen assurant l'anonymat est celui impliquant l'intervention d'un Escrow. Il s'agit d'une personne tierce, souvent un serveur, qui va avertir le vendeur quand l'acheteur aura déposé l'argent. De ce fait, une fois l'argent versé sur le compte Bitcoin du vendeur l'envoi d'une commande par exemple pourra alors être exécutée. L'Escrow est un moyen sûr pour les 2 parties prenantes de la transaction et particulièrement discret étant donné que le versement est fait par un serveur. Le prix de ce « service » varie en fonction du montant échangé.

Figure 29 : Illustration du système Escrow



Le transport

Concernant le transport des marchandises achetées/vendues sur le Dark Web, il se doit d'être d'une discrétion optimale. En effet, à quoi bon être « non traçable » lors de la transaction proprement dite si nous pouvons nous faire repérer lors du processus de livraison ou à la réception du colis. Afin d'éviter ceci, une marche à suivre très précise est mise en place au moment où l'acheteur entre en contact avec le vendeur. L'acheteur fournit donc une adresse où il veut être livré. Le plus souvent les utilisateurs du Dark Web choisissent des points relais, à savoir des magasins ou autres types d'enseignes acceptant de réceptionner des lettres et colis comme le fait la poste. Le colis est alors emballé par le vendeur de manière à ne laisser paraître aucune odeur ou autre forme suspecte. De plus, dans certains cas des poids peuvent y être ajoutés afin de ne pas rendre une grande boîte trop légère suspecte. Le paquet doit donc ressembler finalement à paquet type, avec un poids « adéquat » et de forme « normale ».

La poste n'est pas un problème en tant que tel, car son mandat l'oblige à transporter les colis sans répertorier leurs contenus, le contenu du paquet étant sous la responsabilité de la personne qui expédie le colis. Le réel problème du transport est les douanes. En effet, ces zones sont soumises à de nombreux contrôles qui peuvent mettre « en danger » le contenu d'un paquet.

Il est donc plus sûr de procéder à des commandes sur le Dark Web de son propre pays et de s'y faire livrer afin d'éviter de passer une douane et compromettre la livraison

L'impact du Dark Web sur notre économie

Comme nous l'avons vu précédemment le Dark Web offre la possibilité d'acheter et de se faire livrer des biens ou services des plus variés et ceci dans la plus grande discrétion si nécessaire. La liberté offerte par Tor et les divers moyens de paiements existants sur le Dark Web ont permis de créer une véritable économie parallèle à celle que nous connaissons et utilisons fréquemment sur le Web. Bien que souvent illégales les ventes se multiplient chaque année. En 2016, les ventes sur le Dark Web auraient avoisiné les 20 millions USD par mois, biens et services confondus.

Les marchés

Il est relativement facile de trouver ce que l'on cherche sur le Dark Web grâce au Hidden Wiki ou en indiquant le nom d'un cybermarché dans un forum ou encore simplement en discutant avec d'autres utilisateurs intéressés par des services similaires et cela même sur le Surface Web directement.
Il existe de très nombreux marchés souvent spécialisés dans un type de bien ou de services bien précis. Nous allons analyser chacun d'entre eux afin de comprendre qui en tire le plus grand profit ainsi que d'en connaître leur véritable impact sur notre économie en général.

Les drogues

Le marché des drogues est le plus fréquenté par les utilisateurs du Dark Web. En effet, due à la complexité d'acquérir de la drogue, dans la plupart des cas, due à son illégalité, il est plus sûr pour le consommateur de passer par internet que de se rendre directement auprès de revendeurs dans la rue.

Nous allons séparer cette thématique en 2 parties :

- Les drogues douces
- Les drogues dures

Cette différence est importante à notifier, car le niveau d'illégalité varie en fonction des drogues concernées, douces ou dures, et en fonction des pays dans lesquels on se trouve.

Les drogues douces

Dans la catégorie des drogues douces, nous trouvons par exemple le cannabis, le haschisch, la cire de cannabis, le pollen et tous les autres dérivés du THC ou du CBD (tétrahydrocannabinol et le cannabidiol). Le THC et le CBD sont les deux principales molécules que les consommateurs de drogues douces recherchent en général.
Un simple exemple montre que les transactions concernant la Marijuana représentent à elles seules environ 55 % des transactions liées à la drogue réalisées sur le Dark Web. Il est à noter que dans certains pays comme l'Espagne, les Pays-Bas, certains états des USA ou encore en Uruguay, la vente et la consommation de cannabis sont légales. Dans d'autres pays, elle peut être tolérée principalement pour des raisons médicales et sur présentation d'une ordonnance. Par contre dans de nombreux autres pays les drogues douces sont totalement illégales. Prenons l'exemple des Philippines où un trafiquant de cannabis, ainsi qu'un simple consommateur, peuvent finir leurs jours en prison.

Concernant les pays qui permettent légalement la consommation de Marijuana, cette dernière n'est pas sujette à de nombreuses transactions sur le Dark Web. En effet, il est préférable pour tout le monde de se rendre dans des magasins spécialisés et contrôlés par des professionnels que de passer par un inconnu sur le Web et de prendre le risque d'être soupçonné de trafic sur internet. L'État y gagne aussi, car il a la possibilité de fiscaliser, via une taxe (un impôt), les ventes de drogues douces sur son territoire. L'impact du Dark Web est donc minime concernant les pays ou la légalisation de ces substances a été adoptée. Par contre, pour les pays sans légalisation des drogues douces l'impact sur le Dark Web est comparable à celui des drogues dures.

Les drogues dures

Dans la catégorie des drogues dures, nous retrouvons tout type de stimulant et autres drogues de synthèse. En d'autres termes, la différence entre les drogues douces et dures est que les premières sont créées de manière « naturelle » alors que les secondes sont réalisées par l'Homme et le plus souvent dans un laboratoire.
Nous y trouvons par exemple des drogues comme la cocaïne, la MDMA, l'ecstasy, la méthamphétamine, l'héroïne, l'opium et tout autre psychotrope.
Ce marché représente environ 45 % des cryptomarchés de la drogue. Ces drogues sont interdites partout dans le monde, mais sont souvent accessibles en quelques clics sur le Dark Web.

Après avoir effectué plusieurs recherches sur ce thème, la conclusion montre que l'impact économique est énorme, mais qu'il va au-delà des revenus liés simplement à la drogue.
La vente de stupéfiants n'étant pas légal il est plus difficile de mesurer les impacts économiques directs et indirects.
Qui sont donc les véritables gagnants ? D'après le témoignage d'un agent de la police de New York, qui parlait de ce phénomène lors d'une interview récente, le trafic de drogue sur internet est certainement plus sûr pour les consommateurs et les trafiquants, mais également pour la police elle-même. On ne compte, en effet, plus le nombre d'agents de police morts lors d'interventions qui tournent au bain de sang pour piéger des trafiquants.
Les dégâts humains causés par le trafic de rue sont terrifiants, car les trafiquants, très souvent armés, n'hésitent pas à tirer sur la police tant les sommes d'argent concernées sont importantes et le risque de finir, aux mieux, en prison bien réel.

À l'inverse, sur internet il n'y a pratiquement pas de contact « physique » entre le vendeur et l'acheteur, ce qui crée donc une certaine sécurité pour les deux parties. De plus, cette relative absence de violence correspond mieux à la majorité des consommateurs qui ne sont pas, pour la plupart, des membres de gangs ou autres groupes violents. De plus, de nombreuses enquêtes tendent à montrer que la qualité des produits trouvés sur internet est généralement meilleure que celle des substances rencontrées dans la rue. Des analyses effectuées par la police de New York lors de l'interview ont montré que pour 1 gramme de cocaïne trouvé dans la rue au prix de 80-100. – CHF, le produit était souvent constitué de 60 % de cocaïne pure, le reste étant d'autres molécules anesthésiantes, souvent du paracétamol, alors que pour 1 gramme de cocaïne trouvé sur le net au prix de 50.- CHF le produit contenait un taux de 90 % de cocaïne pure.

En terme économique, l'industrie de la drogue est une réelle mine d'or. Au-delà des millions échangés dans le trafic même de la drogue, il ne faut pas ignorer l'impact économique généré en lien à la lutte de ce fléau. De nombreuses sociétés et entreprises privées sont investies dans ce marché très lucratif (matériel de police, véhicules blindés, laboratoires d'analyses, spécialistes en tout genre). Si une partie de ces activités est prise en charge par les États, les sous-traitances via des sociétés privées sont très fréquentes également. Les retombées économiques sont donc bien réelles pour un nombre important d'acteurs légaux.

Les armes

Les marchés d'armes sur le Dark Web sont une menace bien réelle. En effet, il est possible de se procurer n'importe quel type d'articles tels que pistolets, fusils d'assaut, bazookas, gilets pare-balles, munitions et armes blanches du plus petit couteau de poche jusqu'au grand Katana de Samouraï. Ces armes sont souvent récupérées dans les pays en guerre, principalement volées, puis revendues sur les cryptomarchés. Certaines d'entre elles ne sont même pas autorisées à l'achat au grand public, étant considérées comme des armes de guerre.

Il est aussi possible de trouver, par exemple, des armes autorisées dans son propre pays comme un revolver standard pour 900 USD, mais également un Sniper avec tous les accessoires pour 2'500 USD

Il y a 2 types de commerces qui sont principalement actifs dans le marché des armes légales, il s'agit de la chasse et des sports armés (le tir par exemple). Ces deux activités demandent l'obtention d'autorisations pour leur pratique, ce qui rend donc ces armes difficiles d'accès.

La possession d'armes et leurs utilisations sont généralement illégales sans la possession d'un permis, même si les législations varient beaucoup d'un pays à l'autre (les USA par exemple). La police lutte donc farouchement également contre ce trafic, car l'acquisition d'armes de manière illégale sur son territoire est une réelle menace pour sa population (terrorisme et banditisme).

L'envoi de ce type de marchandise est complexe, mais, paradoxalement, se fait aussi par la poste. Le vendeur va d'abord désassembler l'arme en question pour l'envoyer en plusieurs paquets afin d'assurer un maximum de discrétion sur son envoi.

Ceci permet aussi de passer à travers de nombreux contrôles, y compris des rayons X des postes et des douanes, car les pièces sont dissimulées dans une boîte de jouet.

Il se peut aussi que l'arme soit trop grande pour passer directement par la poste en une seule fois, il est alors réalisé une livraison Dead Drop. En d'autres termes, le vendeur et l'acheteur se retrouvent dans un endroit ou l'échange peut s'effectuer.

Les médicaments

Il existe des sites sur le Dark Web spécialisés dans la vente de médicaments et de matériel paramédical. Ces sites permettent l'acquisition de médicament sans ordonnance, du matériel pour les machines à oxygène et de nombreuses autres substances chimiques. Assez logiquement, les médicaments les plus prisés sont les antidépresseurs tels que le Xanax, les psychostimulants comme la Ritaline ou les antidouleurs comme la morphine. Ces médicaments, avec une utilisation peu rigoureuse et peu d'informations sur leurs effets, et leurs effets secondaires peuvent causer la mort ou de graves dommages.

De plus, cela génère une libre circulation de médicaments qui requièrent normalement une ordonnance et un contrôle pour les obtenir. Ces médicaments sont donc utilisés sans information quant à leur dosage, leur périodicité et sans savoir non plus s'ils répondent vraiment aux symptômes du malade. La vente de médicaments dans un pays doit être régulée par le gouvernement et les ventes doivent se faire dans les lieux commis à cet effet, comme les pharmacies. De plus, aucune mention n'indique s'il n'y a pas incompatibilités avec d'autres médicaments pris simultanément ou avec certaines spécificités même du malade (allergie par exemple). De nombreuses études réalisées par les grands groupes pharmaceutiques démontrent également que la qualité de certains médicaments est mauvaise, rendant au mieux le remède inefficace, au pire très dangereux pour la santé (parfois même mortel).
Cependant, ce type de cryptomarché offre un accès moins cher aux médicaments pour des personnes sans couverture sociale ou assurance maladie.
L'achat en ligne de médicaments sur le Dark Web est une perte économique réelle pour les grands groupes pharmaceutiques estimée à près de 14 milliards USD par année.

La pédopornographie

La pédopornographie sur le Dark Web est malheureusement bien là et représente sans conteste le plus gros fléau des profondeurs du Web. Cela n'est pas uniquement une lutte impliquant la police, les organisations internationales s'occupant de l'enfance et les différentes associations œuvrant pour le droit des enfants, mais également les très nombreux utilisateurs, voir même les créateurs, des Dark Nets qui ne veulent être en aucun cas associés à ce fléau. Car, contrairement à ce que l'on pourrait penser, ce type d'activité totalement illégale et interdite qu'est la pédopornographie ne touche qu'un tout petit pourcentage des Dark Webs. De plus, il faut savoir qu'il est impossible de tomber sur ce genre de sites par hasard. En effet, ces sites sont cachés avec un maximum de moyen et chaque nouvel utilisateur doit être « accepté » pour pouvoir accéder aux différents forum et chat concernés.
Il est à noter que le nombre de pédophiles reste plus grand sur le Surface Web dû à son plus grand nombre d'utilisateurs. Ces sites sont bien entendu la cible principale des activistes et hackers White Hat.

En février 2017, le groupe Anonymous a « hacké » les serveurs de Freedom Hosting II pour y dérober les bases de données et les supprimer ensuite. Les utilisateurs du site ont même pu voir un message des Anonymous sur la page d'accueil du site lors de cette action.
Il y a, cependant, toute une série de rumeurs qui circulent à propos du Dark Web comme celle attestant l'existence de Red Room, des vidéos en streaming où des personnes feraient subir des sévices atroces à d'autres personnes pendant que des utilisateurs regarderaient la scène chez eux depuis leurs ordinateurs. Cette rumeur est bien évidemment fausse comme d'autres encore, mais la réalité est cependant bien plus triste et inacceptable qu'on ne le pense. Heureusement la lutte reste acharnée, avec plusieurs succès, et les peines de prison sont maintenant devenues très sévères tant pour les créateurs que pour les utilisateurs.

Les Hitmans

Les sites de tueurs à gages, les Hitmans, ne sont pas qu'une légende du Dark Web, mais existent bel et bien. Ces sites, à première vue, ont l'air « normaux » et sont tout à fait actifs avec des tarifs affichés, des conditions et même des enchères proposées. À noter quand même que la plupart de ces sites sont souvent des arnaques. Un site de tueurs à gages en Europe de l'Est s'est fait hacké par des activistes et ces derniers ont publié sur le Dark Web leur base de données et ainsi pu prouver qu'il s'agissait bien d'une supercherie. On a pu y retrouver le nom de certains clients du site qui auraient payé pour des exécutions qui n'ont, heureusement, jamais eu lieu. Un groupe d'activistes du Dark Web avait même ouvert un site de tueur à gages pour prévenir la police à chaque personne payant pour leurs faux services.

La falsification de document

Il y a la possibilité de trouver des cryptomarchés spécialisés dans la vente de document d'identité, par exemple des permis de conduire, des passeports, carte d'identité, cartes grises ou différents diplômes. Les prix varient en fonction de la complexité de falsification du document, mais plus encore de par leur rareté et notoriété. Certains Dark Web ne proposent pas seulement des documents physiques, mais incluent également votre nom dans les bases de données du fournisseur du document.

En ce qui concerne les passeports, le prix est dû au nombre de pays auxquels le passeport falsifié donne accès. Le passeport suisse, par exemple, proposant 142 pays est le 5e au classement[5] des pays offrant le plus de « destinations » sans visa. Le prix de ce passeport est de 3'500. – CHF, car en plus de fournir des accès à de nombreux pays il est aussi plus rare. À préciser qu'il s'agisse d'une copie ou d'un passeport volé, le prix est le même.

Il est aussi possible de trouver des cryptomarchés experts dans la falsification de factures et autres documents comptables aidant au blanchiment d'argent.

Les Malwares

Les Malwares sont des programmes installés à l'insu d'utilisateurs afin de changer la programmation informatique de leur machine. Ceci peut aller de la simple application-espionne qui permet de récolter des informations « live » telles que des appels ou messages, jusqu'au vol de données par exemple le couple « identifiant — mot de passe ». Les prix de ces virus en vente sur le Dark Web varient entre 50.- et 3'000. – CHF. Les données d'une entreprise ont une valeur considérable et leur nombre permet de quantifier le pouvoir et le poids d'une entreprise sur les réseaux par rapport à la quantité de données qu'elle stocke. Un exemple de malware qui a sévi récemment est le virus WannaCry, qui a fait perdre 1 milliard d'USD de données. Cependant, aucune preuve ne stipule que WannaCry a été acheté sur le Dark Web.

D'autres exemples sont à mentionner comme la plateforme de streaming sur internet NETFLIX qui s'est fait attaquer par des hackers par le dépôt d'un malware occasionnant un arrêt du site durant quelques heures.

[5] https://www.tdg.ch/vivre/Quel-passeport-vous-ouvre-le-plus-de-frontieres-sans-visa/story/29540110

Spotify et Amazone ont également été les victimes de la même attaque quelque temps après. Ces coupures de site auraient fait perdre plus de 200'000. – USD aux compagnies concernées en quelques heures seulement. Le code source du Malware en question a été publié via des forums de hackers sur le Dark Web.
Les entreprises doivent donc redoubler leurs efforts en termes de sécurité sur le Web ce qui profite à un nouveau secteur d'activités appelé la Sécurité des systèmes d'information. Ce secteur recrute des collaborateurs qui auraient découvert des failles dans la sécurité de certains systèmes.

La contrefaçon et les articles « tombés du camion »

Les offres de produits tels que des iPhone, des téléviseurs Samsung, des haut-parleurs BOSE et bien d'autres encore, se multiplient sur le Dark Web. Ce sont souvent des appareils volés qui sont ensuite totalement « remis à zéro » puis vendus sur le Dark Web et sur le Web. Il existe même des sites spécialisés dans le Sim Card Unblocked. À savoir que des blocages d'appareils, imposés par le fabricant, sont contournés permettant ensuite de rendre le téléphone compatible avec n'importe quel type de forfait ou compte utilisateur. À préciser cependant que beaucoup de ces annonces sont fausses et, de plus, la police est particulièrement active dans ce domaine, car il est plus simple d'acquérir des produits de la sorte comparés à de la drogue par exemple où les vendeurs se font beaucoup plus discrets. Il existe encore des cybermarchés de vêtements et accessoires dans lesquels on trouve des contrefaçons de grands couturiers, des montres de marque, des parfums et autres objets griffés.
On peut encore mentionner la présence sur le Dark Web de sites spécialisés dans la vente d'alcools et de tabacs. Il peut s'agir d'articles contrefaits, mais aussi dédouanés et revendus sur les réseaux ou encore plus simplement de produits volés.
Tous ces trafics sur le Dark Web provoquent bien entendu de grosses pertes financières, mais également des dégâts en termes d'image (perte de contrôle de l'image de la société, failles au niveau de la sécurité, etc.). La marque française Louis Vuitton est l'une des marques les plus contrefaites et très rependu dans les trafics de contrefaçon. Cet engouement pour le faux Louis Vuitton nuit gravement l'image de la marque qui perd le l'authenticité de ses produits.

Le terrorisme

Une nouvelle vague d'informations nous apprend que les Dark Nets sont souvent utilisés par les terroristes en général et ceux de l'EI en particulier. Ces informations sont cependant à moitié vraies. Le recrutement de terroristes ne se fait pas sur le Dark Net, mais plutôt, et surtout, via les réseaux sociaux grâce à leurs facilités d'accès et leur nombre très important d'utilisateurs. Les communications se font plutôt par messagerie cryptée, par exemple l'application Télégramme. Cependant, il est possible à un terroriste ou à un groupe de terroristes de se procurer des armes et explosifs sur le Dark Web comme n'importe qui d'autre, d'où l'immense danger de cette connexion. Un autre exemple d'étude réalisée par la police colombienne indique que les FARC ont longuement utilisé le Dark Web pour se financer via la vente de cocaïne et comme moyen de communication.

Le pouvoir de l'Open Source

La volonté de nombreux utilisateurs, groupes d'utilisateurs à vouloir protéger leurs droits à la personnalité, assurer la sécurité de leurs données, entretenir une certaine confidentialité sur leurs échanges et à l'intérieur des forums a donné naissance à ces nombreux systèmes permettant l'anonymat sur le Web. De plus, ce qui rend les applications ou OS comme Tor, I2P, Qubes, BitTorrent ou encore Tails OS si « puissants » c'est la très grande taille de leurs communautés. À noter qu'à l'inverse d'Apple ou de Windows, ces applications ou systèmes d'exploitation sont Open Source, c'est-à-dire que le code source est mis à disposition des utilisateurs qui peuvent ensuite s'en inspirer, le modifier et le partager sur la toile. Cela devient donc les applications de « tout le monde ». Wikileaks ou Wikipédia fonctionnement d'ailleurs avec le même principe final, chacun peut y ajouter ses propres informations. Ceci est dû à un copyright permettant un tel procédé aux utilisateurs qui ne sont pas les créateurs directs de l'application ou de l'OS. C'est donc un système collaboratif permettant l'extension de l'application par des tiers qui auraient, par exemple détecté une faille ou une erreur, et qui proposeraient une solution. Il permet également au développeur indépendant d'apprendre grâce aux autres utilisateurs et créateurs. La première application Open Source dévoilée au grand public est le navigateur Mozila FireFox. Le navigateur Tor a comme code source ce même navigateur, d'où la ressemblance visuelle entre ces deux navigateurs.
Autour de l'Open Source s'est créé une réelle communauté active qui lutte pour ses droits et regroupant un grand nombre d'activistes.

Il n'y a donc plus de véritables limites, tout ce qui est créé par un utilisateur est directement mis à la disposition d'autres utilisateurs et permet donc une évolution permanente d'un procédé. Par comparaison ceci s'oppose à l'approche, par exemple, des « brevets » déposés par les grandes marques qui cherchent plutôt à bloquer le développement d'un produit, d'une formule ou autre pour des raisons principalement financières (investissement, retour sur investissement, marges, durabilité, etc.).

À noter, pour conclure, que l'Open Source est vu comme une institution pacifiste à but non lucratif aidant au développent et au progrès tout en respectant des principes et valeurs définis.

Conclusion

Ces dernières années les prouesses technologiques n'arrêtent pas de nous surprendre. De nombreux nouveaux objets font désormais partie intégrante de nos vies quotidiennes. Tout cela résulte de maintes années de recherche que ce soit dans le domaine du Hardware ou du Software. L'implication constante d'internet dans tous ces nombreux projets était, est et sera indispensable. Internet est le moyen de communication le plus rapide, le plus sûr et il fait partie maintenant de notre quotidien, qu'on le souhaite ou non. On ne peut stopper le progrès, et d'ailleurs à quoi bon ? Nous avons tout intérêt à apprendre à vivre avec ainsi qu'à voir et utiliser les multiples avantages qu'il peut nous offrir.

Avant tout, il est primordial de commencer par bien comprendre ce moyen de communication utilisé par presque tous. Pour cela il est important de définir précisément le Web, ce qu'il est et ce qu'il fait. Beaucoup de recherches effectuées par de nombreux médias et journalistes confondent le « sens » des différentes « couches » du Web. Cette confusion s'est ensuite étendue mondialement sur une grande partie de la population générant une crainte d'internet. Beaucoup de légendes urbaines se sont également propagées dues au manque d'information. Cette crainte a poussé la population à se limiter à l'accès internet « standard », sans vraiment connaître la stratégie qui y est dissimulée.

La métaphore du centième signe[6] désigne un phénomène inexpliqué de changement de comportement dans un groupe ou une population dans laquelle un membre aurait acquis une nouvelle connaissance qu'il propagerait autour de lui de manière inconsciente. Cette connaissance est ensuite partagée par les nouveaux porteurs de celle-ci. Arrivé à un nombre symbolique de 100, on prédit qu'une personne, sans avoir été en contact avec les porteurs de la connaissance, serait aussi porteuse de cette dernière.
En rapport avec le nombre élevé d'activistes qui dénoncent des actes d'espionnages illégaux et le nombre tout aussi élevé de personnes refusant qu'on viole leurs droits à la protection de la personnalité, on peut en déduire qu'un changement profond de comportement et une réelle prise de conscience de la population se sont mis en place ces dernières années.

Grâce aux projets des premiers « cyberpunks », des outils permettant d'utiliser internet de manière sûre ont pu être mis au point. Ces créations de sous réseaux isolés du Web visible permettent à des activistes de s'exprimer librement et de pouvoir prendre la parole. Certaines vérités cachées ont été révélées au grand public. Nous savons que de nombreux gouvernements espionnent et/ou se font espionner. Des révélations telles que celles faites par Edward Snowdon ont des suites[7] et des conséquences. On sait, par exemple, quelles ont été entendues par la Cour européenne des Droits de l'Homme le 7 novembre 2017 et plusieurs chefs d'accusation ont pu être retenus tels que l'espionnage subi par Amnesty International et le Centre des ressources juridiques d'Afrique du Sud via l'utilisation de données obtenues de manières illégales.

[6] http://www.institut-repere.com/METAPHORES/institut-repere-base-documentaire-m-62-le-100eme-singe.html
[7] https://www.theguardian.com/world/2017/nov/07/uk-intelligence-agencies-face-surveillance-claims-in-european-court?CMP=share_btn_tw

Les faits sont là, nous sommes tous conscients de ce qui se passe vraiment sur la surface de l'iceberg du Web, mais aussi en dessous. Il est donc important de rester informé et de se protéger au mieux avec des outils simples, repenser également à notre comportement sur le net, et demeurer plus actif quand nous avons la possibilité de faire entendre notre voix concernant la sécurité des données, la protection de la personnalité et la surveillance de masse.

« Ceux qui peuvent renoncer à la liberté existentielle afin d'obtenir la sécurité temporaire ne méritent aucune des deux »

Benjamin Franklin écrivait *au nom* de l'Assemblée de Pennsylvanie à l'attention du gouverneur de cette colonie, en 1755

Bibliographie

WIKIPEDIA, [sans date]. Internet [en ligne]. 2017.
[Consulté le 02 octobre 2017].
Disponible à l'adresse :
https://fr.wikipedia.org/wiki/Internet

Absol Video, 2017. Le Deep Web [enregistrement vidéo]. YouTube [en ligne]. 15 juillet 2017.
[Consulté le 02 octobre 2017].
Disponible à l'adresse :
https://www.youtube.com/watch?v=9g2STPKNk_8

SomeOrdinaryGamers, 2015. The Scary Part of the Internet! [enregistrement vidéo].
YouTube [en ligne]. 22 juin 2015.
[Consulté le 02 octobre 2017].
Disponible à l'adresse :
https://www.youtube.com/watch?v=XjyyfmqQazw&list=PL_NnG4jzzKohor2G8liXfgfRboMRGtO-f&index=118

RETROSHARE, [sans date]. Foire Aux Questions [en ligne]. 2016.
[Consulté le 04 octobre 2017].
Disponible à l'adresse :
http://retroshare.sourceforge.net/wiki/index.php/Frequently_Asked_Questions/fr

FRANCECULTURE, [2017] Adieu Darknet, bonjour Librenet [en ligne] 29 mars 2017
[Consulté le 06 octobre 2017]
Disponible à l'adresse :
https://www.franceculture.fr/emissions/la-methode-scientifique/adieu-darknet-bonjour-librenet

WIKIPEDIA, [sans date]. Wikileaks [en ligne]. 2017.
[Consulté le 05 octobre 2017].
Disponible à l'adresse :
https://fr.wikipedia.org/wiki/WikiLeaks

WINTER Alex, 2015, *Deep Web* [film - documentaire] USA, NETFLIX [2015]

NICOLARGO, [2012], Introduction et première utilisation de Tor [en ligne]. 02 avril 2017
[Consulté le 08 octobre 2017]
Disponible à l'adresse :
https://blog.nicolargo.com/2012/04/introduction-et-premiere-utilisation-de-tor.html

TOR PROJECT, [sans date], The Tor Project [en ligne], [sans date]
[Consulté le 10 octobre 2017]
Disponible à l'adresse :
https://www.torproject.org/projects/torbrowser.html.en

VPN MENTOR [sans date], Le Navigateur Tor — qu'est-ce que c'est, comment ça marche et comment s'allie-t-il à un VPN ? [en ligne]. [sans date]
[Consulté le 10 octobre 2017]
Disponible à l'adresse :
https://fr.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/

UBUNTU-FR, [sans date], Tor : Réseau Anonyme [en ligne]. [sans date]
[Consulté le 11 octobre 2017]
Disponible à l'adresse :
http://doc.ubuntu-fr.org/tor

WIKIHOW, [sans date], How to Set a Specific Country in a Tor Browser [en ligne]. 23 mai 2017
[Consulté le 11 octobre 2017]
Disponible à l'adresse :
https://www.wikihow.com/Set-a-Specific-Country-in-a-Tor-Browser

PRIVATE INTERNET ACCES, [sans date], Tor vs VPN vs Proxy [en ligne]. [sans date]
[Consulté le 14 octobre 2017]
Disponible à l'adresse :
https://fra.privateinternetaccess.com/pages/tor-vpn-proxy

WIKIPEDIA, [sans date]. Grams [en ligne]. 2017.
[Consulté le 18 octobre 2017].
Disponible à l'adresse :
https://en.wikipedia.org/wiki/Grams_(search)

JARRETT, H. Marshal, [sans date]. Computer Crime and Intellectual Property Section Criminal Division [en ligne]. Office of Legal Education Executive Office for United States Attorneys. USA: 1979.
[Consulté le 18 octobre 2017].
Disponible à l'adresse :
https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

EUROPEAN COMMISION, [sans date,]. Cybercrime [en ligne]. 2017
[Consulté le 18 octobre 2017]
Disponible à l'adresse :
https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

FORTUNE, [sans date]. Sanctions: America's best new weapon against cyber crime [en ligne].
[Consulté le 18 octobre 2017]
Disponible à l'adresse :
http://fortune.com/2015/04/02/us-cyber-crime-sanctions/

INDEPENDENT, [sans date]. Illegal downloading: what happens if you are caught? [en ligne].
[Consulté le 18 octobre 2017]
Disponible à l'adresse :
http://www.independent.co.uk/life-style/gadgets-and-tech/features/illegal-downloading-what-happens-if-youre-caught-1736013.html

LOS ANGELES TIMES, [sans date]. AlphaBay, the largest marketplace on the dark web, is seized by U.S. [en ligne].
[Consulté le 20 octobre 2017]
Disponible à l'adresse :
http://www.latimes.com/politics/washington/la-na-essential-washington-updates-alphabay-largest-marketplace-on-dark-1500569108-htmlstory.html

MOTHERBOARD, [sans date]. 7 Ways the Cops Will Bust You on the Dark Web [en ligne].
[Consulté le 20 octobre 2017]
Disponible à l'adresse :
https://motherboard.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web

ORGANISATION MONDIAL DE LA SANTE, [sans date]. La menace croissante des contrefaçons de médicaments [en ligne]
[Consulté le 21 octobre 2017]
Disponible à l'adresse :
http://www.who.int/bulletin/volumes/88/4/10-020410/fr/

WIKIPEDIA, [sans date]. Captch [en ligne]. 2017.
[Consulté le 19 octobre 2017].
Disponible à l'adresse :
https://en.wikipedia.org/wiki/CAPTCHA

WIKIPEDIA, [sans date]. Icann [en ligne]. 2017.
[Consulté le 20 octobre 2017].
Disponible à l'adresse :
https://en.wikipedia.org/wiki/ICANN

WIKIPEDIA, [sans date]. Darpa [en ligne]. 2017.
[Consulté le 20 octobre 2017].
Disponible à l'adresse :
https://en.wikipedia.org/wiki/DARPA

WIKIPEDIA, [sans date]. Wikileaks [en ligne]. 2017.
[Consulté le 21 octobre 2017].
Disponible à l'adresse :
https://en.wikipedia.org/wiki/WikiLeaks

TAILS, [sans date]. Tails, the amnesic incognito live system [en ligne]
[Consulté le 23 octobre 2017]
Disponible à l'adresse :
https://tails.boum.org

QUBES, [sans date], A resonably secure operating system [en ligne]
[Consulté le 23 octobre 2017]
Disponible à l'adresse :
https://www.qubes-os.org