ULB UNIVERSITÉ LIBRE DE BRUXELLES

MA en STIC

Tor comme outil de protection de la vie privée sur internet

Selim Ben Ismail

02 Août 2020

Résumé

Cet article, rédigé dans le cadre du cours d'architecture des systèmes d'information de l'Université Libre de Bruxelles, aura pour objet d'appréhender la nature du réseau Tor, d'en comprendre les principes mis en œuvre et d'en évaluer les possibilités actuelles et futures concernant la protection de la vie privée sur internet. L'article est divisé en trois parties : dans un premier temps, nous introduirons les concepts et enjeux liés à la thématique de l'anonymat sur internet. Ensuite nous survolerons les outils de base limitant les traces numériques. Et finalement nous nous attarderons sur le cas controversé de Tor (The onion router) pour en décrire sa nature, ses mécaniques, ses limites et son positionnement idéologique.

***Keywords*—** Tor, Proxy, Anonymat,Internet, données à caractères personnels, vie privée

Introduction

Dans cette ère du web 2.0, où existe une interconnexion quasi permanente des personnes entres elles par le biais des services numériques, l'humain se voit être progressivement représenté par des ensembles de données. Ainsi on observe un phénomène de documentalisation de la personne qui croît de façon parallèle au développement des technologies de l'information et de la communication. Ces systèmes informationnels, alimentés par nos interactions sur les réseaux socio-numériques et nos saisies endogènes dans la toile, sont devenus des éléments clés de notre société hyperconnectée. Ressources commerciales, outils de spéculation, instruments de surveillance, substrats de recherche, etc.. ; les champs d'application sont sans limites pour qui sait les saisir.

Cependant, ces informations en apparence anodines n'en restent pas moins des éléments de notre vie privé, et peuvent être sensibles, préjudiciables, ou simplement fausses. Il convient, dès lors, de se questionner sur la gouvernance de celles-ci, la confidentialité qui les entoure et l'impact que leur exploitation pourrait avoir sur nos libertés individuelles.

Heureusement, cette collecte industrialisée de nos données à caractères personnels n'est pas une fatalité : d'une part, celle-ci est encadrée par un certain nombre de lois et de clauses, d'autre part, il existe des dispositifs de sécurité permettant de masquer nos informations et les contenus échangés.

1 Définition et enjeux relatifs à la protection de l'identité

1.1 Les données à caractères personnels

Avant d'entrer plus dans le détail, il est nécessaire de définir concrètement cette notion de "donnée à caractère personnel", couramment abrégée en "données personnelles" ou "DCP". La définition légale, que l'on peut retrouver sur le site officiel de la Commission Européenne, est définie comme telle :

> "Les données à caractère personnel sont des informations se rapportant à une personne vivante identifiée ou identifiable. Différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel. Des données à caractère personnel qui ont été rendues anonymes, chiffrées ou pseudonymisées, mais qui peuvent être utilisées pour identifier à nouveau une personne constituent toujours des données à caractère personnel et sont couvertes par le RGPD. Les données à caractère personnel rendues anonymes de telle manière que la personne ne soit pas ou plus identifiable ne constituent plus des données à caractère personnel. Pour qu'une donnée soit véritablement rendue anonyme, le processus d'anonymisation doit être irréversible. [...] (4)"

Rentre dans cette définition, les éléments tels que le nom, le prénom, les adresses de résidence ou de courriel, le numéro de carte d'identité, les données de géolocalisation, les adresses IP et MAC, les cookies, ou toutes autres données détenues par un hôpital ou un médecin qui permettraient d'identifier de manière unique une personne.

Il est essentiel de faire la distinction entre les données pseudonymisées et les données anonymisées. En effet, le problème des données anonymisées est qu'elles continuent de permettre l'individualisation d'une personne concernée ainsi que la corrélation entre différents

ensembles de données. Ce qui rejoint un autre point majeur de la définition : la qualité d'irréversible que doit prendre l'anonymisation d'une donnée. Dans cet extrait du rapport de la Commission Européenne sur les techniques d'anonymisation nous retrouvons quelques précisions quant à cette nécessité :

> "Il faut insister sur le fait que l'«identification» ne désigne pas simplement la possibilité de retrouver le nom et/ou l'adresse d'une personne, mais inclut aussi la possibilité de l'identifier par un procédé d'individualisation, de corrélation ou d'inférence" (3)

C'est en effet dans la conjointure des big data aux algorithmes de datamining que des données - à première vue désuètes - révèlent une dimension pernicieuse. L'affaire AOL [1] (7), est un exemple typique de cette surestimation du pseudonymat dans la protection de la vie privée. En août 2006 une équipe de chercheurs d'AOL diffusa publiquement une base de données contenant les saisies de recherche effectuées par près de 658 000 internautes au cours des mois de mars, avril et mai 2006, où l'identifiant des utilisateurs avait été remplacé par une suite de caractères numériques. Très rapidement, la base de données fut rediffusée par des tiers sur des serveurs miroirs rendant son retrait de la toile presque impossible. Et malgré l'immense océan que représentait les données à traiter - il était question de quelques 20 millions de requêtes enregistrées - de nombreux internautes purent être identifiés par le recoupement d'informations au travers des différentes sources de données. On y trouve par exemple, l'utilisateur n°4417749, identifié en la personne de Thelma Arnold, âgée alors de 62 ans, vivant à Lilburn dans l'état de Georgie des États-Unis qui aurait interrogé le moteur de recherche AOL sur les célibataires de 60 ans, les tremblements de la main, les effets de la nicotine et les chiens qui urinent partout. Si ce cas peut paraître anecdotique, le problème que peut poser une mauvaise gestion des données utilisateurs quant à la protection de leur vie privée, y apparaît très clairement et il n'est pas surprenant que cet évènement ait suscité la colère des citoyens américains.

1.2 Le problème des cookies

Un cookie est un petit fichier texte généré par les serveurs HTTP et envoyé aux clients lorsque ceux-ci s'y connectent pour la première fois. Ce fichier est stocké en local dans le cache du navigateur internet et sera renvoyé chaque fois que le client voudra interroger ce même serveur HTTP.

Il existe différents types de cookies et nous n'entrerons pas plus dans le détail de leur fonctionnement, mais leur rôle initial est de permettre à un serveur de "reconnaître" un client et fluidifier la navigation de ce dernier en conservant des informations spécifiques à l'utilisateur. Ce sont les cookies qui permettent des fonctionnalités comme l'identification automatique, le maintien d'une session, l'exécution d'un contenu flash ou la mémorisation de nos préférences sur un site pour une reconnexion ultérieure. Malheureusement, ce sont eux aussi qui permettent le profilage de l'utilisateur et le ciblage publicitaire.

Les informations contenues dans un cookie sont généralement : un identifiant propre à chaque internaute, le domaine de provenance du cookie, la date de création du cookie et un contenu lié à l'utilisateur (identifiant de session, login, mot de passe, etc.). En inspectant le fichier, il est donc possible de suivre la navigation d'un internaute, ce qui place les cookies dans le champ de définition des données à caractères personnels.

1. AOL, America Online, est une société américaine de service internet

2 Outils de base limitant les traces numériques

2.1 Configuration du navigateur

Le premier niveau sur lequel nous pouvons agir pour limiter nos traces numériques et la fuite de données personnelles, est le navigateur. La récolte d'information est inhérente au fonctionnement de celui-ci, il est donc nécessaire d'être vigilant à leur configuration. Pour limiter la collecte d'informations, la suppression automatique des cookies en fin de session et le blocage des cookies tierce partie peuvent être activés. Un outil secondaire est le bloqueur de publicité qui en empêchant l'exécution du code des bannières et pop-up publicitaires, bloque également leurs cookies.

La navigation privée

La navigation privée est un outil intégré à tous les navigateurs actuels. Sa dénomination, presque malhonnête, tend à rendre cet outil populaire. Pourtant, ce mode de navigation ne protège d'aucune manière les internautes d'une quelconque forme d'identification ou de pistage qui aurait eu lieu lors d'une navigation dite "normale". Le mode de navigation privée empêche simplement l'enregistrement local de l'historique de navigation et supprime les cookies HTTP stockés dans le cache client à la fermeture de la session. Mais cela n'affectera en rien les données perçues et enregistrées du côté des serveurs (2).

2.2 Les serveurs proxy

Il est difficile de parler des relais Tor sans aborder auparavant le fonctionnement des serveurs proxy. Ces serveurs proxy, qu'on appelle aussi serveurs mandataires, sont donc des dispositifs que l'on retrouve fréquemment comme éléments de sécurité aux sorties des réseaux locaux. Le principe de fonctionnement est relativement simple : le serveur proxy fait office d'intermédiaire entre deux hôtes – souvent l'un situé à l'intérieur d'un réseau local tandis que l'autre est sur l'internet mondial – relayant les requêtes qu'il reçoit et analysant le trafic qui le traverse. De cette façon, il va mettre à disposition du client ses propres ressources (mémoire cache, compression des données, etc) afin d'accélérer sa navigation et filtrer les contenus non-désirables comme les pubs ou les contenus malveillants. Paradoxalement, si le serveur proxy peut être utilisé comme un outil de censure et de contrôle en restreignant l'accès des clients du réseau sous-jacent à des sites spécifiques ou en leur bloquant certains contenus, il pourra aussi être utilisé comme un outil d'émancipation grâce à la technique du NAT (Network Adress Translation). En effet, lorsque nous accédons au Web par l'entremise d'un serveur proxy, nous ne naviguons plus avec notre propre adresse IP mais avec celle du serveur proxy mandaté. Là, est tout l'intérêt de ce dispositif dans la protection des données à caractères personnels. Car dès lors que notre adresse IP, notre identifiant numérique principal, est anonymisé, il est significativement plus laborieux de pister nos activités sur la toile. Qui plus est, nous masquons au passage les informations qui y étaient liées, comme notre localisation géographique. Pour illustrer ça : supposons une personne résidente d'un certain pays, qui souhaite se connecter à un service spécifique; que, pour une quelconque raison politique, la liaison à celui-ci est bloquée dans sa zone. En passant par un serveur proxy situé physiquement dans un autre pays, cette personne pourrait alors contourner la restriction géographique et joindre le service qu'elle convoitait.

Toutefois, si le proxy intègre des possibilités intéressantes pour protéger nos données à caractères personnels et notre vie privée, il souffre de plusieurs défauts non-négligeables. Le

premier est que la liaison entre le client et le serveur proxy n'est pas protégée et peut être facilement le sujet d'une attaque. Le second est que si l'adresse IP se voit être masquée, ce n'est pas le cas du contenu des requêtes envoyées sur le réseau. Et finalement, la plus grande faille du proxy concernant la protection de la vie privée, est le proxy lui-même. Il est capital de garder à l'esprit que le serveur dispose de toutes les informations que nous voulions initialement cacher et qu'il peut potentiellement les enregistrer ainsi que toutes les autres données confidentielles passant par lui (identifiants, coordonnées bancaires, etc.). Il convient donc de s'assurer de la bienveillance des titulaires du serveur proxy et de la qualité de ses défenses face aux attaques ciblées. Outre cela, les législations auxquelles sont soumis les fournisseurs de serveurs proxy peuvent contraindre ces derniers à fournir les données dont ils disposent à certaines autorités ; c'est notamment le cas aux Etats-Unis où le USA Patriot Act, introduit suite aux attaques terroristes du 11 septembre 2001, octroie au FBI un élargissement de l'utilisation des "Lettres de sécurité Nationale (NLS)"(12).

3 The Onion Router

Dernière la dénomination "The Onion Router", en abrégé "Tor", se cache trois éléments distincts : premièrement, le réseau Tor qui est un réseau de communication informatique, à faible latence, superposé à internet et utilisé dans le but d'anonymiser les communications. Il fut initialement développé par Paul Syverson en 1995 dans le cadre d'un projet de l'US Navy visant à protéger les communications militaires de l'analyse de trafic. L'architecture du réseau Tor reprend le concept de relais proxy ainsi que de l'encryptage par couche successives des Mix network de David Chaums (18). Deuxièmement, le projet Tor (the Tor project incorporated), une association de droit américain fondée en 2004 par Roger Dingledine et Nick Mathewson et financée par la Fondation Frontière Electronique (FFE) ; celle-ci reconnaissant l'apport du réseau Tor aux droits numériques. L'association rassemble une communauté internationale de volontaires travaillant à l'amélioration et l'entretien du réseau Tor. Le projet est fortement engagé politiquement et promeut l'idéal d'un internet, transparent, libre d'accès et respectueux de la vie privée des utilisateurs. Finalement le logiciel Tor, qui est le navigateur permettant de se connecter au réseau Tor. Il est évidement possible de se connecter au réseau sans utiliser spécifiquement le navigateur Tor, mais ce dernier été développé par les membres du Projet Tor en 2009 pour faciliter l'usage du réseau et le rendre plus accessible aux personnes n'ayant pas de connaissances approfondies en informatique(6; 15).

3.1 Principe de fonctionnement

Le réseau Tor est constitué d'une multitude de serveurs – appelés nœud ou onion router (OR) – partout dans le monde, gérés par des bénévoles reconnus de l'association (10).

L'utilisateur souhaitant naviguer anonymement par le réseau Tor doit utiliser un logiciel qui le connectera à ce qu'on appelle un onion proxy (OP). Cet onion proxy, ira chercher les informations de navigation dans les répertoires des serveurs annuaires (DirecTory Server) et établira un circuit de trois nœuds – un nœud d'entrée (entry node ou guard node [2]), un nœud du milieu (middle node , dit aussi non exit node) et un nœud de sortie (exit node)– qu'emprunteront les paquets à travers le réseau Tor [3].

2. Le guard node est un cas particulier de nœud d'entrée remplissant certaines conditions comme avoir un haut pourcentage de disponibilité par semaine, une large bande passante, etc.)

3. Il est aussi possible de se connecter au réseau par un pont relais (relay bridge). Si la liste des nœuds "clas-

La création du circuit commence par l'échange Diffie-Hellman, ensuite le circuit se construit pas à pas par l'envoi de cellules de commande : l'OP envoie une cellule CREATE à l'OR qu'il souhaite intégrer à son circuit, si l'OR accepte il répondra à l'OP par une cellule CREATED. Ensuite l'OP envoie une nouvelle cellule CREATE à l'OR suivant, jusqu'à complétion du circuit. Une fois ce dernier établi, les paquets de données peuvent commencer à circuler dedans. Ce circuit est valable 10 minutes, il est ensuite reconstruit pour limiter l'information qu'un nœud pourrait détenir.

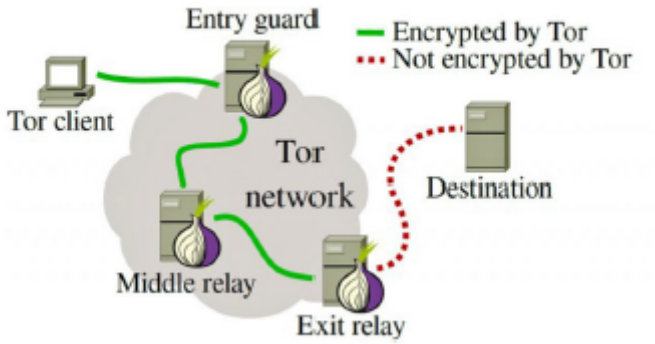

FIGURE 1 – Routage en oignon

A chaque saut dans le circuit, les paquets sont encryptés dans une nouvelle couche par une clé symétrique. Les informations se retrouvent encapsulées sous plusieurs couches de chiffrement; c'est de là que provient le nom "routage en oignons". D'autre part chaque nœud n'a connaissance que de l'adresse du nœud précédant et du nœud suivant dans le circuit; l'adresse des autres leur est inconnue. De ce fait, si l'un des nœuds du circuit est attaqué, l'attaquant ne disposera ni des clés pour récupérer le contenu des paquets ni ne connaîtra l'origine ou la destination finale des paquets

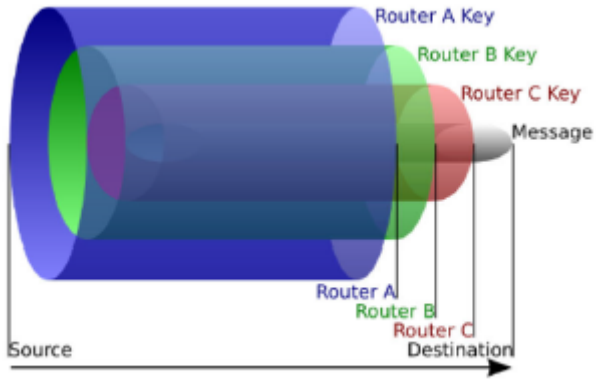

FIGURE 2 – Chiffrement en couche

Tor cache ses utilisateurs entre eux, c'est donc leur nombre et leur diversité qui rend le

sique" (OR) est libre d'accès à tout le monde, la liste des pont relais est, elle, gardé secrète par le Projet Tor. Ces ponts permettent d'atteindre le réseau Tor depuis des endroits où son accès est bloqué.

système si efficace. A l'instar d'un bal masqué, on peut voir ceux qui s'y rendent et ceux qui en sortent, mais personne ne peut savoir qui parle avec qui à l'intérieur.

3.2 Faiblesses et limites

Si la robustesse du réseau Tor est largement reconnue dans monde entier, il n'est pas exempt de critique pour autant. En effet, Tor a ses propres limites, qui depuis la création du réseau, ont déjà été de nombreuses fois éprouvées.

3.2.1 Attaque bout-à-bout

La faiblesse la plus reconnue est celle de l'attaque bout-à-bout, dite end-to-end en anglais. Il s'agit d'analyses conjointes du trafic entrant et sortant du réseau Tor. En observant le volume et le timing des paquets on peut corréler le nœud d'entrée et de sortie d'un circuit(17; 10). Pour entraver ces attaques, des solutions comme l'insertion de paquets parasites ou des variations aléatoires du débit ont été proposées mais celles-ci augmenteraient considérablement la latence du réseau, considéré comme déjà lent.

3.2.2 Attaque sur les noeuds de sortie

Les cibles principales des attaques sur le réseau Tor sont les nœuds de sortie du réseau (exit node) en exploitant les failles des protocoles HTTP. En effet, en sortie, les requêtes s'y retrouvent découvertes de leurs couches de cryptage afin de pouvoir communiquer avec le service distant.

Identifiée depuis longtemps, cette faiblesse est néanmoins toujours présente. Des chercheurs de l'université de Vienne ont mené l'expérience en contrôlant un nœud de sortie de collecter toutes les requêtes HTTP passant par leur serveur et de les analyser ensuite avec un script en python (14). Si l'émetteur de la requête n'est pas directement identifiable, il est néanmoins possible de tirer beaucoup d'informations sensibles de ces dernières : Lorsque des requêtes sont faites sur un moteur de cherche, les termes de celles-ci sont transposés dans l'URL par les requêtes HTTP GET. Ainsi en lisant simplement cette URL :
https ://www.google.com/search? q=restaurant+ULB[...]/ il est très facile de deviner que la personne fait une recherche sur les restaurants de l'ULB. Lorsque ces informations s'accumulent en nombre suffisant, elles peuvent être corrélées et défaire l'anonymat de son émetteur, comme ce fut le cas avec l'affaire d'AOL précédemment évoquée. La situation s'aggrave lors d'une recherche d'itinéraire sur google maps :
https ://www.google.com/maps/dir/50.8284058,4.3734282/restaurant+ULB[...]/. Ici, ce sont même les coordonnées géographiques de l'émetteur au moment de la requête qui se retrouvent lisibles.

Jusqu'ici, il ne s'agissait que d'attaques passives où le trafic était écouté, mais l'utilisateur peut aussi subir des attaques actives : le nœud de sortie corrompu peut modifier les requêtes https en http, évitant ainsi que le contenu des échanges soit chiffré. Outre cela, le nœud de sortie compromis peut devenir un vecteur de propagation de logiciel malveillant en injectant des scripts Javascript dans les pages html renvoyées à l'utilisateur. Ces scripts seront exécutés lors de la lecture de la page par le client et activeront des morceaux de codes malveillants sur l'ordinateur de celui-ci (19).

3.2.3 Honey Connector et Exitmap

Afin de restreindre ce type d'attaque, l'équipe du Tor Project surveille attentivement les nœuds de sortie et des outils de scan comme HoneyconnecTor et Exitmap ont été déployés pour détecter et évincer les "spoiled onions" – littéralement "les oignons pourris" – du réseau (20).

Le Honey connector permet la détection de l'écoute passive du trafic. Le système envoie à travers le réseau Tor une paire login-password unique servant d'appât vers un site "pot de miel" (honeypot) contrôlé par l'équipe Tor. Si par la suite, une nouvelle connexion au pot de miel est enregistrée, c'est que le trafic est écouté et le nœud de sortie corrompu. Ce dernier est alors supprimé de la liste des routeurs que les serveurs annuaires fournissent aux OP.

Quant à Exitmap, il permet, lui, de détecter les attaques actives. Pour cela, il établit une connexion vers un pot de miel de contrôlé par Tor et y crée du trafic. Comme le contenu du trafic est connu à l'avance, s'il arrive modifié au pot de miel, il sera directement repéré.

3.2.4 Analyse du protocole de Routage

Dans une étude statistique publiée en juin 2019, Eric Filiol cherche à démontrer que la sélection des trois nœuds constituant le circuit n'est pas faite de manière aléatoire mais suit une loi de puissance. Si la création du circuit était effectivement totalement arbitraire, comme elle est communément supposée, elle suivrait une loi uniforme ; ce qui signifierait que chaque routeur aurait la même probabilité d'être sélectionné. Or, Tor doit aussi faire face à des problèmes de congestion, de bande passante, et de stabilité pour garantir la performance du système malgré la diversité des nœuds et des capacités de ceux-ci. L'hypothèse de Filiol selon laquelle, les nœuds seraient choisis, en grande partie selon un calcul de poids attribués aux routeurs, semble cohérente et est validée par ses mesures. Selon ses analyses, attaquer un set réduit de 1.463 nœuds (1.217 du milieu, et 246 nœuds de sortie) serait suffisant pour contrôler 50% du trafic (11). Cette faiblesse de sécurité est critique car l'identification du circuit facilite grandement les attaques bout-à-bout face auxquelles Tor est particulièrement vulnérable. Ce serait avec cette méthode que le FBI aurait réussi à démanteler la Silk road, un énorme marché noir caché sur le darknet, en 2014 (5).

Table 4 Number of top-significant routers per percentage Tor traffic

Fraction (%)	*Guard*	*Middle*	*Exit*	Total
33	755	899	166	1065
50	1030	1217	246	1463
66	1326	1617	342	1959
75	1507	1882	425	2307

FIGURE 3 –

3.2.5 Détection du flux Tor par DPI en Chine

La censure de l'internet en Chine n'est plus un secret pour personne, mais au-delà de ça, ce pays surpasse tous les autres en matière de blocage de Tor et de restriction de l'anonymat.

L'utilisation de Tor y est entravé à trois niveaux différent : premièrement, un filtrage d'URL est opéré : les URL's sont scannées à la recherche de mots-clés relatifs à Tor. Deuxièmement, l'accès aux serveur annuaires permettant aux navigateurs d'obtenir la liste des relais Tor est restreint par blocage IP. Et troisièmement, l'accès aux relais eux-même, ainsi qu'aux passerelles, l'est également depuis l'intérieur du pays (21). Pour dénicher les passerelles Tor, le GFC [4] analyse le trafic sortant du pays à l'aide de la technologie DPI (deep paquet inspection) et y cherche des listes de chiffrement spécifiques au protocole TLS (Transport Layer Security) envoyées par les clients Tor aux relais Tor. Lorsqu'un flux Tor est détecté, un scanner du GFC va le suivre, puis tenter d'établir une connexion Tor au relais en simulant une adresse IP chinoise quelconque. Si la passerelle répond alors au protocole Tor émis par le scanner du GFC, elle se trahira elle-même et son accès sera bloqué par le GFC. Le réseau Tor est de plus en plus utilisé pour contourner la censure et dans cette optique, cela pose un problème que le trafic de Tor soit si facilement identifiable, même s'il reste anonyme et confidentiel.

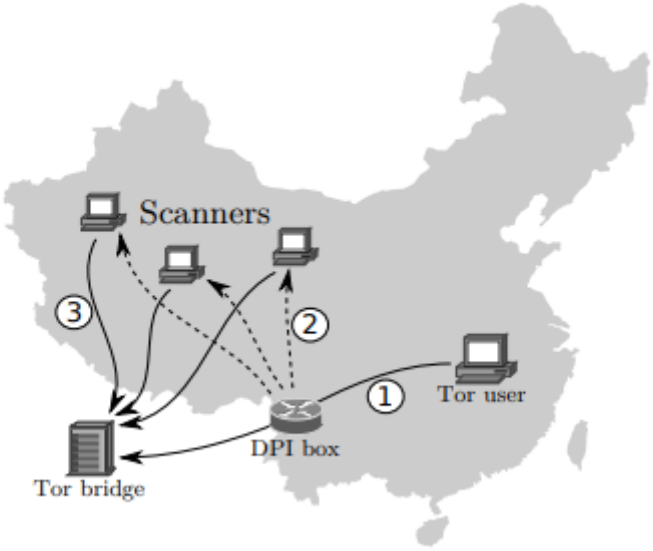

FIGURE 4 – le Grand Firewall de Chine

3.3 Services cachés et positionnement éthique

L'aspect le plus polémiqué et controversé de Tor est, sans aucun doute, les services cachés (hidden services). Il s'agit du fameux "dark net " souvent fantasmé dans les médias et l'imaginaire collectif. Ces services cachés sont concrètement un ensemble de serveurs non-indexés dans le répertoire des serveurs DNS du réseau internet. On les retrouve sous le nom de domaine .onion et sont accessibles via le Tor en paramétrant spécifiquement son navigateur pour les atteindre. Le "dark net " souffre d'une réputation sulfureuse. Pour cause, l'anonymat qu'il confère est propice aux activités illégales et criminelles. On y retrouve entre autres : du commerce de stupéfiants, d'armes, des réseaux de pédopornographies, de cybercriminels ...

4. le Grand Firewall de Chine (GFC) est un projet initié par le Ministère de la sécurité publique de la république populaire de Chine en 2003 dont l'objectif est , entre autre, de contrôler l'accès aux contenus d'internet jugées subversifs.

La couverture que Tor fournit face à la surveillance policière ne sied que peu à certains politiques. C'est ainsi qu'en 2015, après les attentats de Paris et de Bruxelles, Bernard Cazeneuve, alors ministre de l'intérieur de la France, cherchera à rendre Tor illégal dans son pays. Il accusera le réseau et les services cachés auxquels il permet d'accéder, d'être un lieu d'échanges criminels et d'organisation du terrorisme (13) .

Nous pouvons nous interroger sur la légitimité d'un réseau permettant de telles choses. Mais cela nous ramènerait au débat houleux quant au droit à l'anonymat. Ce n'est pas tant l'anonymat que ce qu'on en fait qui pose problème. De plus, le réseau est aussi utilisé par des autorités d'états qui en sont d'ailleurs les premiers mécènes (11; 6).

Outre cela, Tor et ses services cachés sont aussi fort appréciés des activistes et opposants politiques. En Tunisie, sous le régime de Ben Ali, le cyberespace était fortement surveillé par l'ATI (Agence Tunisienne de l'Internet) et un filtrage du contenu y était opéré (16). La critique du régime en place menait à de lourdes sanctions pour les opposants et leur famille. Cette crainte de l'état pour sa légitimité n'était sans fondement : car c'est bien par YouTube (pourtant censuré) et Twitter que l'indignation populaire s'est transformé en un réel soulèvement qui sera désigné sous le nom de "Printemps Arabe". Dans cette révolution, Tor, ainsi que d'autres organisations, mirent en place des relais proxy afin de permettre aux citoyens d'accéder et médias sociaux à travers le monde pendant cette crise (8). Tor, et plus largement les proxys, se présentent aux Tunisiens comme l'opportunité de s'exprimer sans risques de répressions vis-à-vis de la dictature qui les opprime. Cet usage de l'anonymat est décrit par James C. Scott comme un "art de la résistance" (9) .

3.4 Evolution et projets à venir de Tor

Si, à sa création en 2004, le réseau Tor était modestement composé d'un total de 32 nœuds (10) (24 aux Etats-Unis et 8 en Europe), en date du 22 mai 2016, ce nombre n'est plus du tout comparable : c'est près de 7000 nœuds à travers le monde qui étaient recensés (1). Le Tor Project a toujours pour ambition de continuer à grandir, tant par le nombre de relais et de passerelles que par le nombre d'utilisateurs. Pour d'une part améliorer la performance et la sûreté de l'anonymat sur le réseau, et d'autre part, pour éveiller d'avantage la société à la question des droits numériques.

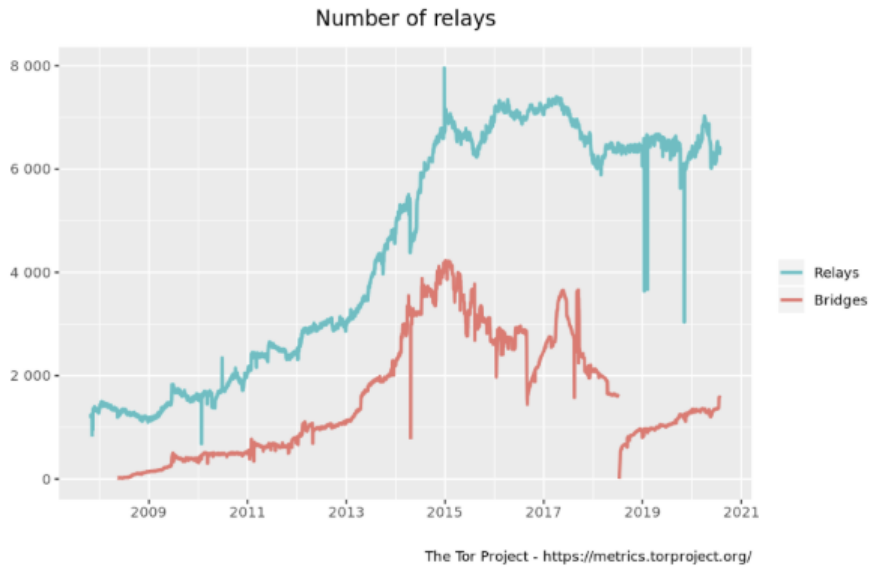

FIGURE 5 – évolution du nombre de relais Tor

Dans une conférence donnée au Fosdem de l'Université Libre de Bruxelles, Roger Dingledine, exprime le souhait aussi de Tor à poursuivre sa lutte contre la censure d'internet. Dans ce sens, une collaboration avec les développeurs de Mozilla Firefox a pu donner naissance à Snowflake : une extension pour le navigateur Firefox permettant de transformer ce dernier en passerelle afin de partager une connexion RTCweb avec un utilisateur de Tor se trouvant dans une zone où l'internet est censuré. 24 En dehors de cela, la recherche d'innovation continue, la course à la censure étant sans fin. Aujourd'hui, l'identification et le blocage presque systématique des communications Tor en Chine et en Iran par la technologie DPI (deep packet inspection) est l'un des défis majeurs auquel Tor se retrouve confronté.

4 Conclusion

L'anonymat relève un enjeu sociétal conséquent où la collecte d'informations à des fins sécuritaires ou commerciales s'oppose aux droits et libertés individuelles. Existant depuis toujours, ces volontés de contrôle et d'émancipation sont deux opposants d'une guerre d'idées, qui aujourd'hui, continue avec toujours plus de ferveur sur le terrain contesté du World Wide Web. Internet, devenu la clé de voûte de la communication et de l'échange informationnel dans notre monde, est un terrain en perpétuel changement qui se redéfini au rythme de l'évolution des technologies, engendrant à chaque fois une nouvelle "société numérique " et les usages qui lui sont propres. Sur ce terrain changeant, les législations censées encadrer les pratiques ont toujours un cycle de retard et se retrouvent désuètes peu de temps après avoir été promulguées. A cela, s'ajoute la complexité de différences réglementaire d'un territoire à l'autre, sur un réseau, qui lui, ne connaît pas de barrières géographiques. Dans ce combat, Tor apporte une proposition concrète au besoin d'anonymat et de sécurité dans nos sociétés. Un besoin qui, au vu des quantités de données collectées, des nouvelles méthodes publicitaires toujours plus intrusives, et des politiques de surveillances, se fait de plus en plus res-

sentir. Cette protection reste toujours relative : il faut comprendre par-là, qu'aucun système n'est infaillible, et que s'il en existait un, la nature évolutive d'internet ferait qu'il ne puisse le rester indéfiniment. Si l'on observe des évolutions technologiques dans la protection de l'information, on en observe également dans le champ de la collecte et de l'analyse.

L'anonymat et la protection de sa vie privée n'est pas seulement une affaire de technologie mais aussi une question d'hygiène numérique. Or celle-ci commence par une prise de conscience du monde qui nous entoure et par poser une réflexion critique sur la manière dont nous interagissons avec ce dernier.

Références

[1]

[2] Fonctionnement de la navigation privée dans Chrome - Ordinateur - Aide Google Chrome. Support google.

[3] LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL. Technical report.

[4] À quoi correspondent les données à caractère personnel?

[5] Did the FBI Pay a University to Attack Tor Users? | Tor Blog, 2014.

[6] Camille Bosqué. Tor, la face chiffrée d'Internet. *Vacarme*, N° 69(4) :79–98, October 2014.

[7] REY Bénédicte. L'insécurité numérique au quotidien : de la régulation quotidienne aux logiques d'alertes.

[8] Manuel Castells. Ni dieu ni maître : les réseaux, March 2012.

[9] Yann Cleuziou. James C. Scott, La domination et les arts de la résistance. Fragments du discours subalterne.. Paris, Éditions Amsterdam, 2009, 270 p. *Études rurales*, (186), March 2010. Number : 186 Publisher : EHESS.

[10] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor : The Second-Generation Onion Router :. Technical report, Defense Technical Information Center, Fort Belvoir, VA, January 2004.

[11] Eric FILIOL. Statistical and combinatorial analysis of the TOR routing protocol : structural weaknesses identified in the TOR network - Université libre de Bruxelles.

[12] Alice Gairard-Bernard. La réponse sécuritaire de l'administration Bush : l'USA PATRIOT Act et les libertés individuelles. *E-rea. Revue électronique d'études sur le monde anglophone*, (9.1), September 2011. Number : 9.1 Publisher : Laboratoire d'études et de recherche sur le monde anglophone.

[13] Amaelle Guiton. Bernard Cazeneuve s'enfonce dans le «Darknet», March 2016. Library Catalog : www.liberation.fr Section : Futurs.

[14] Markus Huber, Martin Mulazzani, and Edgar Weippl. Tor HTTP Usage and Information Leakage. In Bart De Decker and Ingrid Schaumüller-Bichl, editors, *Communications and Multimedia Security*, Lecture Notes in Computer Science, pages 245–255, Berlin, Heidelberg, 2010. Springer.

[15] The Tor Project Inc. Tor Project : Overview. Library Catalog : 2019.www.torproject.org.

[16] Romain Lecomte. L'anonymat comme « art de résistance ». Le cas du cyberespace tunisien. *Terminal. Technologie de l'information, culture & société*, (105), October 2010.

[17] S.J. Murdoch and G. Danezis. Low-Cost Traffic Analysis of Tor. In *2005 IEEE Symposium on Security and Privacy (S&P'05)*, Oakland, CA, USA, 2005. IEEE.

[18] Guillaume Pillot. Anonymat et vie privée sur internet. 2018. Accepted : 2018-11-21T00 :03 :24Z.

[19] Gerard Wagener and Alexandre Dulaunoy. Torinj : Automated Exploitation Malware Targeting Tor Users. page 7, 2009.

[20] Philipp Winter, Richard Köwer, Martin Mulazzani, Markus Huber, Sebastian Schrittwieser, Stefan Lindskog, and Edgar Weippl. Spoiled Onions : Exposing Malicious Tor Exit Relays. In Emiliano De Cristofaro and Steven J. Murdoch, editors, *Privacy Enhancing Technologies*, volume 8555, pages 304–331. Springer International Publishing, Cham, 2014. Series Title : Lecture Notes in Computer Science.

[21] Philipp Winter and Stefan Lindskog. How China Is Blocking Tor. *arXiv :1204.0447 [cs]*, April 2012. arXiv : 1204.0447 version : 1.