Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

LE PROGRÈS
Le Progrès (Lyon)
Une-JUR-SER, lundi 25 mai 2015, p. Une-JUR-SER1

N/A

# Qu'est-ce que le réseau Tor ?

**Internet.La future loi sur le renseignement suscite beaucoup d'indignation, notamment du côté des professionnels du web. Le réseau Tor est-il une alternative ?**

Alors que le gouvernement veut mettre en place une loi sur le renseignement pour tracer les faits et gestes des internautes français, nombreux sont ceux à la recherche de solutions permettant de ne pas être espionné. Parmi elles figure Tor, un réseau décentralisé et anonyme, permettant de devenir quasiment intraçable sur le Web.

Tor repose sur le principe de réseau mélangé. Cela signifie qu'il est composé d'une multitude de couches de routeurs, tous connectés à Tor, autant de « noeuds » par qui transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. En passant par le réseau Tor, les données personnelles de l'internaute (adresse IP, pays) ne peuvent plus être localisées par les sites visités.

Son application la plus répandue prend la forme d'un navigateur Web du même nom. Il est conseillé aux utilisateurs de Tor de désactiver toutes leurs extensions (telles que Flash ou JavaScript) pour garantir leur anonymat, bien que cela ne restreigne l'accès à certains sites et services. ll est aussi possible de passer par le réseau Tor sous d'autres navigateurs, comme Internet Explorer et Firefox, mais au prix d'une manipulation plus complexe.

D'autres programmes, moins aboutis, permettent également de profiter du réseau. C'est notamment le cas d'une messagerie anonyme et d'un client BitTorrent.

Tor s'est d'ores et déjà imposé pour nombre de geeks américains comme une réponse aux révélations d'Edward Snowden sur l'activité de l'Agence nationale de la sécurité américaine (NSA). Vitrine du Web underground, le réseau jouit néanmoins d'une réputation sulfureuse, car il a est notamment utilisé par de nombreux revendeurs de drogues ou d'armes.

Encore méconnu en France, il bénéficie d'un regain d'intérêt depuis les premières discussions sur le projet de loi sur le renseignement, laquelle prévoit notamment d'installer une « boite noire » chez les fournisseurs d'accès afin de contrôler l'ensemble du trafic des données échangées sur internet en France.

Adopté par une très large majorité à l'Assemblée nationale le mardi 5 mai, le projet de loi sur le renseignement doit maintenant être proposé aux sénateurs.

**Note(s) :**

torproject.org

**Illustration(s) :**

Le réseau Tor revendique 2,5 millions d'utilisateurs quotidiens. Photo DR



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Blogs - Science and technology - Gizmodo
Wednesday, July 02, 2014

# 7 Things You Need to Know About Tor

**Cooper Quntin - EFF**

JUL 02, 2014 - We posted last week about the Tor Challenge and why everyone should use Tor . Since we started our Tor Challenge two weeks ago we have signed up over 1000 new Tor relays. But it appears that there are still some popular misconceptions about Tor. We would like to take this opportunity to dispel some of these common myths and misconceptions.

1. Tor Still Works

One of the many things that we learned from the NSA leaks is that Tor still works. According to the NSA "Tor Stinks" slides revealed by the Guardian last year, the NSA is still not able to completely circumvent the anonymity provided by Tor. They have been able to compromise certain Tor users in specific situations. Historically this has been done by finding an exploit for the Tor Browser Bundle or by exploiting a user that has misconfigured Tor. The FBI-possibly in conjunction with the NSA-was able to find one serious exploit for Firefox that lead to the takedown of Freedom Hosting and exploit of its users. Firefox was patched quickly, and no major exploits for Firefox affecting Tor users appear to have been found since.

As the Tor developers noted in 2004 , if someone is actively monitoring both your network traffic and the network traffic of the Internet service you're communicating with, Tor can't prevent them from deducing that you're talking to that service. Its design does assume that at least one side of the connection isn't being monitored by whomever you're trying to stay private from.

We can conclude from this that Tor has probably not been broken at a cryptographic level. The best attacks on Tor are side-channel attacks on browser bugs or user misconfiguration and traffic correlation attacks.

2. Tor is Not Only Used by Criminals

One of the most common misconceptions we hear is that Tor is only used by criminals and pedophiles. This is simply not true! There are many types of people that use Tor. Activists use it to circumvent censorship and provide anonymity. The military uses it for secure communications and planning. Families use Tor to protect their children and preserve their privacy. Journalists use it to do research on stories and communicate securely with sources. The Tor Project website has an excellent explanation of why Tor doesn't help criminals very much. To paraphrase: Criminals can already do bad things since they will break laws they have much better tools at their disposal than what Tor offers, such as botnets made with malware, stolen devices, identity theft, etc. In fact using Tor may help you protect yourself against some of these tactics that criminals use such as identity theft or online stalking.

You are not helping criminals by using Tor any more than you are helping criminals by using the Internet.

3. Tor Does Not Have a Military Backdoor

Another common opinion that we hear is that Tor was created by the military and so it must have a military backdoor. There is no backdoor in the Tor software. It is true that initial development of Tor was funded by the US Navy. However, it has been audited by several very smart cryptographers and security professionals who have confirmed that there is no backdoor. Tor is open source, so any programmer can take a look at the code and verify that there is nothing fishy going on. It is worked on by a team of activists who are extremely dedicated to privacy and anonymity.

4. No One in the US Has Been Prosecuted For Running a Tor Relay

As far as EFF is aware, no one in the US has been sued or prosecuted for running a Tor relay. Furthermore we do not believe that running a Tor relay is illegal under US law. This is, of course, no guarantee that you won't be contacted by law enforcement, especially if you are running an exit relay. However EFF believes this fact so strongly that we are running our own Tor relay. You can find out more about the legalities of running a Tor relay at the Tor Challenge Legal FAQ . However, if you are going to use Tor for criminal activity (which the Tor project asks that you not do)

you can create more problems for yourself if you get prosecuted. Criminal activity also brings more scrutiny on to Tor making it worse for the public as a whole.

5. Tor is Easy to Use

You might think that because it is privacy software Tor must be hard to use. This is simply not true. The easiest way to get started with Tor is to download the Tor Browser Bundle . This is a browser that comes pre-configured to use Tor in a secure manner. It is easy to use and is all you need to start browsing with Tor. Another easy way to use Tor is with Tails . Tails is a live operating system that runs on a DVD or thumb drive. Tails routes your entire Internet connection through Tor. And when you shut it down, Tails "forgets" everything that was done while it was running.

6. Tor is Not as Slow as You Think

It is true that Tor is slower than a regular Internet connection. However, the Tor developers have been doing a lot of hard work to make the Tor network faster. And it is faster today than ever before. One of the best things that can be done to speed up the Tor network is to create more relays. If you would like to contribute to making the Tor network faster, you can check out our Tor Challenge

7. Tor is Not Foolproof

Tor is not perfect; you can destroy your own anonymity with Tor if you use it incorrectly. That's why it is important to always use Tor Browser Bundle or Tails and make sure that you keep your software up to date. It is also important to remember that if you log into services like Google and Facebook over Tor, those services will still be able to see your communications within their systems. Additionally Tor users should be mindful of the fact that an adversary who can see both sides of there connection may be able to perform a statistical analysis to confirm that the traffic belongs to you.

Tor is some of the strongest anonymity software that exists. We think that it is important to dispel misconceptions about it so that the public can be more informed and confident in its usefulness. There are many great reasons to use Tor and very few reasons not to. So get started with Tor, and take back your privacy online.

This article first appeared on the Electronic Frontier Foundation and is reproduced here under the Creative Commons license.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

Micro Pratique, no. No 229
DOSSIER, jeudi 1 octobre 2015, p. 44,45

INTERNET ET VIE PRIVÉE

# Préservez votre vie privée

**Dossier réalisé par Jean-Michel Plisson**

**Vos données personnelles et votre vie privée sont de plus en plus menacées sur Internet. Même si des options, des paramètres et des outils permettent de protéger plus ou moins votre sphère privée, le plus simple et le plus efficace est encore d'adopter de bons comportements sur Internet.**

De très nombreux sites et services vous demandent de vous inscrire en créant un compte. Il faut généralement indiquer un pseudo, une adresse mail et un mot de passe. Le problème est que vous donnez votre adresse mail à un site que vous ne connaissez pas et que vous n'utiliserez peut-être plus.

## Utilisez une messagerie jetable

Au lieu de fournir votre véritable adresse mail, vous pouvez fournir une adresse jetable. Yopmail (www.yopmail.com) est un site Web qui vous procure gratuitement une adresse mail jetable. Son utilisation est simplissime :

Vous indiquez l'adresse de votre choix à yopmail.com lorsque vous vous inscrivez sur un site. Par exemple, jj3429ca@yopmail.com. Choisissez ce que vous voulez, cela n'a pas d'impor tance.

Connectez-vous à yopmail.com.

- Dans le champ **Saisissez le mail jetable de votre choix,** communiquez l'adresse mail que vous avez choisie.

- Cliquez sur **Vérifier les mails.**

## Utilisez une messagerie chiffrée

Les internautes échangent beaucoup de mails et ces mails contiennent souvent des informations confidentielles comme des identifiants ou des mots de passe. Vos messages transitent par les serveurs de votre fournisseur de messagerie. Ils ne sont pas à l'abri des services d'écoute et d'espionnage et, sans être paranoïaque, ils ne sont pas à l'abri des grands collecteurs de données.

Si vous souhaitez préserver la confidentialité de vos correspondances, vous pouvez chiffrer vos messages. Vous disposez de plusieurs solutions pour cela. Vous pouvez utiliser la messagerie Web chiffrée ProtonMail (https://protonmail.ch/) ou installer l'extension Mailvelope (https://www.mailvelope.com/) compatible avec toutes les messageries Web.

## Surfez en toute confidentialité

Votre fournisseur d'accès à Internet peut collecter des données pendant vos navigations. Les sites sur lesquels vous vous connectez tentent également de collecter des données. Pour empêcher cela, surfez anonymement sur Internet en utilisant Tor. Tor sécurise votre navigation Internet en routant votre connexion à travers plusieurs routeurs et en chiffrant les données que vous échangez.

Il était assez difficile d'utiliser Tor jusqu'à ce que Tor Browser soit mis en ligne. Tor Browser est un navigateur Internet basé sur Firefox. Il comprend des modules qui permettent de se connecter au réseau Tor très facilement.

## Utilisez un moteur qui n'espionne pas

Les moteurs de recherche comme Google ou Bing utilisent certaines de vos données personnelles pour vous présenter de meilleurs résultats de recherche et, surtout, pour vous présenter de la publicité ciblée. Vous pouvez très facilement utiliser un moteur de recherche qui ne vous piste pas et qui garantit ne collecter aucune donnée personnelle. Il en existe deux qui sont très efficaces et qui fournissent de bons résultats de recherche :

DuckDuckGo
https: //duckduckgo.com/) et Qwant (https://www.qwant.com/).

## Soyez vigilant

Protéger sa vie privée, c'est bien mais ce n'est pas suffisant. En effet, vous n'êtes pas seul à publier des informations personnelles vous concernant, vos proches et connaissances le font également. Cela peut être des photos, des informations, des statuts... Vous devez donc vous assurer qu'aucune information personnelle vous concernant n'est publiée sur Internet. Le service Google Aler te (www.google.fr/alerts) est idéal pour cela. Google Alertes est un outil gratuit qui surveille en permanence Internet et vous alerte dès qu'apparaissent un ou plusieurs mots que vous avez indiqués. Créez une alerte sur votre "prénom nom", une autre sur vos numéros de téléphone, une autre sur le pseudonyme que vous utilisez le plus souvent. Google Alertes vous enverra un message dès que les mots clés que vous avez définis apparaîtront sur le Web.

**Encadré(s) :**

**À SAVOIR Surveillance de vos données personnelles**

Les récentes lois relatives à la surveillance des informations circulant sur Internet permettent aux autorités de police de demander des informations aux grandes entreprises du Web comme Facebook, Google, Apple... sans réquisition judiciaire. Facebook, Apple et Microsoft ont annoncé qu'ils préviendraient leurs utilisateurs lorsqu'une demande d'accès à des informations sera transmise par la police sans justification judiciaire. Seules les demandes formulées par un juge resteront secrètes ainsi que les demandes dont la divulgation pourrait entraîner un risque ou une mise en danger.

**IMPORTANT Portez plainte en ligne avec la CNIL**

Normalement, vous pouvez demander la suppression ou la rectification des données personnelles vous concernant publiées sur Internet. En pratique, cela est difficile car il faut trouver les coordonnées de l'éditeur de site et il faut que l'éditeur du site réponde à votre demande. En cas d'impossibilité de supprimer, de faire supprimer, de rectifier ou de faire rectifier des données personnelles vous concernant publiées sur un site Web, vous pouvez faire appel à la CNIL (Commission Nationale de l'Informatique et des Libertés).

La page http://goo.gl/TRQ7QDpermet de porter plainte en ligne auprès de la CNIL.

Pour les plaintes concernant Internet, le cas de suppression des informations est prévu.

Pour porter plainte auprès de la CNIL, vous devez :

- avoir adressé une demande au site Web concerné,

- attendre la réponse pendant au moins deux mois,

- disposer d'une copie de vos démarches.

**PRATIQUE Paramétrez votre smartphone**

Vos données personnelles risquent d'être collectées et divulguées lorsque vous utilisez votre smartphone. En fait, le risque est plus important avec un smartphone qu'avec un ordinateur car vous disposez de moins d'outils pour vous défendre. Vous devez être vigilant lorsque vous vous connectez sur un réseau Wi-Fi et être certain qu'il s'agisse bien d'un vrai réseau et non pas d'un réseau installé spécialement pour pirater vos données. En plus de cela, vous pouvez demander à minimiser le suivi publicitaire et désactiver la géolocalisation de certaines applications.

**LIMITEZ LE SUIVI PUBLICITAIRE**

Votre iPhone ou votre Android dispose d'un paramètre permettant de limiter le suivi publicitaire. Cette option réinitialise l'identifiant Ad-in utilisé par les publicités. Cet identifiant est un peu l'équivalent des cookies sur votre ordinateur.

- Sur un iPhone : ouvrez l'appli Réglages, **touchez** Confidentialité **puis** Publicité. **Activez le paramètre** Suivi publicitaire limité.

- **Sur un Android : ouvrez les paramètres et sélectionnez** Annonces. **Désactivez l'option** Annonces par centre d'intérêt.

**DÉSACTIVEZ LA GÉOLOCALISATION DE CERTAINES APPLIS**

De très nombreuses applications accèdent à la géolocalisation de votre smartphone même lorsqu'elles n'en ont pas besoin. Par souci de confidentialité et pour économiser la batterie, nous vous conseillons de désactiver le service de géolocalisation des applications qui n'en ont pas besoin pour fonctionner.

- Sur un iPhone : ouvrez Réglages, **touchez** Confidentialité **et** Service de localisation.

**Passez en revue la liste d'applications pouvant utiliser le service de localisation et désactivez**

**le service pour les applications qui n'ont pas besoin de vous localiser.**

- Sur Android, vous ne pouvez pas désactiver le service de localisation pour certaines applications et le conserver actif pour d'autres. Vous pouvez simplement désactiver ou activer la localisation globale. Ouvrez les paramètres, sélectionnez Position **et désactivez le paramètre.**

**Illustration(s) :**

Tor Browser est un navigateur Web permettant de se connecter très facilement au réseau Tor, de manière à surfer anonymement en toute sécurité.

Yopmail est une messagerie jetable qui vous propose des adresses mail temporaires et anonymes. C'est idéal pour s'inscrire sur tous les petits sites Web qui vous obligent à créer un compte pour vous connecter.

Google Alertes vous envoie un message dès que de nouveaux résultats de recherche apparaissent sur Internet. C'est en quelque sorte une recherche permanente. Vous êtes de cette manière informé très rapidement dès que votre nom est mentionné sur Internet ce qui autorise une réaction rapide.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde.fr
Le Monde.fr
jeudi 3 juillet 2014

# TOR, logiciel-clé de protection de la vie privée, dans le viseur de la NSA

On savait que The Onion Router (TOR, « le routeur oignon »), outil très puissant qui permet de contourner la censure et d'anonymiser sa navigation sur Internet, posait problème à la National Security Agency (NSA). Mais des documents publiés jeudi 3 juillet par la chaîne allemande Das Erste détaillent la surveillance très poussée, et aux marges de la légalité, dont font l'objet les gestionnaires et les volontaires de ce programme, en Europe et aux Etats-Unis.

TOR est un réseau d'ordinateurs : lorsqu'un utilisateur cherche à se connecter à un site, ses données cheminent par de multiples points du réseau, chaque étape constituant une couche de chiffrement. L'avantage est double : la connexion est intraçable (on ne sait pas qui se connecte, et de quel ordinateur) et il est impossible, la plupart du temps, de voir le contenu de la discussion.

Financé en partie par... l'administration américaine, qui y voit un outil d'aide aux activistes, dissidents ou journalistes dans des régimes répressifs pour contrecarrer la censure et protéger leur vie privée et celle de leurs sources, il a aussi été adopté par toutes sortes de criminels, notamment des groupes terroristes, ce qui explique en partie l'intérêt de la NSA.

La chaîne de télévision allemande a pu se procurer le code informatique du logiciel de la NSA XKeyscore, utilisé pour diverses opérations de surveillance, et ainsi en détailler le fonctionnement et ses cibles.

## La NSA surveille des serveurs cruciaux du réseau

Plusieurs serveurs centraux, faisant office de noeuds cruciaux au sein du réseau TOR, ont été spécifiquement et constamment surveillés. L'un d'entre eux, situé à Nuremberg, en Allemagne, appartient à Sebastian Hahn, une figure *« particulièrement respectée dans la communauté TOR »*, souligne la chaîne allemande. Plusieurs autres serveurs de ce type, en Europe mais aussi aux Etats-Unis, faisaient l'objet d'une surveillance.

## Mais aussi les mails adressés à l'équipe gérant TOR, notamment des activistes du monde entier

Certains pays, comme l'Iran ou la Chine, bloquant systématiquement TOR, il est possible pour les activistes et les dissidents de ces pays de réclamer une liste de serveurs privés, plus discrets, pour se connecter au réseau. Il s'avère que tous ces mails, provenant d'utilisateurs du monde entier, étaient interceptés par la NSA.

## Et de simples visiteurs de sites Web

Enfin, la NSA a consigné les visites de tous les internautes se rendant sur le site de TOR, sur celui de Tails (The Amnesic Incognito Live System, un autre outil de protection de la vie privée) et de LinuxJournal (une publication spécialisée dans le système d'exploitation Linux).

Toutes les visites sur plusieurs sites proposant des solutions pour protéger sa vie privée, dont certains sont situés aux Etats-Unis (l'un d'entre eux est sur le campus du Massachusetts Institute of Technology (MIT), sur la côte est du pays), ont été également consignées et sont accessibles aux analystes de la NSA grâce à leur outil XKeyscore.

## TOR, encore inviolé

Rien n'indique, dans l'enquête de Das Erste, que le coeur du fonctionnement de TOR ait été compromis. Le *Guardian* avait déjà fait état des efforts, vains, de la NSA pour venir à bout des protections que confère TOR à ses utilisateurs.

La surveillance de la NSA concerne soit des serveurs situés au coeur du réseau, limitant ce qu'ils peuvent apprendre sur ceux qui les utilisent, soit des sites en dehors du réseau TOR.

Ces révélations montrent à quel point la NSA se méfie des outils permettant de protéger et de camoufler sa connexion. Tails est ainsi décrit dans un document comme un outil *« utilisé par des extrémistes »* (il est en réalité avant tout destiné aux activistes et aux journalistes afin de protéger leur utilisation d'un ordinateur en n'y laissant aucune trace).

Roger Dingledine, un des principaux développeurs de TOR, a été joint par la chaîne allemande et s'est voulu rassurant :

« Nous réfléchissons à la surveillance étatique depuis des années, à cause de notre travail dans des lieux où les journalistes sont menacés. L'anonymat conféré par TOR se fonde sur le grand nombre d'utilisateurs. Observer le trafic à un endroit précis du réseau, même central, ne suffit par à le casser. »

En théorie, la NSA ne peut pas collecter des données concernant des Américains. Or, dans le cas présent, plusieurs sites et utilisateurs américains ont directement été ciblés.

Interrogée par la chaîne allemande, la NSA s'est défendue de la façon habituelle :

« La NSA collecte ce qu'elle est autorisée à collecter par la loi, concernant des cibles valides de surveillance, quel que soit le moyen technique employé par ces cibles. »

>> Jouer à notre jeu : Tentez d'échapper à la surveillance de la NSA

**Les problèmes légaux**



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde.fr
Le Monde.fr
jeudi 16 février 2012

# Un nouvel outil contre la cybercensure testé en Iran

Les autorités iraniennes ont encore renforcé leur étau sur Internet. Entre le 9 et le 11 février, plus de 30 millions d'Iraniens n'ont plus pu accéder à leur messagerie en ligne, rapporte ainsi le blog Nouvelles d'Iran . Pour les sites spécialisés, l'origine de cette "panne" est simple : le régime a décidé de bloquer les adresses Web utilisant le protocole https , version cryptée et *"sécurisée"* des pages Web.

La conséquence, note Hacker news , est que les sites d'entreprises américaines comme Google et Yahoo ! ne sont pas les seuls bloqués : les services bancaires sont également affectés. Le site blockediniran permet de vérifier quelles adresses Internet ont été bannies par les autorités. Mercredi 15 février, Google.com et Yahoo.com étaient de nouveau disponibles, y compris dans leurs versions sécurisées.

## TRIPLE MÉTHODE DE BLOCAGE

*"Ces coupures d'accès à Internet ont été concomitantes des célébrations organisées à l'occasion du 33e anniversaire de la Révolution"*, note Nouvelles d'Iran. D'après le blog Tor project , qui conçoit un logiciel permettant de contourner la censure en ligne, trois méthodes ont été utilisées pour rendre impossible l'accès à ces sites.

Le gouvernement a ainsi procédé à une inspection des paquets en profondeur (en anglais *"Deep Packet Inspection"* ou DPI), du trafic des certificats SSL. Ces certificats sont utilisés par les navigateurs Internet pour vérifier qu'un site est bien un original et non une version détournée. Cette méthode a été complétée par un blocage sélectif de certaines adresses IP et par un filtrage de certains mots-clés. *"L'Iran expérimente la détection et la manipulation de certificats SSL depuis au moins un an"*, explique Andrew Lewman, directeur exécutif du projet Tor, contacté par le Monde.fr.

Lors des coupures, le nombre d'utilisateurs du programme d'anonymisation Tor a d'ailleurs connu une baisse significative , entre le 10 et le 12 février, alors que le pays compte entre 50 000 et 60 000 utilisateurs de Tor. *"La raison en est simple. Tor utilise le SSL, s'il est bloqué ou ralenti, il en est de même pour Tor"*, résume M. Lewman.

## MÉTHODE EXPÉRIMENTALE

Mais, avec un nouveau système, baptisé *" Obfsproxy "*, Tor semble avoir trouvé une nouvelle parade. Si la solution technique est complexe, encore expérimentale et donc pas encore "clé en main" pour l'utilisateur, le principe est simple : il s'agit de masquer le fait que l'internaute utilise un certificat SSL. Plusieurs milliers d'internautes iraniens utiliseraient cette version de test, indiquent les personnes à l'origine du projet Tor.

Ce jeu du chat et de la souris sur Internet semble infini. Mais pour Andrew Lewman, il sera très difficile pour le régime iranien de lutter contre *"Obfsproxy"*. *"La vraie option serait de déconnecter l'Iran d'Internet. Mais j'imagine que la réaction sera bien plus violente que face à la tentative actuelle de manipuler des certificats SSL"*, prévient Andrew Lewman. C'est pourtant ce qu'il s'était passé il y a un an en Egypte . Afin de contenir les manifestations de la population, les autorités avaient ordonné une coupure d'Internet dans l'ensemble du pays.

Classé dans la liste des *"dix pays ennemis de l'Internet"*, l'Iran a vu *"la censure des sites d'information traitant de politique ou de droits de l'homme considérablement renforcée"*, selon Reporters sans frontières . Depuis un an, le pays dispose par exemple d'une *"cyberpolice"* chargée d'assurer le contrôle du Net.

LEMONDE.FR Laurent Checola

**Retour à la table des matières**

**RFI (site web) (français)**
vendredi 27 décembre 2013

# Etats-Unis / Drogue - Le FBI peut-il arrêter Silk Road, l' « eBay de la drogue » ?

USA / Drugs - The FBI Can Stop Silk Road, the "eBay of drugs?"

Créé en 2011 par un jeune Américain créatif en affaires et en technologie, Silk Road proposait de la drogue sur internet payable en Bitcoin, la monnaie électronique.

La traque continue. Si la Route de la soie, la vraie, commençait en Chine et menait jusqu'en Syrie médiévale, celle de Silk Road (« Route de la soie » en anglais) part, elle, tous azimuts. Vendredi 20 décembre, trois hommes ont été arrêtés - l'un aux Etats-Unis, le deuxième en Irlande et le troisième en Australie - pour leur participation présumée à ce vaste réseau de vente de stupéfiants par internet dénommé donc Silk Road et surnommé l' « eBay de la drogue », une définition qui rend tout de suite les choses plus claires.

Supermarché de la drogue

Comme sur eBay en effet, les acheteurs y choisissaient leurs produits d'après photo, les payaient en ligne - mais uniquement en Bitcoins (la fameuse monnaie électronique) - avant d'être livrés à domicile par voie postale, ni vu ni connu. Première différence avec eBay cependant, il s'agissait d'un commerce illégal puisqu'il ne concernait pas des biens de consommation courante mais des substances illicites : héroïne, cocaïne, haschisch, marijuana, ecstasy, etc. ... un véritable supermarché de la défonce, en ligne.

Autre différence avec eBay, on ne trouvait pas Silk Road sur l'internet classique mais via Tor (acronyme de The Onion Router), un réseau informatique mondial parallèle et superposé (comme les pelures d'un oignon, d'où le nom) qui garantit un anonymat sinon total du moins partiel à ses utilisateurs. Tor attire ainsi quantité d' « alternautes » pour des motifs louables ou inavouables, selon les cas car il permet tout aussi bien l'échange de recherches scientifiques que les trafics les plus divers (drogue, armes, faux papiers, pédopornographie etc.).

Le 1er octobre dernier, les non-initiés ont découvert l'existence de Silk Road lors de l'arrestation de celui qui est accusé d'en être le cerveau, Ross William Ulbricht, un Américain de 29 ans qui pilotait le site depuis février 2011. Pisté par le FBI sans succès depuis deux ans, Ulbricht se croyait intouchable. Il avait même accordé une interview au magazine Forbes sous son pseudo opérationnel de « Dread Pirate Roberts » un mois avant son arrestation.

Cueilli comme un débutant

Il s'est pourtant fait cueillir bêtement dans une bibliothèque de San Francisco pour avoir associé, sous un autre pseudonyme, un message vieux de deux ans à sa véritable adresse électronique : rossulbricht@gmail.com, ce qui a permis au FBI de remonter sa trace par recoupement d'informations. Inculpé de trafic de stupéfiants, de complot, de conspiration, de piratage informatique et de blanchiment d'argent, Ulbricht aurait accumulé une véritable fortune électronique évaluée à 33 millions de dollars (24 millions d'euros) en Bitcoins.

L'accusé, qui est incarcéré au centre de détention de Brooklyn à New York, risque de ne pas profiter avant longtemps de sa fortune plus que jamais virtuelle car la justice américaine l'accuse également d'avoir commandité plusieurs assassinats auprès de tueurs à gage recrutés également via Silk Road, ce qui pourrait lui valoir de très longues années derrière les barreaux, l'un des tueurs à gage contactés n'étant autre qu'un agent du FBI infiltré, selon l'enquête.

Dans la foulée de l'arrestation d'Ulbricht, les autorités ont fermé Silk Road séance tenante. Le site comptait alors près d'1 million d'utilisateurs dont environ 200 000 étaient, selon le FBI, enregistrés comme acheteur ou vendeur. En moins de deux ans d'existence, Silk Road avait vu passer pour 1,2 milliard de dollars de transaction (875 millions d'euros) et, le jour de l'arrestation, les agents fédéraux ont saisi 3,6 millions de dollars en Bitcoins provenant d'une centaine d'achats effectués sur le site, au grand dam des usagers.

Sitôt fermé, sitôt rouvert

Un peu plus d'un mois plus tard, le 6 novembre, Silk Road a néanmoins fait sa réapparition sur l'internet parallèle dans une version 2.0 censée être plus sécurisée, de quoi donner du corps aux affirmations d'Ulbricht selon lesquelles il n'était pas le seul cerveau du réseau. Même si les autorités américaines laissent logiquement filtrer très peu d'informations sur l'enquête, il semble bien que les trois arrestations de vendredi dernier soient autant en corrélation avec la nouvelle version de Silk Road qu'avec l'ancienne.

Appréhendé à Brisbane en Australie, Peter Nash, 40 ans, officiait en tant que modérateur du site sous les pseudonymes de « Batman73 » et « Anonymousasshit » depuis janvier 2013, selon le chef d'accusation formulé par le parquet de New York qui s'est saisi de l'affaire. Andrew Jones, 24 ans, arrêté dans l'État de Virginie, et Gary Davis, 25 ans, interpellé à Wicklow en Irlande étaient pour leur part des administrateurs de Silk Road dans leur région respectives sous les pseudos d' « Inigo » pour Jones et de « Libertas » pour Davis. Les trois hommes sont accusés de trafic de drogue, de piratage informatique et de blanchiment d'argent.

S'il ne fait guère de doute que le portail va être à nouveau fermé, il y a fort à parier qu'il réapparaîtra sous une autre forme, ou sous un autre nom. Prenant les devants, un administrateur répondant au pseudo de Defcon a d'ailleurs fermé la plateforme lundi 23 décembre, promettant de la rouvrir ce samedi 28 décembre D'ailleurs des alternatives à Silk Road ont éclos sous des noms aussi évocateurs qu'Atlantis ou Black Market Reloaded. D'autres encore verront certainement le jour dans les entrailles du Darknet, sur d'autres réseaux parallèles que Tor, soupçonné d'être trop perméable aux grandes oreilles de la justice.

En attendant, les agents fédéraux continuent de mener l'enquête en communiquant au minimum. Quant à Ross William Ulbricht, il a décidé de contre-attaquer et accuse le FBI de lui avoir prélevé illégalement ses 33 millions de Bitcoins, preuve que le jeune entrepreneur ne manque ni d'aplomb, ni de ressource.

More videos available on http://www.rfi.fr/ (http://www.rfi.fr/)

USA / Drugs - The FBI Can Stop Silk Road, the "eBay of drugs?"

Created in 2011 by a young American creative business and technology, Silk Road offered drugs on internet payable Bitcoin electronic currency.

The hunt continues. If the Silk Road, the true, began in China and led until medieval Syria, the Silk Road ("Silk Road" in English) hand it all over the place. Friday, December 20, three men were arrested - one in the United States, the second in Ireland and the third in Australia - for their alleged that vast network of drug sales by internet so called Silk Road, nicknamed the participation "eBay drugs", a definition that makes immediate things clearer.

Drug supermarket

As on eBay, in fact, buyers are choosing their products after photo, the paid online - but only Bitcoins (the famous electronic money) - before being delivered to your home by mail, neither seen nor known. First difference with eBay, however, it was an illegal trade it did not affect the consumer goods but illegal drugs: heroin, cocaine, hashish, marijuana, ecstasy, etc.. ... A real supermarket smashes, online.

Another difference with eBay, it was not Silk Road on the classic internet but via Tor (The Onion Router acronym), a global computer network parallel and superimposed (like layers of an onion, hence the name) that guarantees total anonymity if at least part to its users. Tor and attracts amount of "alternautes" for good motives or shameful, as appropriate because it allows as well the exchange of scientists that the most diverse (drugs, weapons, false documents, pornography etc.). Traffic research.

On October 1st, the uninitiated have discovered the existence of Silk Road during the arrest of the man accused of being the brain, Ross William Ulbricht, an American 29 year old who drove the site since February 2011 . Tracked by the FBI unsuccessfully for two years, Ulbricht thought untouchable. He even granted an interview with Forbes magazine under his operational nickname "Dread Pirate Roberts" a month before his arrest.

Picked as a beginner

It is however foolishly pick from a library of San Francisco to have associated under another pseudonym, an old post from two years to his real email address: rossulbricht@gmail.com, which allowed the FBI to trace his track by cross-checking information. Charged with drug trafficking, conspiracy, conspiracy, hacking and money laundering, Ulbricht had accumulated a fortune estimated at real e 33 million dollars (24 million euros) in Bitcoins.

The accused, who is incarcerated at the detention center in Brooklyn, New York, may not take long before her more than ever virtual fortune because the U.S. Justice also accused of ordering several murders with killers also recruited via the Silk Road, which could earn him many long years behind bars, one of the killers being contacted other than undercover FBI agent, according to the survey.

In the wake of the arrest of Ulbricht, the authorities closed Silk Road forthwith. The site then had nearly 1 million users of which about 200,000 were, according to the FBI, registered as buyer or seller. In less than two years of existence, Silk Road had seen go for $ 1.2 billion transaction (875 million) and the day of the arrest, federal agents seized $ 3.6 million in Bitcoins from one hundred purchases made on the site, to the chagrin of users.

Soon closed, reopened soon

A little over a month later, on November 6, Silk Road has nevertheless made its reappearance on the parallel internet in a more secure version 2.0 expected, enough to give body to the assertions that he Ulbricht n ' was not the only brain network. Even if the U.S. authorities allow logically filter very little information about the investigation, it appears that the three arrests last Friday are all correlated with the new version with the old Silk Road.

Apprehended in Brisbane, Australia, Peter Nash, 40, officiated as moderator of the site under the pseudonyms "Batman73" and "Anonymousasshit" since January 2013, according to the charge made by prosecutors in New York s' is hearing the case. Andrew Jones, 24, arrested in the state of Virginia, and Gary Davis, 25, arrested in Wicklow in Ireland for their part were directors of Silk Road in their respective area under the pseudonyms of "Inigo" for Jones and of "Libertas" for Davis. The three men are accused of drug trafficking, software piracy and money laundering.

While there is little doubt that the gate will be closed again, there is a good chance they will reappear in another form, or by any other name. Taking the lead, responding to an administrator username Defcon has also closed platform Monday, December 23, promising to reopen this Saturday, Dec. 28 Moreover alternative to Silk Road hatched under names as evocative Atlantis or Black Market Reloaded. Still others might see the date in the bowels of the Darknet, other parallel networks Tor, suspected of being too permeable to large ears of justice.

Meanwhile, federal officials continue to investigate communicating to a minimum. As for Ross William Ulbricht, he decided to strike back against the FBI and accused him of illegally taken its 33 million Bitcoins, proof that the young entrepreneur lacks neither plumbing nor resource.

More videos available on http://www.rfi.fr/ (http://www.rfi.fr/)



Numéro de document : news·20131227·SRFA·men-127922-13881565636450693989

PUBLI-© news·20131227·SRFA·men-127922-13881565636450693989

Ce certificat est émis à à des fins de visualisation personnelle et temporaire.

Date d'émission : **2016-04-08**

Le Monde
Le Monde
Économie et Entreprise, mardi 12 novembre 2013, p. SCQ4

Eco et Entreprise

Economie et entreprise

# Le site illégal Silk Road est rouvert, un mois après sa fermeture par le FBI

L'ancien propriétaire de la plate-forme de vente de stupéfiants est poursuivi par la justice américaine

Guénael Pépin

Plus d'un mois après sa disparition, le site Internet de vente de produits illégaux Silk Road est de retour. Le 6 novembre, « Silk Road 2.0 » a été mis en ligne, pour reprendre un flambeau très convoité, celui de la vente de stupéfiants.

*« Le FBI a mis deux ans pour faire ce qu'ils ont fait. Mais il n'a obtenu que quatre semaines de silence »* , affirment fièrement, dans un message en tête du site, ses nouveaux responsables, dont les identités ne sont pas connues, mais qui reprennent le pseudonyme - Dread Pirate Roberts - endossé par les précédents « propriétaires » .

Cette réouverture est intervenue alors que Ross William Ulbricht, le propriétaire présumé de Silk Road première version, comparaissait pour la première fois devant une cour new-yorkaise. Il est, notamment, accusé de piratage informatique, de trafic de drogue et de blanchiment d'argent.

Le maître présumé de Silk Road, considéré comme un petit empire de la drogue, avait été arrêté le 1er octobre et le site fermé dans la foulée. Malgré ses nombreuses mesures de précautions, le responsable du site aurait été trahi par une adresse e-mail utilisée sur un forum des années auparavant.

Silk Road n'est pas accessible comme n'importe quel autre site Internet. C'est un site « caché » : pour y accéder, il faut passer à travers le réseau TOR ( *The Onion Router* , soit le routeur oignon), qui rend anonyme l'activité des utilisateurs sur la Toile. La fermeture de Silk Road par le FBI avait constitué un choc pour les utilisateurs de TOR, un réseau considéré intraçable.

Silk Road, qui fonctionne comme une place de marché, se rémunérant par commission sur les ventes, utilise comme moyen de paiement la monnaie numérique bitcoin, qui échappe encore à toute régulation.

**Prise record de bitcoins**

Lors de l'arrestation de Ross William, 26 000 bitcoins ont été saisis, soit 0,2 % du total en circulation à l'époque. Une prise record dont la valeur fluctue au gré de la valorisation de cette monnaie alternative, qui atteint désormais plus de 300 dollars. En plus des sécurités de la première version, pour protéger l'identité des vendeurs et des acheteurs, le nouveau Silk Road permet de signer les transactions avec une clé spécifique.

Quelque 12 500 personnes se seraient inscrites une journée après la réouverture de Silk Road. Même si les anciens vendeurs sont toujours recherchés par la police, de nouvelles annonces sont très rapidement réapparues.

Le réseau caché TOR est particulièrement ciblé par la police américaine. En août, le FBI avait fermé Freedom Hosting, considéré comme le premier hébergeur mondial de sites pédophiles, également réservé aux utilisateurs de TOR. La grande majorité des sites accessibles par le réseau anonyme y étaient hébergés. Le propriétaire de Freedom Hosting a été arrêté et des pièges ont été posés sur les sites pour démasquer les internautes.



Numéro de document : news·20131112·LM·0s1211_871301

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Chennai online (web site)
Tuesday, March 10, 2015 - 23:58 UTC -0400

# The Silk Road a Billion Dollar Black Market

**What is Silk Road?**

Not too many of us aware about **Bitcoins** (https://bitcoin.org/en/), the currency of future. But for Ross William Ulbrich, Bitcoins are just like the normal money we use everyday. He made over a billion dollars by creating a market place for drugs called "Silk Road" just like eBay in the **deepweb** (http://en.wikipedia.org/wiki/Deep_Web). Federal authorities confirms that Ross Ulbricht is Dread Pirate Roberts, the cyber name for the admin of online anonymous drug market the Silk Road. Ulbricht was arrested in Oct. He is accused of narcotics trafficking, computer hacking, money laundering and hiring hitmen for several murders. He was denied bail on Nov. 21, 2013 in a New York district court.

**How did he build it?**

Silk Road was able to do about $1.2 billion in net sales during the two years if its operation. Illegal narcotics, drugs, Marijuana to cocaine can be purchased from anoynomus sellers. The sellers and the buyers were kept anonymous by using **Tor** (https://www.torproject.org/index.html.en) (Designed by onion routing project of the U.S. Naval Research Laboratory.) and paid for their goods in cryptocurrency Bitcoin.

Federal officials also allege that Ross Ulbricht tried to gain citizenship in the island nation of Dominica and top flee from US to continue operating the Silk Road Market Place. This is the main document shared as an evidence against granting Ulbricht bail on Nov. 21, 2013.

He was known as Dread Pirate Roberts, the leader of "the Silk Road". Silk Road was created in February 2011 The name "Silk Road" is inherited from the historical trade routes during the Han Dynasty (206 BC - 220 AD), between Europe, India, China, and many other countries on the Afro-Eurasian landmass. Silk Road was operated by the pseudonymous "Dread Pirate Roberts" (the fictional character from The Princess Bride), who was famous for espousing libertarian ideals and criticizing regulation.

The authorities were able to track down 9 ID's of Ross William Ulbrich which were also furnished as an evidense against the approval of bail for Mr. Ross William Ulbrich. FBI agents arrested Ross Ulbricht on Oct. 1, 2013 from the Glen Park library in San Francisco. He is currently in a Brooklyn detention center after after the denial of bail on Nov. 21, 2013. The FBI was also able to shutdown the illegal marketplace on Oct. 2, 2013 and all operation of the anonymous online narcotics marketplace was put to an end.

FBI said they were able seize $28.5 Million In Bitcoins From Ross Ulbricht, The owner of Silk road. The bureau has seized a collection of 144,000 bitcoins, the biggest seizure of cryptocurrency ever , close to $28.5 million. One username that's waht changed his life, he was living under the shadows and kept a very low profile. The FBI would have never captured him if he didn't post in a coding forum under the username " Frosty". The Laptop seized along with Ross Ulbricht had this proof which is also standing in support of the allegation against him.

The seizure of his laptop also revealed that, he operated an administrator account to manage the silk road transactions under "mastermind", A Tor based URL. This page also revealed that he ad almost 6.8 Million Bitcoins at that time. He also used a Tor based **chat client** (http://en.wikipedia.org/wiki/TorChat) to perform official silk road communications.

His friends and family started the Ross Ulbricht Defense Fund in Nov. 2013 to raise money for the legal fees. The fund calls him, "a peaceful, honest citizen," the **fund's website** (http://freeross.org/) is seeking to raise up to $500,000 in donations.

Shutting down The Silk Road will not retaliate the Bitcoin E-commerce, developers have come up with a new solution to anyone can privately and directly buy and sell goods online with no mediators. They describe it as "pseudonymous, uncensored trade."

There is virtually no hosting on any servers, **OpenBazaar** (https://openbazaar.org/index.html) can be installed in any computer, and allows the users to list products in the form of "distributed hash table," a database with is spread among millions of computers across the globe. The devlopers say that they

will not support drug trade but even they don't have any control over theservice they've designed. Anyone can sell or buy anything, practically it is impossible to track the sales.

When **Napster** (http://en.wikipedia.org/wiki/Napster) , the peer to peer music streaming service was shut down, the devlopers came up with **Bittorrent** (http://www.bittorrent.com/). This is the exact replica of the situation. When the silk road is down, another channel is open and which is practically impossible to track and in fact no one even can touch a tiny glimpse of it.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

La Tribune (France), no. 5752
Focus, samedi 18 juillet 2015, p. 13

Internet

# Darknet : l'Internet invisible, lieu de tous les crimes...

**Charles de Laubier**

**Internet est-il devenu synonyme d'interlope? Le Web souterrain, qui échappe aux moteurs de recherche, aux navigateurs Internet et même aux cyberpoliciers, est devenu à la fois le terrain de jeu des activistes anonymes et l'arme virtuelle du cybercrime organisé. La face immergée du cyber-iceberg est trois fois plus vaste que sa partie visible. Le Deep Web et le Dark Net constituent-ils une menace pour nos libertés et démocraties? Ou permettent-ils de se protéger contre la surveillance généralisée?**

Le Conseil constitutionnel devra se prononcer - à la demande de La Quadrature du Net, de French Data Network et de la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) - sur plusieurs dispositifs de surveillance en temps réel des connexions des internautes et des mobinautes prévus dans deux textes de loi controversés : la loi de programmation militaire (en vigueur depuis le 1er janvier 2015) et la loi sur le renseignement adoptée en mai-juin (en attendant sa promulgation).

Le cyberarsenal mis en place par la France ne risque-t-il pas de porter atteinte à la vie privée et à la liberté d'expression des utilisateurs du Net, pendant que les vrais criminels, eux, ont depuis longtemps déserté l'Internet ouvert pour se mettre à l'abri de la surveillance, dans l'espace obscur de la Toile? Autrement dit, la lutte tous azimuts contre le terrorisme et la cyberdélinquance pourrait avoir un effet contre-productif, celui de renforcer la fréquentation de la face cachée de l'Internet : le Darknet.

## Des criminels longtemps hors de portée

L'Europe, elle, n'a pas attendu le durcissement des mesures de cyberpolice en France pour interpeller des criminels qui sévissent de façon anonyme sur des réseaux occultes censés être inviolables. Ce fut le cas des responsables du serveur Silk Road - « route de la soie » - qui faisait partie de la face cachée du Net, de même que les sites clandestins Black Market Reloaded, Agora, Blue Sky ou encore Pandora.

Jusqu'au jour où cette nébuleuse de plus de 400 sites malfaisants a été fermée, en 2013, à la suite d'une opération de police baptisée « Onymous » menée conjointement par le FBI (la police judiciaire américaine) et Europol (la police criminelle européenne). Le 29 mai dernier, son fondateur - un Texan de 31 ans, Ross Ulbricht - a été condamné par un tribunal de New York à la réclusion à perpétuité pour s'être rendu coupable de trafic de stupéfiants, de blanchiment d'argent et de piratage informatique. Il vient de faire appel de cette décision. Ross Ulbricht avait créé un marché noir électronique de la drogue entre l'Amérique du Nord et l'Europe, qui a oeuvré dans l'ombre du Net de janvier 2011 à octobre 2013. On l'appelait même « l'eBay de la drogue » ! Relié au réseau Tor (lire page 8), lequel permet de communiquer sous couvert d'anonymat, Silk Road permettait à des internautes de se procurer de la drogue (cocaïne, héroïne, ecstasy, LSD...) et d'autres produits illicites (faux papiers par exemple) en payant en toute discrétion à l'aide de la monnaie virtuelle bitcoin.

Les transactions de ce site Web caché de narcotrafiquants auraient ainsi généré un chiffre d'affaires de plus de 200 millions de dollars à travers le monde, grâce à des dizaines de milliers d'acheteurs anonymes. Dix-sept personnes impliquées dans Silk Road (vendeurs et administrateurs) ont été arrêtées. Sur le Vieux Continent, où seize pays étaient concernés (dont la France), c'est le centre EC3 d'Europol, spécialisé depuis janvier 2013 dans la lutte contre le cybercrime et situé à La Haye aux Pays-Bas, qui a coordonné l'opération avec Eurojust, l'agence européenne de coopération judiciaire entre les États membres.

« « Nous n'avons pas simplement supprimé des services de l'Internet ouvert. Cette fois, nous les avons aussi frappés sur le Darknet utilisant Tor, où, pendant longtemps, les

criminels se sont considérés hors de portée », s'était félicité Troels Oerting, qui fut directeur du EC3 jusqu'en février dernier. »

Europol coopère depuis 2001 avec Interpol, organisation de police plus internationale (lire page 10 l'interview de Mireille Ballestrazzi, présidente française d'Interpol, à propos notamment du centre de recherche de Singapour sur la cybersécurité).

En plus de la prison à vie pour trafic de drogue (sans possibilité d'être libéré), Ross Ulbricht, écope de cinq, quinze et vingt ans d'emprisonnement - soit des peines maximales - pour respectivement piratage informatique, trafic de faux documents et blanchiment d'argent. Ces lourdes peines ont été infligées trois jours après la condamnation, dans la même affaire, du responsable et modérateur du forum de discussion de Silk Road, un Australien de 42 ans, Peter Nash : dix-sept mois de prison. Cette double condamnation historique par la justice fédérale américaine se veut exemplaire et dissuasive, au moment où le Darknet prend de l'ampleur.

« « Ce que vous avez fait avec Silk Road était terriblement destructeur pour le tissu social », a lancé la juge fédérale de Manhattan, Katherine Forrest, à Ross Ulbricht. »

Ce Texan, ayant fait des études supérieures qui ne le prédestinaient pas à être cyber-narcotrafiquant, reconnaît aujourd'hui avoir fait de « très grosses erreurs ». Sa fortune personnelle atteindrait, selon l'accusation, 18 millions de dollars grâce à Silk Road qu'il dirigeait sous le pseudonyme de « Dread Pirate Roberts ».

[Image : http://latribune-static.fr/article_content/491807/darknet.jpg]

**Ici, tous les coups sont permis**

Cette affaire retentissante au niveau mondial illustre à elle seule la gravité des méfaits qui peuvent être perpétrés dans ce monde interlope. Pêle-mêle : trafic de drogue, exploitation d'êtres humains, réseau de prostitution, pratiques pédopornographiques, ventes illégales d'armes, activités terroristes, atteinte à la vie privée, vol de données personnelles, commerce de cartes bancaires volées, usurpation d'identité, vente de faux papiers, trafic de fausses monnaies, vente d'armes, commerce de cigarettes, trafic de stéroïdes, recrutement de tueurs à gage, etc.

Ce « cyberunderground », où tous les coups sont permis, est le terrain de jeu des pirates informatiques (« hackers »), des délinquants informatiques (« blackhats »), des « whitehats » (les même sans intention de nuire), des « botnets » (réseaux de robots informatiques déclenchant des attaques en ligne), des « spywares » (logiciels espions), des « spoofers » (logiciels de vol d'identités), des « malwares » (logiciels malveillants), des « Trojan horses » (chevaux de Troie), des adeptes du « phishing » (pratiques d'hameçonnage de coordonnées personnelles) ou encore des cyberterroristes, voire des cybermafiosi. Certains de ces délits menacent de plus en plus le Web grand public. Selon Google, la fonction « navigation sécurisée » - proposée sur les navigateurs Chrome (Google), Firefox (Mozilla) et Safari (Apple) - permet aujourd'hui de lancer plus de 5 millions d'avertissements par jour à près de 1,1 milliard d'internautes dans le monde en cas de tentative d'accès à des sites suspects et à des logiciels indésirables. Et plus de 50.000 sites malveillants et de 90 000 sites d'hameçonnage sont détectés par mois!

« « Nous avons aussi commencé récemment à identifier les publicités infectées par des logiciels indésirables », a prévenu Google en mars dernier. Cependant, les géants du Net restent impuissants face au Web invisible qui n'est accessible qu'à partir d'outils tels que Tor, Freenet ou encore I2P (Invisible Internet Project). »

Ces réseaux décentralisés de type peer-to-peer (poste-à-poste), qui cachent les adresses IP des utilisateurs soucieux de préserver leur anonymat, sont les « Sésame, ouvre-toi » de tous les Ali Baba qui souhaiteraient découvrir les richesses plus ou moins terrifiantes des cyber-Quarante Voleurs d'aujourd'hui.

Sur ces réseaux d'anonymisation, les dialogues se font par des messageries instantanées telles que IRC ou bien Jabber. La monnaie d'échange sur ces serveurs malfamés est le bitcoin ou le litecoin.

**Même les géants du net y sont aveugles**

Le Darknet ne doit pas être confondu avec le Deep Web, lequel désigne l'ensemble des pages non référencées dans les moteurs de recherche, et non exploitables par les aspirateurs de données. L'ultra-dominant Google est en fait atteint de cécité, tout comme ses concurrents Yahoo Search, Bing de Microsoft ou encore DuckDuckGo (« le moteur de recherche qui ne vous espionne pas »). Les réseaux sociaux tels que Facebook, Twitter, Pinterest

ou Reddit s'en tiennent, eux, aux « cybermondanités ». Quant aux navigateurs Internet Explorer, Firefox, Chrome, Opera ou Safari, leurs indexations s'arrêtent aussi là où commence le « no man's land » du Net. La face immergée de l'iceberg que constitue le cyberespace échappe ainsi aux géants du Net; l'Internet ouvert - le « Clear Net » -ne dit pas tout. On l'aura compris : le Deep Web cache le plus souvent des contenus légaux ou légitimes qui ne veulent pas être « Googlelisés », alors que le Darknet aura tendance à être le repère des contenus et trafics illicites.

Dans ces deux mondes parallèles numériques, pas de publicité en ligne ni d'offres légales. En France, la création en 2009 et 2010 de l'Hadopi - pour « traquer » les pirates de musiques ou de films sur les réseaux « peer-to-peer » - aurait poussé nombre d'internautes récidivistes à passer du côté obscur du Net...

À défaut d'être civilisé, le Darknet n'est pas pour autant dépourvu de réseaux sociaux : Twitter Clone, Deep Tube et Galaxy se sont développés pour être - sur le réseau Tor - les clones de respectivement Twitter, YouTube et de Facebook. Selon une étude récente de RadiumOne, 32 % des internautes interrogés échangent des contenus en ligne uniquement sur le « Dark Social ». Cela n'empêche pas les « hacktivistes » de faire part de leurs « exploits » sur les réseaux sociaux qui ont pignon sur rue. C'est sur Twitter que des membres de Rex Mundi (« rois du monde »), site Web de maîtres chanteurs utilisé pour la divulgation de données personnelles ou de données d'entreprises, ont annoncé - après des mois de rançonnement - avoir rendu publique la base de données de clients de la chaîne Domino's Pizza, volée en juin 2014. Le « doxxing » désigne le fait de révéler sur Internet des informations personnelles d'une personne après chantage.

Si les victimes refusent de payer la rançon demandée, les informations personnelles ou confidentielles sont effectivement divulguées. C'est également sur Twitter que les pirates numériques du groupe Lizard Squad (« l'escadron lézard ») ont revendiqué le piratage informatique, perpétré en décembre 2014, du réseau Xbox Live de la console de jeux vidéo Microsoft. Le vol de photos de célébrités nues, dont a été victime Apple sur son service iCloud à partir de l'été 2014, est aussi une illustration des méfaits des nouveaux cyberpaparazzi du Darknet.

Les réseaux sociaux, clairs ou obscurs, servent aussi pour les organisations criminelles à rallier de nouvelles recrues et sympathisants. Ils permettent de lancer des appels à l'action qui sont « retweetés » pour former une véritable campagne de communication auprès des cybermilitants. C'est par exemple le mode opératoire du collectif (non criminel) Anonymous, sur Twitter ou Facebook. L'organisation terroriste Daesh (dite « État islamique ») prospecte lui aussi de nouvelles recrues sur les réseaux sociaux et poursuit les échanges avec les candidats potentiels au djihad avec des outils de communication cryptée. Le réseau communautaire Reddit fait aussi émerger des fins fonds du Net certains marchés noirs.

« « Le fil Reddit "Darknet Deals" est un bon exemple d'espace consacré aux dernières "bonnes affaires" des marchés noirs en vogue sur le Darknet. Les promotions de magasins tels qu'Agora, Evolution ou encore Panacea seront ainsi diffusées auprès du public de Reddit et accessibles sur le Web ouvert. En utilisant Reddit, les cybercriminels bénéficient d'une plateforme idéale de veille et de mise à jour. Le fil DarkNetMarkets propose par exemple une actualisation régulière des arnaques et faux marchés noirs, et de "l'état de santé" des sites les plus visités », explique la Compagnie européenne d'intelligence stratégique (Ceis) dans un rapport sur la cybercriminalité et les réseaux sociaux, publié en février. »

**[Image : http://latribune-static.fr/article_content/491811/darknet-market-place.jpg]**

**Une cyberguerre géopolitique**

Les États sont aussi des victimes du Darknet. Considérée comme la plus grave jamais lancée contre les États-Unis, la cyberattaque de Sony, à la fin novembre 2014 sur ses serveurs américains, avec vol massif de données confidentielles (de 47 000 personnes) et divulgation d'au moins cinq films de Hollywood sur Internet, a scandalisé l'Amérique. Le président américain, Barack Obama, a lui-même accusé la Corée du Nord d'être à l'origine de cette magistrale cyberattaque. Washington a aussi été sérieusement inquiété, à la mi-janvier 2015, par le piratage du compte Twitter du commandement militaire américain au Moyen-Orient (Centcom). Plus récemment, le Washington Post a révélé que pas moins de 4 millions de données d'employés fédéraux américains avaient été dérobées lors d'une cyberintrusion d'origine chinoise.

L'Europe n'est pas à l'abri, qu'il s'agisse des États ou des entreprises.

La chaîne de télévision francophone TV5 Monde a été victime en avril d'une cyberattaque - dont l'origine serait russe, selon L'Express. Les responsables de la sécurité des systèmes d'information (RSSI) des entreprises sont sur les dents. Les cyberdélinquants se servent des réseaux souterrains pour échanger sur les vulnérabilités des entreprises et organisations, tout en y faisant connaître leurs exploits.

Cela va de l'utilisation d'un RAT (remote administration tool), outil d'administration à distance permettant la prise de contrôle totale d'un ordinateur, à l'exploitation d'une faille de sécurité dite « Zero Day », inconnue du fabricant du matériel informatique ou de l'éditeur de logiciel, en passant par une attaque par déni de service perpétrée par plusieurs « soldats » ou « zombies », attaque informatique groupée appelée DDoS (« distributed denial of service »).

« Il convient de rechercher des signaux faibles et de détecter des signes avant-coureurs, par exemple en trouvant des "rootkit" ou des "malwares" en préparation, mais également de retrouver les données volées lors d'une attaque précédente », a expliqué Henri Codron, responsable de l'espace RSSI du Club de la sécurité de l'information français (Clusif), lors d'une conférence sur le Dark Web le 16 avril dernier. »

Tout aussi inquiétant, le développement du e-paiement en ligne ou dans les magasins - avec Apple Pay ou Google Wallet - devrait s'accompagner d'une recrudescence de piratage de ces systèmes de paiement.

**Edward Snowden sauve-t-il la vie privée?**

Mais le Darknet est-il pour autant infréquentable? L'affaire « Prism » - révélée en juin 2013 par Edward Snowden, l'ex-informaticien de la National Security Agency (NSA), sur l'espionnage généralisé mené illégalement par cette agence des services de renseignements américains au détriment de plusieurs pays, y compris des alliés européens - a déclenché une prise de conscience mondiale sur la vulnérabilité de la vie privée et des données personnelles. Tout le monde - particuliers et gouvernements - peut être surveillé par l'État américain. Ce qui a provoqué un appel d'air vers la face cachée du Net.

De Wikileaks de Julian Assange à l'internaute lambda, en passant par les « hacktivistes », nombreux sont ceux qui répondent à l'appel du Darknet pour communiquer à l'abri des mouchards indiscrets. L'anonymat fait partie de la liberté d'expression. Le chiffrement informatique des contenus et des messages sur Internet - qui permet de les rendre illisibles en les transformant en une suite inintelligible de chiffres et de lettres - est voué à un bel avenir. Yahoo a annoncé en mars dernier qu'il va, d'ici à la fin de l'année, permettre aux internautes de chiffrer leurs mails « de bout en bout ».

Ce niveau de protection très élevé sera alors à la portée de tous, et non plus seulement de quelques-uns, afin de déjouer les surveillances de masse et les piratages en tout genre. Yahoo travaille en outre avec Google pour rendre ce service de chiffrement compatible avec Gmail. « Beaucoup d'utilisateurs de Yahoo vivent dans des pays où leur liberté d'expression et leur liberté d'association ne sont pas respectées, et où les États tentent d'introduire des "malwares" dans leurs ordinateurs pour les surveiller », a justifié Alex Stamos, directeur de la sécurité informatique de Yahoo.

**60 millions de pages dans le Deep Web**

De son côté, Facebook a annoncé en novembre dernier la création de l'adresse https://facebookcorewwwi.onion pour que l'utilisation de Tor (2,5 millions de personnes s'en servent chaque jour) soit compatible avec les règles de sécurité de Facebook. Plus ironique : une application de chiffrement de communications, Scrambl3, a été lancée début juin aux États-Unis pour les smartphones sous Android par la société USMobile qui a utilisé une technologie de la... NSA.

En France, c'est l'application Gossip qui a récemment défrayé la chronique : elle permet d'échanger de façon anonyme des potins (traduction de l'anglais « gossip »), ce qui inquiète jusqu'à la ministre de l'Éducation nationale, Najat Vallaud-Belkacem. Les journalistes cryptent aussi : mi-février 2015, quatre médias français et belges (Le Monde, Le Soir, La Libre Belgique et la RTBF) ont lancé le site Web Sourcesure.eu conçu à partir du logiciel italien de « dénonciation anonyme » GlobaLeaks déjà utilisé par la presse - à l'instar de SafeHouse du Wall Street Journal. En quelques clics, un document peut être envoyé par les lanceurs d'alertes de façon chiffrée et de manière « intraçable ».

Il s'agit aussi pour les États de faire la lumière sur le Darknet. L'agence américaine Darpa (Defense Advanced

Research Projects Agency), qui fut dans les années 1970 à l'origine de la création de l'Internet avec son projet Arpanet, a mis au point un moteur de recherche nouvelle génération - baptisé Memex - pour explorer non seulement les 60 millions de pages estimées du Deep Web, mais aussi tous les recoins du Darknet. Cette tête chercheuse du cyberespace ne se contente pas d'aller fouiner dans les contenus textuels en ligne, mais va aussi explorer les images, les vidéos, les publicités, les formulaires, les scripts et toutes autres formes d'informations en ligne.

À l'issue de quoi, ce « Google » qui voit plus loin que son bout du nez est capable d'associer des contenus disparates pour faire ressortir un même sujet. Pour cela, la Darpa a mis en place des robots d'indexation augmentés pour qu'ils se comportent comme des navigateurs dans les tréfonds du Net - à la manière d'un robot sous-marin équipé de capteurs et caméras explorant la faune abyssale en mer profonde. C'est ainsi que les États-Unis ont pu démanteler en 2014 un réseau de trafiquants d'êtres humains.

**Un « super-préfet » contre les cybermenaces**

Le FBI, lui, détient une copie de TorMail, l'ancienne messagerie du réseau Tor, pour infiltrer des réseaux suspects et débusquer les cybercriminels, tels que ceux qui avaient créé le site Fakeplastic.net en juin 2012 pour y proposer de quoi fabriquer soi-même des cartes bancaires moyennant paiement en bitcoin. Grâce à leur serveur TorMail, qui serait hébergé en France, les limiers du FBI mettent toutes les chances de leur côté pour confondre des fraudeurs et les cyberterroristes. Mais, début juin, le chargé de la lutte antiterroriste au FBI a lancé un cri d'alarme en implorant le Congrès américain de légiférer pour lui donner accès aux données de suspects qui utilisent les outils de chiffrement fournis par les acteurs du Net eux-mêmes. D'autres dispositifs destinés à lever le voile sur le Darknet existent, tels que Flashpoint ou Grams.

En France, la fonction de « cyberpréfet » a été créée en décembre 2014 avec la nomination de Jean-Yves Latournerie au poste de préfet chargé de la lutte contre les cybermenaces et cyberattaques. Il dépend du ministère de l'Intérieur, tout comme Anne Souvira, qui est commissaire divisionnaire chargée de mission aux questions relatives à la cybercriminalité et chef de service de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti) à la préfecture de Police de Paris. Créée en février 1994, cette unité compte 25 policiers spécialisés dans les nouvelles technologies, dont la mission est d'élucider les crimes et délits informatiques.

Les peines encourues pour la plupart de ces infractions sont, en France, de cinq ans d'emprisonnement et de 300 000 euros d'amende. Rien qu'en 2014, la Befti a été saisie à 281 reprises. La France s'est dotée dès 2009 d'une Autorité nationale de défense et de sécurité des systèmes d'information (Anssi) vouée à la sécurité de la société de l'information et à la protection des réseaux interministériels les plus sensibles de l'État. C'est l'Office de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui transmet les données des sites Web jugés illégaux aux fournisseurs d'accès à Internet (FAI), lesquels devront en bloquer l'accès - même s'ils sont hébergés hors de France. En revanche, la Commission nationale de l'informatique et des libertés (Cnil) nous dit ne pas avoir de travaux précis en cours sur le Darknet... Pas très rassurant.

———

**>>> REPÈRES**

**Barack Obama exige plus de cybersécurité**

La lutte contre le piratage informatique est le cheval de bataille du président des États-Unis qui a encore exigé le 5 juin que le Congrès américain « sorte de l'âge de pierre » (dixit un porte-parole de la Maison Blanche) et « entre dans le XXIe siècle » en renforçant les lois cybersécuritaires. Barack Obama intervenait après que le Washington Post a révélé le jour même le vol de données de 4 millions d'employés fédéraux américains, par cyberintrusion provenant, a priori, de la Chine. La veille, le 4 juin, c'était au New York Times de publier des documents « Snowden » révélant que le gouvernement Obama avait autorisé en 2012 la NSA (l'agence de renseignement américaine mêlée à l'affaire Prism) à traquer sur Internet (sans mandat judiciaire) les pirates numériques et les logiciels malveillants.

**La « pègre numérique » en 320 pages!**

The Darknet. Inside the Digital Underworld est le titre d'un livre paru en août 2014, écrit par Jamie Bartlett (l'auteur et chercheur britannique, pas l'acteur sud-africain!). Publié par par l'éditeur William Heinemann, cet ouvrage (en anglais) montre dans le

détail la face cachée du Net : « C'est un monde aussi choquant et perturbant qu'il est innovant et créatif. Un monde beaucoup plus près que vous ne le pensez », écrit-il.

**Illustration(s) :**

DR



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

la Croix
La Croix, no. 40360
Sciences et éthique, mardi 8 décembre 2015, p. 15-16

# La face cachée du « dark Web »

## Enquête Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaires

**THOMASSET Flore; SCHNEIDER Frédérique**

«S*ur Internet, on peut acheter une kalachnikov en deux clics.* » Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge. Depuis les attentats de janvier notamment, **Internet** (1)est au coeur des préoccupations. *« Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles? »*, interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web... Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un **navigateur** personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une **adresse IP**, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

*« Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre,* explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. *En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet. »*

Une fois sur TOR, pas de **moteur de recherche**. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches... C'est l'Internet « surfacique », une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur... C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de **réseaux virtuels privés** et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden **Wiki** (le « wiki » caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 euros ou un pistolet SIG Sauer de calibre 9 mm pour 790 euros.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas... Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en **bitcoins**, une monnaie virtuelle et **chiffrée**, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et

sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer

*(Lire la suite page 16)*

des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire « confiance » à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un *« facilitateur de la performance criminelle »,* selon Solange Ghernaouti: *« Internet reflète notre réalité sociale, économique, politique et criminelle*, poursuit-elle. *Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation - on agit caché derrière un écran - à distance. »*

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les *« internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques »,* poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins *(voir le débat).*



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Hindustan Times (New Delhi)
Sunday, August 09, 2015

# The Darknet: A secret world of snuff porn, drugs and guns

**Pranav Dixit and Rezaul H Laskar**

AUG 09, 2015 - Aug. 09--Videos of women torturing and killing animals such as cats and rabbits while simultaneously having sex, lethal weapons like the Walther PPK 9mm pistol being sold for a few Bitcoins, and groups that offer "rape and murder services". This and much more are available in the Darknet, a shadowy part of the internet. You can't access the Darknet through search engines like Google or Bing -- and even the world's most powerful security agencies can rarely crack its clandestine activities.

The Dark Web entered public consciousness in 2013 when the FBI shut down Silk Road, a notorious Darknet website that that allowed anyone to buy or sell recreational drugs, and made over $8 million a month. Silk Road founder Ross William Ulbricht aka Dread Pirate Roberts was sentenced to life imprisonment. The website allowed users to trade in Bitcoin, a crypto-currency completely disconnected from banks and thus offering completely anonymity.

Silk Road which was shut by FBI was notorious for selling illicit drugs.

Indian cyber security experts believe criminals and terrorists in the country could already be using the Darknet for their activities because law enforcement agencies simply don't have the wherewithal to track such activities.

"The Dark web is something that you can't figure out unless you get into it yourself," said senior technology journalist Prasanto Roy. "Unfortunately, our government is clueless."

That may be true, but 8 of the 857 websites that the government asked ISPs to block recently are Darknet websites, characterised by their telltale .onion URLs. They include Agora Market, a Silk Road clone that also specialises in selling illegal drugs.

No other direction @prasanto, see the image. @TedhiLakeer @anjakovacs @shailichopra
pic.twitter.com/tSFWFlu1cd

-- Ajay Data (@ajaydata) August 4, 2015

Pavan Duggal, cyber law expert and author of "Darknet and Law" said, "Law enforcement agencies and governments round the world don't even acknowledge the presence of the Darknet because they are incapable of tracking activities."

Just this week, the Interpol's Cyber Research Lab formed a private dark web network to reverse engineer its technologies in order to better understand how criminals use it.

A study done last year by the University of Portsmouth's computer science researcher Gareth Owens found that 80% of the traffic on the Darknet was to websites hosting child pornography. After a six-month study of the hidden services and websites that can be accessed through the Tor browser, Owen found that sites offering drugs and contraband made up the single largest category within the Dark Web.

"Before we did this study, it was certainly my view that the Darknet is a good thing," Owen was quoted as saying by the media. "But it's hampering the rights of children and creating a place where paedophiles can act with impunity."

Despite its depth and complexity, accessing the Dark Web is not very difficult. Most websites on the Darknet cover their tracks by using Tor, short for The Onion Router. People surfing the Darknet too can cover their tracks by using the Tor browser.

Military-grade weapons being sold on the Darknet.

Tor was initially a worldwide network of services developed by the US Navy that allowed people to anonymously browse the internet. Now, it's an open-source project that hides a user's identity on the web by encrypting a computer's unique IP address and bouncing it across several volunteer servers, known as "nodes", around the world so that it's virtually impossible to trace the user.

A Kolkata-based professional, who used Tor to access sites on the Darknet while he was a student in Karnataka, said he used Silk Road and

Evolution, a marketplace for contraband, to order banned drugs.

"These websites change their IP every 12 hours, and I found a blog that had the latest address. I then got some bitcoins from my Australian friend by transferring money to him through my bank account," he said.

"I ordered twice from Darknet sites -- once, blots of acid (LSD) and Ecstasy the second time. The acid was delivered in the form of small pieces of paper that had been dipped the drug and hidden within a stamp album. The ecstasy was delivered in a lipstick."

Professional hitman services being offered on the Darknet.

People sometimes confuse the Darknet with the Deep Web, which too cannot be accessed by search engines. But a lot of the material on the Deep Web could be innocuous, such as the academic databases of universities and educational institutions, libraries or even material on internal servers of the Hindustan Times.

Despite its reputation, the Dark Web does have a few bright spots. During the Arab Spring, activists used Tor to anonymously pass on messages. Around the world, political dissidents and journalists have taken to the Darknet to cover their digital tracks for oppressive regimes.

"Indians are increasingly going on the Darknet after the revelations by (whistleblower) Edward Snowden about government surveillance and because non-state actors such as hackers groups could be watching their activities," Duggal said.

"The Indian nation has not even woken up to the reality of the Darknet. We are still in the medieval age as far as our laws are concerned. We need to update tools and sensitise law enforcement agencies to this new challenge for India, which has the potential to destabilise security," he added.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

Sunday Telegraph (UK)
Sunday, September 07, 2014, p. 13,14,15

# Click here for crime

## Ten years ago, the US Navy invented an anonymous internet network. Today the 'dark web' is used to trade guns, drugs and child pornography. Why do they insist it's a force for good?

**Words by Jake Wallis Simons**

On Friday, August 13 2004, three unassuming computer experts ascended the stage at the San Diego Town and Country Hotel and Convention Centre in California.

It was blisteringly hot outside, and the complex was filled with holidaymakers strolling to and from the pool. But inside the darkened auditorium, everybody was wearing business clothes, and the air conditioning made it chilly.

This was the last session of the Usenix Security Symposium, a five-day conference for digital security professionals. Already people had started to go home. But the audience that remained - a mixture of researchers, systems administrators and policy wonks - greeted the speakers with polite applause.

Roger Dingledine and NickMathewson were members of Free Haven, a Massachusetts Institute of Technology research project that looked for ways to use data so that it could resist "attempts by powerful adversaries to find and destroy [it]".

Their colleague, Paul Sylverson, a mathematician with a PhD in philosophy from Indiana University, had been working for the US Navy to find a way to use the internet anonymously. That had been his goal since 1995. An alpha version of his solution had been running since 2002; now, in 2004, they were going to present the updated version that was to make history.

As modest as they appeared, these three men have become known as the people who - in that darkened conference room in 2004 - unleashed the Tor anonymity network, one of the most controversial phenomena in the history of the internet.

An acronym for The Onion Router, Tor bounces data and messages through as many as 5,000 other computers, known as "nodes" or "relays", adding layers of encryption to the data like skins on an onion, until it is virtually impossible to discern the original user's location and identity.

And although it has positive applications, especially in repressive regimes such as Iran and China, where prodemocracy activists use it to publicise human rights abuses and foment dissent, it is also used by many thousands of people to trade guns, drugs, stolen goods and child pornography. It has been implicated in hundreds of cases of fraud, identity theft and paedophilia. Remarkably, though, the US Navy continues to provide most of its funding.

"When we started working on Tor, we didn't sit back and think too much about the implications of privacy, security and anonymity," says Sylverson, on the phone from the US Naval Research Laboratory inWashington, DC. "The reason for our research was to allow US government employees to go to public websites to gather information, without anybody knowing that there was somebody from the Navy looking for this stuff."

To guarantee anonymity,Tor had to have mass appeal and so the software was designed to be "open-source", meaning that the source code could be distributed and developed by anybody. "It had to be picked up by the public and used. This was fundamental," says Sylverson. "If we created an anonymous network that was only being used by the Navy, then it would be obvious that anything popping out or going in was going to and from the Navy."

Every additional ordinary user, he says, enhances the security and protection that the network is designed to offer to Navy employees, and is, in a way, their "payment".

Fast-forward to 2014, and that attitude seems at best naive, at worst willfully negligent. Sites that are blocked by most internet service providers, including those peddling hardcore child pornography, are accessible using Tor and available to browse following some simple steps well within the grasp of most computer-users.

Each page can take up to 30 seconds to load, but that aside, when I log on to the network on aMonday afternoon after downloading the Tor browser, I find it easy to access a wealth of illegal goods and services, ranging from the appalling to the ridiculous.

Gun Grave, for instance, offers a selection of weapons including a "mint condition" M4 semi-automatic rifle that can be "shipped worldwide". "Chances are if you are looking for it we can find it," the vendor writes. On another site, a user calling himself "The FacebookHacker from Belgium" offers to hack into any social media account for 0.86 Bitcoin (the internet-only currency favoured by the dark net), or about £250. Business is obviously brisk - he has accumulated 23 positive reviews, with satisfied customers leaving messages like "the perfect vendor", "totally impressed", and "legit seller".

And this is only the tip of the iceberg. On a retail site called Evolution, a vendor called Cat, based in China, sells illegal rhinoceros horns, someone from India offers morphine tablets and "Science Guy", another Chinese seller, offers testosterone and steroid pills. User "Amazon Gold" is selling "1000s of credit card details" for one Bitcoin, or about £290, along with a guide to credit card hacking for "noobs", or newcomers.

There is also a host of even more disturbing material, including a plethora of upsetting pornographic sites, sinister suicide forums telling vulnerable users how to kill themselves, and sites offering the services of hit men and corrupt government officials. A search engine called Grams makes it as easy to find these things as Google does to find conventional websites. In fact, Grams, with its multicoloured lettering and white background, appears, at first glance, to be part of Google. But the slogan on the homepage gives it away: "The only way to deal with an unfree world is to become so absolutely free that your very existence is an act of rebellion."

There can be little doubt: this is not just the WildWest, this is the modern-day Sodom and Gomorrah. As well as the obvious human cost of those being exploited by online paedophiles, it is estimated that electronic fraud, which relies heavily on Tor, costs the British economy tens of billions of pounds a year.

In July, security researchers at Kaspersky Lab, the world's largest private software security company, announced that a new strain of ransomware - malicious software that encrypts users' data and demands hundreds of pounds for its release - had appeared, which usedTor "to hide its malicious nature" and made those responsible "hard to track".

Ransomware is so sophisticated that it has even made victims of the police. Last year, a police force in Massachusetts was forced to pay $1,338 (£795) to unlock data that had been infected with Cryptolocker, a forerunner of the new Tor-based programme.

Above all, perhaps, Tor has become a hugely popular means of buying drugs online without getting caught. Users can visit websites on the dark net, browse a selection of thousands of drugs, pay for them using Bitcoin, and have them delivered to their door.

"I started using it two years ago. It made life a lot easier," says Alistair Roberts (not his real name), who buys drugs regularly usingTor. "It cut out a lot of the danger involved in drug buying. No one can rob you or stab you, and the police can't get involved."

Another benefit of buying drugs online, he says, is that you are given access to a vast range at the click of a mouse. "Normally you can only buy drugs if you know the dealers. But this opens up the whole market. It's a totally free market that regulates itself."

The drugs arrive in a variety of ways. Some are in Amazonstyle envelopes, vacuum packed to prevent odour. Others are hidden in CD cases, or inside food packaging.

"I once bought some MDMA pills, and they arrived in a sports supplement tub," says Roberts. "The company was selling nutrition supplements legitimately through a normal website, and illegal drugs on the dark web using the same packaging."

In October 2013, Silk Road, the biggest drug-dealing site, was shut down by the authorities. But despite the fact that its alleged founder, Ross Ulbricht, is now in custody, a new, 2.0 version of the site reopened in May, and business is booming. There are countless smaller sites, too.

When I contacted GCHQ about the impact that Tor has had on its work, the agency declined to comment. But Andy Archibald, deputy director of the National Crime Agency's national cyber crime unit, which takes responsibility in Britain for countering online criminal activity, provided a statement. "Online environments such as Tor have been a

game changer for law enforcement," he said. "Policing online environments is a constant challenge, as criminals develop ways to conduct their illegal activity. "Law enforcement, both nationally and internationally, continues to develop approaches to identify and apprehend those who try to stay under the radar."

There are signs that the police are closing in on dark net users. In July, more than 650 suspected paedophiles were arrested as part of a six-month operation targeting people accessing child abuse images online.

Similarly, the FBI has developed a form of malware that infiltrates high-traffic websites and infects all of its visitors, allowing users of Tor to be tracked and identified. As a result, more than a dozen alleged users of child porn sites are facing prosecution in the US.

This technique was also involved in the identification and arrest of Eric Eoin Marques in Ireland in 2013; he was accused of being the owner and administrator of an anonymous hosting server called Freedom Hosting, where members posted millions of images of child porn.

But, despite all Tor's criminal applications, internet ideologues who champion freedom of information refuse to condemn the network. Few would dispute the right to privacy, which can be a useful corrective to the overextension of government agencies into our lives.

Journalists and campaigners in countries such as Iran, Syria and China have found the network invaluable in avoiding detection by their governments. Indeed, Vladimir Putin, the Russian president, is so worried about Tor's potential for undermining his regime that he has announced a prize of four million roubles (£65,000) to anyone who can crack the network. To many, this can only be a good sign.

In 2010, Tor won the award for projects of social benefit at the Free Software Awards. In a statement, the judges said: "Using free software, Tor has enabled roughly 36million people around the world to experience freedom of access and expression on the internet while keeping them in control of their privacy and anonymity."

But it is impossible to ignore the fraud, the paedophile rings, the drug dealing and the rest. Does Sylverson have any regrets about introducing his software to the world?

"I'm not authorised by the Navy to talk about the ethics of Tor in detail," he says cagily. "The internet is used in a wide variety of ways, and not everyone is happy with those ways. But when you create a technology, it's a tool that anybody can use for good or ill. To some extent, you have to trust society broadly to do good things.

"The same is true of automobiles. In the early 20th century, police in Detroit were upset because criminals could suddenly vanish because they had these things called automobiles, and the police didn't. Then the police caught up. But I'm going to start using phrases like 'democratising technology', and I don't want to get into that."

He does, however, "have opinions" about the balance of positive uses against negative ones, and his strong implication is that overall,Tor has been a force for good.

"I'm aware of wide-scale use ofTor in the Arab spring," he says. "There was a time when the only communication coming out of Egypt was over Tor. But if someone uses Tor to do something illegal, that's often what gets on the news. It creates an asymmetry about what is visible. But I'm a wrench turner. I do the science, not the policy."

Sylverson's hesitation in talking about the issue points to the paradoxical relationship between theTor project and his employer, the government of the United States. On the one hand, the authorities - who lie behind its creation in the first place - continue to heavily fund its development. On the other, they are seeking to destroy it.

According to theTor Project's latestfinancial statements, it received more than $1.8million in federal funding last year, primarily from the State Department and Department of Defence, as well as filtered through independent organisations such as Internews Network, a non-profit network that aims to support freedom of information around the world. This amounts to about 60 per cent of its total funding.

At the same time, documents disclosed in October last year by thewhistleblower Edward Snowden - who, ironically enough, used Tor to send top-secret information to The Guardian newspaper - reveal that both the National Security Agency (NSA) and GCHQ have made efforts to disable Tor, or at least to remove anonymity from its users.

Although Tor remained fundamentally intact, the two agencies were able to

gain some success by targeting individual browsers when used in conjunction with Tor, and take control of targeted computers. This allowed them to view all the files on the machine, as well as all online activity.

The US government's selfdefeating approach was again brought into sharp relief last month. Two researchers at Carnegie Mellon University in Pittsburgh, Pennsylvania, Alexander Volynkin and Michael McCord, revealed that they had launched a successful cyber attack on Tor between January and July this year, and had unmasked a signifi-cant number of people using the network.

They were due to present their findings at the Black Hat computer security conference in Las Vegas last month, in a session entitled "You don't have to be the NSA to break Tor: de-anonymising users on a budget". But the event was cancelled for "legal reasons".

In an official blog post, Roger Dingledine, one of the three founders of Tor, seemed rattled. He admitted that he had no idea how many users had been stripped of their anonymity, or how much data had been captured. But he announced an immediate upgrade to the system, which would "close the particular protocol vulnerability the attackers used".

Once again, however, further scrutiny reveals that the US is running two dogs after the same ball. Volynkin and McCord's department, the Software Engineering Institute, has received $584million (£351million) in funding from none other than the US Department of Defence - with the special target of finding security vulnerabilities.

"From one point of view, it's not surprising that the United States is funding both sides of the story," says Prof Bill Buchanan, an electronic security expert at Edinburgh Napier University. "For a start, they still have to monitor threats. More importantly, they want secret channels for their own use, but if anybody is going to break it, they'd rather it was them than someone else. That's how they stay at the cutting edge of technology."

Ultimately, he says, the development of Tor is the story of the maturation of the digital age. "The internet is grown up now. It recognises no boundaries, and it is very difficult to stop anything from happening," he says. "We have all gradually become disillusioned in the dream of the pure democratisation of information and technology. It is starting to reflect life more closely, in all its light and shade."

One thing is certain: on Friday, August 13 2004, when Sylverson and his colleagues stood on that stage in San Diego, they could never have imagined just what they were bringing into the world.

"When you create something you think is useful, you hope people will use it," says Sylverson. "But the trajectory and scale was simply not something we had predicted."

*GunGrave offers a 'mint condition'M4 semi-automatic rifle that can be 'shipped worldwide'*

*'When you create a technology it's a tool that anybody can use for good or ill'*

**Figure:**

PETER GRUNDY

FREE WORLD? The Tor network offers guns for sale, as well as anonymity for freedom campaigners in countries such as Egypt, top

DARK ARTS Ross Ulbricht, top, the alleged founder of Silk Road, the drug-dealing website, is in prison awaiting trial



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

Libération
Économie, mardi 9 juin 2015, p. 12

# Anti-surveillance : extensions du domaine de la lutte

## L'ère de la surveillance de masse a sonné et le Sénat devrait l'entériner ce mardi dans le cadre de la loi sur le renseignement. Les conseils de «Libération» pour préserver votre vie privée sur les réseaux.

**Pierre ALONSO; Amaelle Guiton**

Avec la loi sur le renseignement, la France s'apprête à graver dans le marbre la surveillance massive de nos communications. Voté aujourd'hui au Sénat, le texte prévoit des dispositifs de détection d'une potentielle *«menace terroriste»*, des «boîtes noires» installées chez les opérateurs et les hébergeurs. Une surveillance algorithmique qui confie à des logiciels le soin de trouver des aiguilles dans des bottes de foin - et ce, alors que de nombreux chercheurs alertent sur le caractère intrusif d'une telle méthode et sur les risques d'erreurs, les «faux positifs».

Les révélations d'Edward Snowden l'ont amplement démontré : avec la possibilité d'intercepter, de stocker et de traiter de très grandes quantités de données, la surveillance a changé de dimension, et même de nature. *«Ce n'est plus "suivez cette voiture", c'est "suivez chaque voiture"»*, dit ainsi l'expert en sécurité informatique américain Bruce Schneier. Pourtant, comme l'explique Snowden lui-même (lire *Libération* de vendredi), de nombreuses entreprises du numérique ont revu leur copie et renforcé la sécurité de leurs services. Et des équipes de développeurs travaillent sur des outils qui *«peuvent permettre un accès à une protection de base du droit à la vie privée»*. A l'inverse des «boîtes noires», ceux-ci sont transparents : leur code source, librement accessible, peut être examiné par des experts. Contrairement aux idées reçues, plus besoin d'être un geek averti pour s'en servir. Tour d'horizon de quelques moyens techniques pour retrouver un peu de confidentialité à l'ère de la surveillance de masse (plus d'infos dans le guide de l'ONG Tactical Tech).

### Surfer hors des filets

C'est en quelque sorte le «péché originel» du Web : par défaut, on y navigue tout nu, tout ce qu'on y fait est visible - se connecter à un site, mais aussi lui transmettre un mot de passe... A partir de 1994, le protocole de connexion sécurisée HTTPS est venu remédier à cet état de fait. Il crypte (ou «chiffre», en bon français) le contenu de la communication avec un site web. Un petit cadenas apparaît alors dans la barre de navigation. Les banques et les sites de e-commerce ont été les premiers à l'utiliser. Plus récemment, la plupart des grands services internet (Google, Facebook, Twitter...) l'ont adopté. L'Electronic Frontier Foundation, l'association américaine de défense des libertés sur Internet, a lancé il y a quatre ans HTTPS Everywhere, une extension qui fonctionne avec la plupart des navigateurs, s'installe en un clic et «force» la connexion sécurisée partout où elle est possible.

En revanche, un curieux saura qui communique avec qui. C'est à cela que veut répondre l'équipe qui travaille sur le réseau d'anonymisation Tor, et sur le Tor Browser, un navigateur «dédié» très simple à installer (la connexion, qui passe par plusieurs relais, est cependant plus lente). *«Tor cache un utilisateur parmi les autres»*, explique Nick Mathewson, l'un de ses principaux architectes. Une image tenace voudrait que seuls des criminels s'en servent; dans les faits, partout dans le monde, des activistes, des ONG, des journalistes l'utilisent - sans compter les forces de l'ordre. Le réseau compte aujourd'hui deux millions d'utilisateurs quotidiens. Signe qu'il se démocratise, Facebook a travaillé à faciliter l'accès à ses services via Tor.

### Sécuriser ses mails

Avec le développement du webmail (à savoir la gestion des e-mails dans un navigateur web), nos échanges ont longtemps plus tenu de la carte postale que de la lettre cachetée. Il a fallu attendre 2010 pour que Gmail, le premier, active par défaut la connexion sécurisée à ses boîtes de messagerie. D'autres ont attendu l'affaire Snowden...

S'assurer qu'on accède à son service de messagerie en HTTPS et non en HTTP est un minimum pour protéger un tant soit peu ses échanges épistolaires en ligne. Encore faut-il avoir confiance en son fournisseur de messagerie.

Le cryptage (ou chiffrement) du contenu des messages entre deux correspondants reste une autre paire de manches. Le logiciel PGP, pour «Pretty Good Privacy» («assez bonne confidentialité»), a beau avoir près de 25 ans, son usage n'est toujours pas à la portée du premier venu. Mailvelope, une extension pour Chrome et Firefox, permet au moins de l'utiliser plus facilement dans un navigateur. Plusieurs équipes de développeurs travaillent à le rendre véritablement accessible à tous. Signe de ce retour de hype, Google comme Facebook s'y intéressent. Le premier a promis pour cette année la sortie officielle d'une extension pour Chrome. Le second propose désormais à ses utilisateurs familiers de PGP l'envoi de notifications cryptées.

Tchater couvert

Le regard indiscret ne verra qu'une suite de caractères incohérents, du type «0I1Egb3uPK4». Seuls les destinataires connaîtront leur traduction en langage courant. C'est l'avantage des messages cryptés, qui ne sont plus réservés aux militaires (l'usage de la cryptographie est libre depuis 2004 en France), ni aux experts en sécurité. Ainsi, Cryptocat, une extension pour navigateurs web (Firefox, Chrome...), permet au néophyte de renforcer la confidentialité de ses échanges instantanés. Son jeune fondateur, Nadim Kobeissi, l'a pensé pour le plus grand nombre : *«Il y avait un «class gap», mais au lieu des riches et des pauvres, un gouffre entre ceux qui peuvent utiliser la cryptographie et ceux qui ne peuvent pas.»*

Pour combler le fossé et permettre à chacun de protéger sa vie privée, Nadim a lancé Cryptocat en 2011. Plus designer qu'expert en cryptographie, il mise d'emblée sur une interface très simple et un logo sympathique, un petit chat pixellisé. Les failles initiales, qui lui avaient valu de vives critiques, ont depuis été corrigées. Pour toucher un public toujours plus large, Cryptocat peut être utilisé avec le tchat de Facebook, pour protéger ses conversations , y compris du géant du Net.

«Skyper» sans Skype

Depuis que Microsoft et Google ont été mis en cause dans les révélations sur le programme Prism de la NSA, Skype et Hangouts sont regardés de travers par les défenseurs de la vie privée, et écopent de scores peu glorieux dans le comparatif des outils de communication en ligne de l'Electronic Frontier Foundation. Des concurrents à ces solutions de conversation audio et vidéo ont commencé à voir le jour. L'un des plus prometteurs vient de la fondation Mozilla, l'organisation à but non lucratif qui développe le navigateur Firefox. Firefox Hello (c'est son nom) ne nécessite même pas de créer un compte : il suffit d'ouvrir une «conversation» et d'y inviter un ami (y compris s'il utilise de son côté les navigateurs Chrome ou Opera). Pas encore disponible, la conversation à plusieurs fait partie de la feuille de route.

Pour ne pas être géolocalisé...

Idée reçue : pour éviter la géolocalisation, il suffirait de la couper sur son smartphone. Faux. Cela permet, au mieux, d'éviter le pistage commercial d'Apple, de Google et de toutes les applis qui ont accès à ces données. Mais pour suivre un téléphone, et son propriétaire, il existe un moyen beaucoup plus simple et difficile à contourner : le bornage. Les téléphones communiquent à intervalle régulier avec les antennes-relais à proximité. Ces données de localisation sont conservées pendant un an par les opérateurs de téléphonie français. Il est donc possible, a posteriori, de savoir où se trouvait un téléphone («smart» ou non). De manière générale, les métadonnées (qui communique avec qui, quand, où) constituent l'angle mort de la protection de la vie privée : par exemple, si le contenu d'un mail crypté est illisible par un tiers, l'expéditeur, le destinataire et l'objet du mail demeurent accessibles. Les méthodes les plus rustiques restent parfois les meilleures. Pour éviter d'être géolocalisé à cause de son téléphone, rien de mieux que de le laisser dans un tiroir.

Crypter ses SMS

Pas facile d'échanger de façon sécurisée sur un téléphone portable. Un certain Nicolas Sarkozy l'a appris à ses dépens. S'il s'était renseigné, il aurait pu découvrir l'offre pléthorique d'applications permettant de sécuriser ses communications sur les smartphones. Toutes ne sont pas recommandables, notamment celles qui n'ouvrent pas leur code source aux regards extérieurs. Depuis 2011, Open Whisper System fait le pari inverse. L'entreprise propose les applications TextSecure et RedPhone, pour envoyer des SMS et des appels

cryptés sous Android, ainsi que Signal, qui regroupe les deux fonctions sur iPhone. Elles sont évidemment compatibles entre elles.

Des applications pensées pour être faciles à utiliser. L'un des développeurs, Frederic Jacobs, pas encore 25 ans, prône *«la facilité d'usage de la cryptographie»* pour qu'elle se répande au-delà des cercles d'initiés. Le pari de la simplicité est réussi. Comme pour n'importe quel outil de tchat, il suffit de sélectionner le nom d'un correspondant qui l'utilise pour entamer une conversation cryptée, écrite ou orale. Consécration ultime, Edward Snowden lui-même en a recommandé l'usage lors de son intervention, l'an dernier, au festival South by Southwest.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde.fr
Le Monde.fr
dimanche 28 décembre 2014

# Comment la NSA tente de percer les remparts de sécurité sur Internet

Depuis plusieurs mois et le début des révélations d'Edward Snowden, les experts en sécurité informatique et les défenseurs de la vie privée en ligne ne savent plus à quel saint se vouer.

Révélation après révélation, les documents exfiltrés par le lanceur d'alerte américain au sujet de la NSA témoignent de la puissance de l'agence de renseignement et de sa capacité à percer les protections les plus robustes sur Internet. La question qui revenait sur toutes les lèvres était à la fois simple et complexe : quel outil lui résiste encore

» Lire aussi : Affaire Snowden : comment la NSA déjoue le chiffrement des communications

Au Chaos Communication Congress de Hambourg, un festival de quatre jours traitant notamment de sécurité informatique, les deux journalistes américains Jacob Appelbaum et Laura Poitras ont finalement apporté, dimanche 28 décembre, des réponses à cette question.

Lors d'une conférence, les deux journalistes ont présenté de nouveaux documents - également et simultanément publiés dans Der Spiegel - issus du stock soustrait par Edward Snowden. Ceux-ci révèlent que plusieurs outils, programmes ou langages informatiques posent de gros problèmes à la NSA lorsqu'il s'agit de les percer à jour. Ces documents, datent de 2012, mais le magazine allemand explique qu'ils ont de grandes chances d'être encore valables aujourd'hui.

Des outils résistent

Les outils dont la robustesse résiste à la NSA sont peu nombreux : GnuPG, qui sert à la protection des courriels, Tails, un système d'exploitation « amnésique » , OTR, un protocole informatique protégeant la confidentialité des discussions instantanées, les applications développées par le collectif Whispersystems ( comme Signal ), Truecrypt, un système de chiffrement des documents dont l'interruption mystérieuse a suscité de nombreuses interrogations et Tor, un navigateur permettant notamment une navigation anonyme sur Internet.

Les efforts de la NSA à l'encontre de Tor étaient déjà connus. Les nouveaux documents publiés montrent que ces efforts sont restés, pour le moment et jusqu'en 2012 au moins, sans effets.

» Lire : TOR, logiciel clé de protection de la vie privée, dans le viseur de la NSA

*« Je voulais faire une conférence positive »* explique Jacob Appelbaum, qui a fait applaudir par les 3 500 personnes massées dans l'auditorium du centre des congrès de Hambourg les développeurs de certains de ces outils.

De nombreux outils peu fiables

Lui et Laura Poitras n'ont cependant pu éviter l'énumération de quelques-uns des outils de protection des communications qui n'ont pas résisté à la NSA. Cette liste témoigne de l'ampleur des ressources consacrées par la NSA et certains de ses alliés à défaire certains des principaux moyens de protection des communications sur Internet.

*Der Spiegel* écrit par exemple que les connexions dites « https », où le « S » signifie « sécurisé » n'ont *« plus grand-chose de vraiment sécurisé »*. Selon un des documents publiés par le magazine allemand, la NSA prévoyait de *« casser 10 millions de connexions en https d'ici la fin de l'année 2012 »*. Ce type de protection permet à un internaute d'être certain de se connecter à un site authentique (de sa banque par exemple), et empêche un intermédiaire d'intercepter des informations qu'il lui transmet. Elle est utilisée quotidiennement par des centaines de millions d'internautes dans le monde entier, parfois sans même qu'ils s'en aperçoivent.

D'autres moyens de protection sont également à portée de la NSA, comme SSH, une technique pour connecter de manière sécurisée deux ordinateurs entre eux, largement utilisés par les informaticiens. Plus inquiétant, les documents indiquent que la NSA peut s'attaquer avec succès aux VPN (« réseaux privés virtuels »). Cette technologie, derrière son nom obscur pour le grand public, est pourtant centrale pour la sécurité de nombreuses entreprises, qui les utilisent par exemple pour accéder

depuis l'extérieur à leur réseau interne. Douze agents de la NSA ont ainsi été chargés de passer outre le VPN utilisé par le gouvernement grec, indique un des documents.

Une « guerre contre la sécurité sur Internet »

Pour contourner ces robustes protections, la NSA a recours à *« tous les moyens disponibles »*, écrit *Der Spiegel*, des super-ordinateurs capables de milliards de calculs à la seconde à l'envoi d'agents sous couverture pour tenter d'influencer le développement de ces moyens de protection. Ces moyens déployés ne sont pas surprenants : selon un document de la NSA reproduit par *Der Spiegel* le chiffrement des communications (et donc la confidentialité d'une part croissante des échanges sur Internet) est aujourd'hui *« une menace »* pour l'agence.

Ces nouveaux documents éclairent un peu plus ce que le magazine allemand décrit comme *« une guerre contre la sécurité sur Internet »*. Une sécurité, rappelle-t-il encore, qui est loin d'être l'apanage des terroristes ou des criminels, mais qui protège des centaines de millions d'internautes dans leur utilisation quotidienne d'Internet.

Les centaines d'activistes et militants qui ont applaudi, debout pendant plusieurs minutes, à la fin de la présentation de ces documents ont donc de quoi avoir la migraine devant les capacités de la NSA. Mais aussi de quoi se réjouir : *« ce n'est pas sans espoir, la résistance est possible »* a ainsi lancé M. Appelbaum. *« Le logiciel libre et une cryptographie bien implémentée fonctionnent.*

» Lire l'article de Der Spiegel dans son intégralité, en anglais



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde
Le Monde
France, mercredi 18 mars 2015, p. 8

France

# Débuts difficiles pour le blocage des sites Internet djihadistes

## Le ministère de l'intérieur a révélé, lundi, les cinq premiers sites bloqués en vertu de la loi antiterroriste, dont quatre restaient accessibles

**Soren Seelow (avec William Audureau)**

Il s'agit d'une des mesures phares de la loi antiterroriste votée en novembre 2014. L'une des plus difficiles à appliquer, et des plus contestées. Depuis le décret d'application du 5 février 2015, l'autorité administrative peut ordonner le blocage, sans passer par un juge, des sites Internet *« provoquant à des actes de terrorisme ou en faisant l'apologie »* . L'objectif affiché est de limiter, à défaut de pouvoir l'éradiquer, la propagande islamiste en *« libre-service »* sur la Toile.

La liste des cinq premiers sites « djihadistes » bloqués - théoriquement inaccessibles depuis vendredi - a été dévoilée, lundi 16 mars, par le ministère de l'intérieur. La Place Beauvau n'avait pas prévu de divulguer maintenant les premiers résultats de cette mesure qui est *« encore en phase de rodage »* , souligne-t-on dans l'entourage du ministre Bernard Cazeneuve. Mais la révélation du blocage d'un de ces sites par le journaliste de RFI David Thomson l'a incité à communiquer. Peut-être un peu tôt.

Si les cinq sites évoqués par le ministère sont bel et bien inaccessibles chez les principaux fournisseurs d'accès à Internet (FAI) - Free, SFR, Orange et Bouygues -, quatre d'entre eux étaient en revanche toujours visibles mardi chez des FAI d'importance moindre, comme Numericable. *« Il s'agit d'une mesure radicalement nouvelle, délicate à mettre en place »* ,explique-t-on place Beauvau pour justifier ces quelques problèmes de réglage.

**« Entraver au maximum »**

La divulgation de ces premiers sites bloqués permet néanmoins de comprendre l'esprit de ce nouveau dispositif de censure administrative. L'un de ces sites publie la traduction d'un discours d'Abou Bakr al-Baghdadi, chef de l'Etat islamique. Deux autres sites permettent de télécharger le magazine d'Al-Qaida, *Inspire*. Le quatrième, Alhayat Media Center, un site sympathisant de l'EI qui rediffuse des vidéos de propagande, parmi lesquelles des exécutions. Le dernier est un blog confidentiel, que son auteur a déclaré inactif début mars.

Les forums les plus actifs, où s'échangent les informations les plus détaillées, constituent une mine d'informations pour la lutte antiterroriste, et ne sont pas ciblés. Seuls des sites relativement statiques et accessibles au grand public ont été bloqués. Une approche assumée par le gouvernement, qui entend promouvoir au-delà de ses frontières le principe d'une *« régulation »* de la propagande djihadiste sur Internet, sans pour autant gêner le travail des services de renseignement.

*« On ne cherche pas à tout bloquer, mais à entraver au maximum*, explique un conseiller de Bernard Cazeneuve. *L'idée est de cibler l'apologie du terrorisme en libre-service. Les contournements sont possibles. On sait que les djihadistes convaincus accéderont à ces sites »* , grâce notamment à des logiciels libres comme Tor.

Concrètement, la loi votée en novembre 2014 permet à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de dresser une liste de sites à bloquer, préalablement validée par les services de renseignement. Ces demandes sont ensuite adressées aux éditeurs ou aux hébergeurs, qui ont vingt-quatre heures pour obtempérer.

Passé ce délai, l'autorité administrative est habilitée à ordonner directement aux fournisseurs d'accès de détourner les requêtes DNS (les demandes d'accès à un nom de domaine) vers une page du ministère de l'intérieur frappée d'une main rouge.

Mais la loi prévoit aussi la possibilité de contourner les hébergeurs quand ils ne figurent pas dans les mentions légales du site afin de solliciter directement les FAI. C'est la solution qui a été retenue pour cette *« phase d'essai »* . Les autorités ont ciblé cinq sites dont les hébergeurs n'étaient pas mentionnés explicitement et ont envoyé leurs demandes mercredi aux principaux FAI, pour un blocage effectif vendredi chez la plupart d'entre eux. L'idée, ambitieuse, d'une régulation de la propagande djihadiste en ligne est l'un des chevaux de bataille du ministère de l'intérieur. Fin février, Bernard Cazeneuve a entamé, lors d'une visite dans la Silicon Valley, des discussions informelles afin de sensibiliser les principaux géants du Net (Google, Facebook, Microsoft, Twitter...) à la conception française de *« l'apologie »* du terrorisme et des limites de la liberté d'expression. Un dialogue *« compliqué »* ,résume-t-on dans l'entourage du ministre, qui a vocation à se poursuivre.

La collaboration des principaux opérateurs américains sera pourtant indispensable : la page Facebook de Islamic-News, un des sites bloqués depuis vendredi par les autorités françaises, est toujours active et compte plus de 40 000 membres.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Atlantico (site web)
lundi 10 novembre 2014 - 10:17 UTC +01:00

# La guerre contre le deep web et les hors la loi en ligne peut-elle être gagnée ?

**Jean-Paul Pinte**

**Le FBI a annoncé avoir arrêté l'administrateur de Silk Road 2.0, une plateforme de vente de produits et de biens illicites comme de la drogue ou encore des armes, alors que la première version du site avait déjà été suspendue en 2013.**

**Atlantico : Récemment, le FBI a annoncé avoir arrêté l'administrateur de Silk Road 2.0, une plateforme de vente de produits et de biens illicites comme de la drogue ou encore des armes. A quelles difficultés spécifiques à la lutte contre les criminels du deep web les autorités sont-elles confrontées ?**

**Jean-Paul Pinte :** Les internautes ne connaissent en général que le Web surfacique, celui accessible principalement par leur moteur de recherche préféré "Google". Ils ne balaient alors qu'une infine partie du Web. D'autres parlent du Web invisible, pas si invisible que cela mais nécessitant une bonne culture informationnelle sur la toile et des outils en dehors des chemins battus de Google. Tout ceci parce qu'ils ne savent pas que des outils gratuits existent pour explorer. Ces derniers leur permettraient alors d'accéder à ce Web abyssal qui regroupe tous les résutats que les moteurs de recherche traditionnels n'indexent pas pour des raisons de format par exemple. Une autre poignée initiés connaissent les méandres de la toile et utilisent un autre espace parallèle. Appelons comme on le veut, Web profond, Dark Web ou encore Deep Web, ce réseau est un lieu où prospèrent les trafics en tout genre. On y retrouve, entre autre**, des clients vendant tous les jours de la méthamphétamine, une drogue de synthèse hautement addictive aux effets euphorisants à 32 euros le demi-gramme. On peut aussi y vendre en Australie de la drogue achetée en Hollande. Des documents ou pièces d'identité comme bien d'autres produits s'y achètent.**

*A lire egalement >>>>>>> 4chan et les photos de trop : le site de tous les mauvais goûts tombera-t-il sur les images du meurtre d'une jeune américaine postées par son tueur ?*

Sur le Darknet, vous avez la garantie de rester anonyme parce que vos navigations sont cryptées, donc indéchiffrables. Le principe de tor est que quand on va sur un site, on passe par différents noeuds et a chaque fois que l'on passe par un noeud on nous attribue son adresse IP. Voila pourquoi on dit que c'est anonyme. Une aubaine pour ceux qui, du fait de leurs activités illégales, ont besoin d'avancer masqués. Mais une aubaine aussi pour opérer sans risque dans des pays où Internet est censuré, où les opposants sont pourchassés. Bref, comme souvent, on y trouve le meilleur comme le pire.

L'installation de Tor n'est pas suffisante pour accéder au Darknet associé. Pour utiliser le réseau, il faut utiliser un navigateur spécifique à Tor (installé avec le package Tor, *Tor Browser Bundle*) et connaître les adresses des sites à visiter, toutes se terminant par ".*onion*".

Les produits traversent souvent les frontières. Un marché dynamique et en expansion comme un continent virtuel ouvert au monde entier à l'aide des réseaux et où se retrouvent des milliers de trafiquants, où se croisent des hackers, pirates, vendeurs d'armes, dissidents ou djihadistes. Les opposants politiques, les avocats et les journalistes désireux de communiquer en toute discrétion le connaissent bien. C'est le réseau TOR (The Onion Router), constitué, comme les pelures d'un oignon, de multiples strates. Une fois cette frontière passée, vous êtes en mode furtif. Depuis quelques temps, le Bitcoin sorte de monnaie virtuelle y est même utilisé et permet aux cyberdélinquants de ne plus être traçables sur la toile. On compterait à ce jour près de 1500 vendeurs qui y travaillent sans stock. On remarque aussi que les produits voyagent beaucoup.

**Les deux stars du *deep web* sont Hidden Wiki et Silk Road**. Cette dernière route de la Soie représentait l'an passé 1,2 million de dollars par mois, dont 92 000 étaient reversés aux seuls administrateurs. A ce jour, seul un trafiquant présumé opérant sur Silk Road a été arrêté à l'été 2012. Il s'agit d'un Australien, Paul Leslie Howard.

**Il y a fort à parier que la guerre menée contre cet espace parallèle ne cessera pas subitement même si l'on vient d'arrêter à San Francisco, l'administrateur présumé d'une seconde version du site Silk Road, surnommé "l'eBay de la drogue".** Ross William Ulbricht, âgé de 26 ans, encourt une peine de prison à vie. "Derrière ces marchés noirs se cachent en effet des personnes qui gagnent des millions d'euros", précise Lodewijk van Zwieten, expert en cybercrimes au parquet néerlandais. Les idées ne manquent pas et ces cyber-délinquants qui ont toujours un pas d'avance dans le domaine.

**La première version du site avait déjà été suspendue en 2013, avant d'être remplacée seulement un mois plus tard par Silk Road 2.0. Si la lutte contre cette criminalité peut ressembler à celle contre la criminalité traditionnelle, en quoi le fait qu'elle ait lieu sur Internet facilite-t-il une plus grande rapidité dans l'implantation et le succès de ces mafias ?**

Internet a été pensé et conçu sans sécurité et très vite des cyberdélinquants y ont pris place car il est vrai que la peine encourue y est bien moins importante pour eux que dans la criminalité traditionnelle. **Tout va très vite sur la toile et si ceux qui luttent contre la cybercriminalité ont fait de gros efforts ces dernières années pour tenter de ralentir ce fléau, ils vont moins vite que ceux qui ont pour principal but de préparer des attaques ou toute autre forme de criminalité numérique.**

La disparition des frontières avec la toile n'est pas non plus sans favoriser le développement de ces mafias et l'on sait très bien que dès que l'on a reussi à déjouer une attaque, ceux qui sont de l'autre côté ont déjà prévu la suite. Espace décentralisé et anomyme, Internet facilite le développement des mafias comme il le fait pour le terrorisme. Tout devient complexe pour qui veut suivre au jour le jour le fonctionnement de ces mafias et leur pérégrination sur la toile. L'époque du pirate en chambre est révolue et la sophistication des attaques couplée à un développement des techniques d'ingénierie sociale n'a fait qu'évoluer ces dernières années. On peut même parler aujourd'hui d'organisations criminelles de plus en plus organisées voire même d'un certain hooliganisme version numérique. **Les ventes de produits illégaux prennent alors une tournure de plus en plus professionnelle.**

**Une autre opération d'envergure appelée Onymous a permis de fermer 414 autres sites illégaux et d'interpeller 16 personnes impliquées dans plusieurs pays. Cette lutte exige-t-elle une coopération particulière entre les Etats pour aboutir ?**

La question de la coopération internationale en matière de cybersécurité n'est pas nouvelle à en croire ce rapport d'un laboratoire de l'IRSEM. Depuis une vingtaine d'année, le rôle croissant de l'Internet dans le fonctionnement de la société conjugué à l'explosion de la cybercriminalité ont incité les États à coopérer afin de répondre à un phénomène de plus en plus organisé. Depuis elle a gagné en importance avec la démocratisation de l'usage de l'internet.

L'État se trouve impuissant à lui-seul pour garantir sa sécurité nationale. **La coopération internationale constitue donc une composante indispensable à la mise en oeuvre d'une réponse qui se voudrait efficace.** Une telle coopération doit cependant faire face à un certain nombre d'enjeux. Aucun progrès ne peut être accompli dans le monde au niveau des attaques sans un travail de coopération entre les pays et Europol en est le principal coordonnateur avec le FBI.

**Dans le contexte de la cyberscriminalité, la coopération internationale entre les États, les organisations internationales et régionales et d'autres entités s'impose par la nature de plus en plus sophistiquée des cybermenaces qui évoluent sans frontières.** Tout acteur, que ce soit un pays ou une organisation non gouvernementale, qui suit ses objectifs en matière de cybersécurité requiert alors la coopération de nombreux partenaires internationaux. Cette collaboration internationale aura principalement lieu en dehors des cadres nationaux spécifiques.

**Les progrès en cybersécurité dépendent donc pour un pays, dans une large mesure, de la volonté politique des divers acteurs**. Tous les dommaines comme le partage de l'information et du renseignement et l'aide mutuelle peuvent devenir essentiels pour gérer une cybercrise mais l'efficacité d'une telle coopération dépend considérablement de la cohérence des objectifs politiques et des relations bilatérales et multilatérales signale une chronique de l'ONU à ce sujet. Dans de nombreux domaines, comme la coopération internationale en matière pénale, plusieurs conditions préalables doivent être mises en place dans les pays qui coopèrent, comme le

droit positif national, le droit procédural et les accords internationaux, avant qu'un dialogue sur la possibilité d'une coopération internationale quelconque donne lieu à des discussions sur l'efficacité d'une telle coopération. Au niveau de l'Europe, la Commission européenne propose un plan de cybersécurité pour l'UE qui prône pour les opérateurs une obligation de signaler les incidents de sécurité significatifs qui touchent leurs services essentiels.

La proposition de directive prévoit notamment les mesures suivantes :

Les États membres doivent adopter une stratégie de SRI et désigner des autorités nationales compétentes en la matière, qui disposeront de ressources financières et humaines suffisantes pour prévenir et gérer les risques et incidents de SRI et intervenir en cas de nécessité.

Un mécanisme de coopération entre les États membres et la Commission doit être instauré pour diffuser des messages d'alerte rapide sur les risques et incidents au moyen d'une infrastructure sécurisée, pour collaborer et organiser des examens par les pairs.

Les opérateurs d'infrastructures critiques de secteurs tels que les services financiers, les transports, l'énergie et la santé, les facilitateurs de services internet clés (notamment les magasins d'applications en ligne, les plateformes de commerce électronique, les passerelles de paiement par internet, les services informatiques en nuage, les moteurs de recherche ou les réseaux sociaux) ainsi que les administrations publiques doivent adopter des pratiques en matière de gestion des risques et signaler les incidents de sécurité significatifs touchant leurs services essentiels.

Même si cela se passe pas à pas, de nombreuses avancées et progrès ont déjà été faits dans le domaine de la coopération internationale autour de la cybercriminalité car la prise de conscience est présente aujourd'hui pour tous les Etats.

**"Pendant longtemps les criminels (du Darkweb) se sont considérés comme intouchables", a déclaré Troels Oerting, le chef de l'unité de crimes sur Internet d'Europol. Comment les autorités comme Europol ou le FBI se sont-elles adaptées aux spécificités du Deep Web ?**

Le sujet n'est pas neuf pour le FBI la CIA et Interpol et cela faisait un moment qu'ils attendaient de pouvoir arrêter l'une des grandes pointures du réseau TOR. Ces organismes ont du recul dans le domaine et s'y sont intéressé il y a déjà plusieurs années avec des sujets comme la pédopornographie. Dans ce domaine, l'arrestation en Irlande du fondateur présumé de l'hébergeur anonyme Freedom Hosting semble constituer l'épilogue d'un techno-thriller haletant. Selon des experts, les autorités américaines l'auraient traqué aux confins du "deep Web", notamment via un virus qu'elles auraient spécifiquement conçu pour le débusquer.

C'est aussi toute une coordination étroite d'équipes de spécialistes entre ces trois organisations travaillant sur des investigations de plus en plus pointues dans le Web profond qui ont permis aujourd'hui d'y voir plus clair. Cartographie de réseaux, cyber-infiltration de la toile sont au coeur de leurs pratiques avec des équipes de plus en plus formées et compétentes.

Le FBI, la CIA et Interpol sont trois organisations bien distinctes dans le gouvernement américain. Le FBI et la CIA sont tous deux responsables de la collecte de renseignements pour protéger le pays. Le FBI concentre ses ressources sur les crimes fédéraux tandis que la CIA recueille des renseignements à des fins de sécurité nationale. Interpol est une organisation internationale dont la mission est d'aider les Etats-Unis à résoudre un crime dans 190 pays. C'est ainsi que le réseau Tor est sorti de l'ombre grâce à une fine analyse et surveillance assidues de ces organismes mais il reste encore énormément de contenu, car 90% du contenu du web n'est pas référencé sur Google, et une bonne partie transitait sur le réseau Tor.

**Peut-on s'attendre à une escalade technique de ces criminels pour échapper à la justice en préservant leur anonymat ? Quelles en sont les limites ?**

La course au pseudonymat ne fait que commencer et de plus en plus il s'agira pour nos Etats de connaître ceux qui agissent sous cet angle de la cybercriminalité qui était restée jusqu'à ce jour difficilement pénétrable. Le Big Data et l'Open Data dont on parle tant aujourd'hui ne feront qu'accroître le phénomène car nous allons vers une science des données où les compétences d'exploration du Deep Web trouveront plus leur sens encore. Dans les entreprises, on évoque déjà l'embauche de Data Scientists comme une compétence inestimable. On ne peut vraiment parler de limites en ce domaine car tout va très vite mais la

capacité des Français à imaginer des solutions pour contrer les attaques des cybercriminels progresse. Dans ce contexte, certaines start-up vont même plus loin en conciliant intelligence artificielle et Big Data. L'enjeu étant de détecter très rapidement des signaux et des comportements incongrus avant que le pillage ou la destruction des données n'aient commencé.

On peut citer quelques initiatives françaises reprises dans ce lien intéressant :

- CybelAngel scrute la face cachée du Web.- Ercom met les Smartphones Android sous haute protection.- Qosmos décrypte le trafic de données.- Akheros détecte les comportements incongrus.- Idecsi protège les boîtes mail.- Wooxo, ange gardiden des PME et TPE.

**Note(s) :**

Mise à jour : 2014-11-10 12:17 UTC +01:00

**Illustration(s) :**


Le FBI a annoncé avoir arrêté l'administrateur de Silk Road 2.0.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Intelligence ONLINE
Intelligence Online - Édition française, no. 717
RENSEIGNEMENT D'ETAT, TERABYTES, mercredi 30 juillet 2014

## L'anonymat de Tor attaqué de toutes parts

**Tor | STiS | NSA | Edward Snowden | GCHQ | Das Erste | MIT | US Naval Research Laboratory | Tor | Broadcasting Board of Governors | I2P**

**Les agences de renseignement cherchent à identifier les usagers du réseau Tor, qui permet de naviguer anonymement sur Internet.**

**5,25,2BASE**

**Offensive russe** - Développé pour permettre aux opposants et journalistes de communiquer anonymement sur la Toile, mais aussi utilisé pour contrôler les réseaux d'ordinateurs piratés (*botnets*), le réseau décentralisé **Tor** est plus que jamais ciblé. Moscou vient d'émettre un appel d'offres - réservé aux sociétés russes - visant explicitement à trouver les moyens d'identifier ses utilisateurs et l'équipement informatique qu'ils emploient pour s'y connecter. Ce contrat, qui doit être attribué fin août, est piloté par l'unité **STiS**, le centre de R&D du ministère russe de l'intérieur pour les "équipements spéciaux".

**La NSA sur la brèche** - L'ex-*Contractor* de la **NSAEdward Snowden** avait révélé fin 2013 que l'agence américaine et le **GCHQ** britannique planchaient eux aussi sur cette problématique. Selon les documents rendus publics à l'époque, la NSA affirmait notamment qu'elle ne pourrait *"jamais"* démasquer tous les utilisateurs de Tor. Mais l'agence progresse. Dans une enquête de la télévision allemande **Das Erste** diffusée le 3 juillet, des développeurs de Tor ont déclaré que le logiciel d'interception de masse *XKeyScore* de la NSA a été récemment paramétré pour repérer tous les internautes se connectant aux "annuaires" de Tor, des serveurs distribuant la liste de tous les relais du réseau. Cette manoeuvre permettrait à la NSA de lister tous les utilisateurs de Tor, mais pas encore de déchiffrer leurs communications.

The Tor Project (Torproject.org) Développé en 2004 par des chercheurs du MIT et de l'US Naval Research Laboratory, Tor a bénéficié de l'appui du département d'Etat et du Broadcasting Board of Governors, qui y voyaient un moyen d'aider la dissension contre les régimes adverses (IOL nº597).I2P (Geti2p.net) Alternative à Tor, le réseau décentralisé I2P (Invisible Internet Project) est développé et maintenu par un collectif de bénévoles, tous anonymes. Il n'emploie pas de listes centralisées de noeuds réseaux, principale faiblesse du modèle de Tor, que la NSA exploite à son avantage (lire ci-contre).

Tor | STiS | NSA | Edward Snowden | GCHQ | Das Erste | MIT | US Naval Research Laboratory | Tor | Broadcasting Board of Governors | I2P5,25,2BASE



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde.fr
Le Monde.fr
mardi 23 avril 2013

# La police japonaise recommande le blocage du réseau TOR

La National Police Agency (NPA), un équivalent japonais du FBI, souhaite que les fournisseurs d'accès Internet bloquent l'accès au réseau anonyme TOR (The Onion Router). Ce réseau décentralisé fait transiter les connexions des internautes par des serveurs de volontaires répartis partout dans le monde, dans le but de les anonymiser. La volonté des autorités est née d'un échec dans la traque d'un internaute en fin d'année dernière, rapporte The Mainichi , cité par Wired UK .

Un pirate du nom de Demon Killer a ainsi envoyé des menaces de mort sur des forums en utilisant quatre adresses de connexion (adresses IP) différentes. La police a d'abord arrêté les quatre personnes dont les adresses avaient été utilisées et obtenu de faux "aveux"... avant de voir que des messages étaient toujours envoyés. En début d'année, la police a arrêté l'auteur présumé de ces menaces. En inspectant ses ordinateurs, les enquêteurs ont découvert qu'il utilisait régulièrement TOR pour anonymiser sa connexion.

## EMPÊCHER DES "ABUS" DE TOR

La NPA a formé un panel chargé de se pencher sur des moyens de lutter contre les crimes *"abusant"* du système TOR. Dans son rapport, remis jeudi 18 avril, le panel explique que l'outil d'anonymisation a été utilisé ces dernières années pour l'envoi de menaces de mort sur des forums, le vol d'argent par intrusion dans des sites de banques, l'envoi de messages sur des *"sites de rencontre"* entre hommes et enfants ou encore la publication d'informations de sécurité de la police tokyoïte.

Pour lutter contre ces abus, le panel recommande de bloquer la connexion de l'internaute quand il accède à un site par une adresse IP officiellement listée comme celle d'un serveur de TOR. *"Il existe ainsi environ 3 400 noeuds TOR répertoriés "*, identifiables et potentiellement blocables, explique Vigdis, un bénévole qui maintient un noeud. Il existe pourtant environ un millier d'autres noeuds non-répertoriés, les "bridges", dont les adresses ne sont pas connues publiquement, explique le bénévole.

Le réseau TOR, s'il est ici exploité pour des activités illégales, est également un outil essentiel à certaines luttes politiques, au point que Reporters sans frontières le recommande dans son kit de survie numérique. *"TOR est utilisé par ceux qui ont envie de garder un minimum d'anonymat et de vie privée et par ceux qui veulent garder leurs serveurs anonymes avec les noms de domaine en .onion* [uniquement accessibles par ce réseau], *ce qui permet de publier sans être inquiété"*, explique Vidgis, qui évoque notamment Wikileaks ou des blogueurs dissidents de certains pays.

<< Lire : " Surfer sans entraves"

## UN MOYEN PARMI D'AUTRES

*"La liste des noeuds est publique, il suffit de tuer toutes les connexions vers ces noeuds* [pour espérer bloquer TOR]. *Ensuite, il reste les 'bridges'* [non-répertoriés], *donc ce blocage est inutile et il faut aller plus loin, par des scans massifs de réseau*", à la manière de la Chine, affirme Vidgis. *"Pour les 'pirates' qui s'en servent pour s'introduire dans des sites de banques, il leur est toujours possible d'anonymiser leur connexion autrement. C'est comme interdire les couteaux de cuisine parce qu'on peut tuer avec"*, juge pour sa part Nicoo, un ex-bénévole qui a retiré son noeud du réseau en novembre.

*"Bloquer TOR est faisable, certains Etats y arrivent* [notamment par l'inspection des paquets], *mais c'est compliqué. J'attends de voir ce que vont faire* [les Japonais]. *Ça permettra d'avoir une plate-forme de test pour les versions qui servent en Chine et en Iran , sans les risques liés à ces pays. TOR est un moyen technique, ça n'empêche pas les forces de police de faire des enquêtes traditionnelles"*, ajoute Vigdis.

Parmi les outils de contournement de censure, les réseaux privés virtuels (VPN) - des tunnels qui permettent d'accéder à des sites censurés dans certains pays -, sont dans le collimateur de gouvernements, qui ont multiplié les mesures de blocage ces derniers mois.

<< Lire : " RSF liste les pays et entreprises "ennemis d'Internet" en 2012"

Le Monde.fr



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Les Echos.fr
Les Echos.fr
jeudi 12 novembre 2015

# Le FBI aurait payé une université pour attaquer le réseau TOR

## LES ECHOS

**Selon les responsables du projet TOR, des chercheurs de l'Université Carnegie Mellon aurait été payés pour attaquer le réseau informatique permettant de communiquer sur Internet de façon anonyme.**

Il est clair que les gouvernements n'aiment pas lorsque ses administrés se terrent dans l'ombre. D'autant plus quand ceux-ci naviguent de manière anonyme sur un vaste territoire comme Internet. Aux Etats-Unis par exemple, le FBI mène une guerre totale contre le réseau Tor, considéré comme la principale porte d'entrée menant à l'Internet anonyme.

Pour l'instant, la dextérité des développeurs arrivait plus ou moins à contrecarrer la grosse machine gouvernementale. Mais à en croire l'équipe du projet Tor qui gère le réseau, cet équilibre pourrait être mis à mal. Et c'est l'idée même de Tor qui serait visée. Dans un billet de blog, elle explique que des chercheurs de l'Université Carnegie Mellon, aurait été payés pour mener une opération de « désanonymisation » des utilisateurs de Tor.

Dans leur article, Tor Project, dévoile même le montant de la transaction entre le FBI et l'université : 1 million de dollars.

### Libertés civiles attaqués

L'accusation repose pour l'instant uniquement sur les témoignages de spécialistes de la cybersécurité. Mais de forts soupçons existaient déjà.

Ainsi, comme le relève le site spécialisé Numerama, en 2014, lorsqu'un membre de l'équipe de Silk Road -une plate-forme permettant d'acheter et de vendre de la drogue sur Internet de manière anonyme - se retrouve face au tribunal, les pièces du procès montrent que l'homme a été retrouvé grâce à un *« institut de recherche basé dans une université qui opérait ses propres ordinateurs sur le même réseau anonyme que celui utilisé par Silk Road »* . Comprendre Tor.

Dans le même temps, des chercheurs de l'université Carnegie Mellon avaient annulé une conférence qui tendaient à démontrer comment désanonymiser Tor. Selon le site The Verge, les attaques auraient aussi permis une énorme opération contre l'internet de l'ombre baptisée Opération *« Onymous »* .

Pour l'équipe de Tor, il s'agit là d'une attaque qui va à *« l'encontre des libertés civiles »* , considérant qu'il y a peu de chances que le FBI ait obtenu un mandat pour agir de la sorte.

Pourtant, si cette manoeuvre était confirmée, elle ne serait pas la première de ce type. En juillet 2014, la Russie avait annoncé offrir près de 4 millions de roubles - 85.000 euros - à ce celui qui serait capable de décrypter les données envoyées par l'intermédiaire du réseau Tor.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Point.fr
Le Point.fr
Tech & Net, lundi 21 mars 2011

# L'Iran étrenne une puissante technique de cybercensure

**Par Guerric Poncet**

**La technologie DPI n'a jamais été exploitée à si grande échelle par un État. Des entreprises occidentales sont soupçonnées d'aider Téhéran.**

Humiliés par le virus Stuxnet, les spécialistes informatiques iraniens ne sont pas pour autant à la traîne. Au cours des dernières semaines, les autorités du pays ont réussi à mettre hors service Tor, un réseau très utilisé par les opposants au régime de Mahmud Ahmadinejad. Tor repose sur Internet, mais n'utilise pas exactement les mêmes mécanismes. Il permet aux internautes de naviguer ou de communiquer de façon cryptée. Il est très apprécié des cyberactivistes et des journalistes. Environ 250 000 ordinateurs y sont connectés en permanence dans le monde, rapporte le Daily Telegraph.

Sans un appareillage sophistiqué, il est impossible de distinguer le trafic crypté de Tor du trafic crypté d'un banal site d'e-commerce ou de banque. Et c'est bien le problème : l'Iran a réussi à couper uniquement Tor, laissant transiter normalement le reste des données. Pour cela, les ingénieurs ont très probablement utilisé la technologie DPI (deep packet inspection), très intrusive. Le DPI consiste à ouvrir chacun des paquets de données transitant sur un réseau pour en vérifier le contenu, l'origine et la destination. Très décrié, il équivaut grosso modo à une ouverture systématique du courrier postal dans les centres de tri.

## Course à l'armement

Le matériel nécessaire est très lourd, car il faut disposer de puissants systèmes d'analyse pour ne pas perturber l'ensemble du trafic. Dans le monde, une poignée de fabricants maîtrisent cette technologie, dont l'américain Cisco Systems ou l'européen Nokia-Siemens communications. Le premier avait été accusé de fournir du matériel de filtrage à la Chine lors de la construction de sa cyber Grande Muraille, et le second avait été entendu par le Parlement européen après la vente de matériel de surveillance à un opérateur iranien.

"D'un point de vue technique, ce qu'ils ont fait est fantastique", explique Andrew Lewman, directeur exécutif du Tor Project, une organisation à but non lucratif. Selon lui, l'Iran est désormais plus avancé que la Chine en matière de filtrage d'Internet. Le réseau est parfaitement conscient de ses points faibles, et s'attendait à être attaqué de la sorte. Tor a rapidement été modifié pour mieux passer inaperçu et le nombre de connexions venant de l'Iran est revenu à la normale. Mais le pire cauchemar de Tor semble se réaliser : des États, et probablement des multinationales, lancent une "course à l'armement" avec les réseaux cryptés.

Courant 2010, l'Iran avait subi une attaque informatique très sophistiquée. Le ver Stuxnet, visiblement développé par des experts occidentaux, avait infiltré les logiciels de contrôle du programme nucléaire civil iranien. La découverte de l'attaque et de son niveau technique a profondément modifié les doctrines de cyberdéfense des États et les pratiques de sécurité des grandes entreprises. En France, la Hadopi, gendarme du piratage, est accusée de mener des expérimentations sur le DPI, ce que dément catégoriquement son secrétaire général Éric Walter.

**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

L'OBS
L'Obs (site web)
Tech, mardi 8 décembre 2015

# Supprimer le wifi public, interdire TOR : les inquiétants souhaits de la police

**Schmitt, Amandine**

**Selon les informations révélées par "Le Monde", le gouvernement envisagerait d'interdire TOR et de restreindre l'accès au wifi public. Mais est-ce bien raisonnable ?**

L'état d'urgence pourrait-il justifier la fin de l'anonymat sur internet ? "Le Monde" a révélé ce week-end de surprenants documents internes au ministère de l'Intérieur. Etabli le 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), le texte recense toutes les mesures que les policiers et les gendarmes souhaiteraient voir passer dans le cadre de projets de loi en cours d'élaboration. Ces demandes ne sont pas encore approuvées, mais simplement étudiées avant un arbitrage du gouvernement. Elles laissent entrevoir des envies particulièrement liberticides que le climat post-attentats serait censé excuser. Revue de détails.

# Supprimer les connexions wifi publiques

Parmi ces mesures, qui s'apparentent parfois à une "liste au Père Noël" selon le quotidien, "interdire les connexions WiFi libres et partagées" durant l'état d'urgence et supprimer les "connexions wifi publiques", "sous peine de sanctions pénales". Si les réseaux wifi ouverts agacent les policiers, c'est parce qu'ils compliquent l'identification des personnes connectées.

Une mesure qui paraît démesurée dans un pays champion du monde du wifi avec plus de 13 millions de bornes selon le cabinet spécialisé Maravedis Rethink. Rien qu'à Paris, le wifi gratuit est accessible dans plus de 300 lieux.

L'Etat ne peut donc pas contrôler tous les réseaux wifi sur le territoire, mais peut définir une peine suffisamment élevée pour qu'il soit dissuasif de braver l'interdiction. Ce serait donc la fin des écrivains du dimanche qui passent leur vie au Starbucks pour mieux profiter du wifi. Il faudrait également que les opérateurs ferment leurs réseaux partagés comme le très utilisé Free Wifi et ses trois millions de hotspots.

Pour Adrienne Charmet-Alix, coordinatrice des campagnes de l'association La Quadrature du Net, la mesure serait extrêmement "impopulaire", d'autant qu'elle pourrait empêcher certaines entreprises de travailler dans de bonnes conditions. "C'est paradoxal d'encourager l'économie numérique d'un côté et de créer de mauvaises conditions d'utilisation des réseaux de l'autre", note-t-elle.

NextInpact rappelle aussi que, en amont des débats sur la loi Hadopi sur le téléchargement illégal, le Conseil général des Technologies de l'Information avait déjà proposé en 2009 de restreindre les accès wifi publics proposés à titre gratuit. L'idée avait été rapidement abandonnée en raison des difficultés pratiques.

Manuel Valls a finalement réagi mercredi 9 décembre sur BFMTV/RMC : "Non, l'interdiction du Wifi n'est pas une piste envisagée aujourd'hui, je vous le confirme", a-t-il déclaré. Le Premier ministre a affirmé "ne pas avoir entendu parler" d'une demande de la police de faire interdire ces réseaux ouverts.

# Interdire TOR

Autre mesure désirée par les autorités, "interdire et bloquer les communications des réseaux TOR en France". TOR est un réseau d'anonymisation de la navigation. Il est constitué de multiples strates, comme les pelures d'un oignon - TOR est l'acronyme de The Onion Router - et fait passer l'information par de multiples relais afin qu'il soit impossible de remonter jusqu'à la source. Créé à l'origine par l'US Naval Research Laboratory, un laboratoire militaire américain, ce réseau privé est devenu particulièrement populaire après la fermeture de la Route de la Soie, ou "eBay de de la drogue", mais aussi après les révélations d'Edward Snowden sur l'espionnage par la NSA.

Bloquer entièrement TOR serait compliqué, mais pas impossible. Les noeuds de sortie utilisés par le réseau sont publics : pour éviter que les utilisateurs s'y connectent, il faudrait

s'adresser aux fournisseurs d'accès à internet (FAI) pour qu'ils les bloquent. Mais, TOR s'appuie aussi sur certains noeuds non publics, les "bridge relay", qui seraient plus difficiles à détecter par le censeur. Certains utilisateurs se servent également d'un VPN (réseau privé virtuel) avant d'utiliser TOR, ce qui permet de brouiller sa localisation. Là, le gouvernement devrait bloquer tous les VPN existants, ce qui est impossible.

L'Iran et la Chine ont déjà tenté de bloquer TOR, des comparaisons en terme de liberté d'expression qui ne seraient pas flatteuses pour la France.

# Livrer les clés de chiffrement des applis

les policiers et les gendarmes font par d'un autre souhait selon le document consulté par "Le Monde" : "identifier les applications de VoIP [téléphonie par Internet] et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement".

Là encore, difficile de savoir comment le gouvernement pourrait appliquer cela techniquement. Comme le rappelle BFMTV, certaines applications utilisent le chiffrement "de bout en bout" : l'éditeur ne dispose d'aucune clé, seuls les utilisateurs en ont connaissance. C'est notamment le cas de l'application Facetime d'Apple.

La seule possibilité serait que l'éditeur laisse une "back door", une porte de sortie qui serait utilisable par le gouvernement. Problème : une telle porte fonctionne dans les deux sens. "Les points de fragilité dans les systèmes peuvent très bien être utilisés par les pirates ou les pays ennemis", indique Adrienne Charmet-Alix.

Avec de telles mesures, c'est la sécurité sur internet dans son ensemble qui est attaquée."

"Cela fait au moins deux ans que les autorités parlent d'obtenir des clés de déchiffrement, que ce soit en France, aux Etats-Unis ou au Royaume-Uni", reprend-t-elle. "En gros, on peut chiffrer, tant que l'Etat peut déchiffrer. Il n'y a pourtant aucune donnée qui montre à quel point le chiffrement entrave les enquêtes. Est-ce que ça empêche totalement de remonter les réseaux ? Quelle est la part du chiffrement dans les actes criminels ? Est-ce qu'on y perdrait en vie privée ? Par contre, on sait parfaitement que ça ne permettrait pas d'arrêter qui que ce soit."

Le débat sur le chiffrement avait déjà repris à l'annonce que Daech se sert de l'appli de messagerie Telegram pour mieux communiquer. Ils ne sont pourtant pas les seuls à utiliser Telegram, ni WhatsApp, que "la plupart des gens utilisent sans même savoir que c'est crypté", selon Adrienne Charmet-Alix. Tandis qu'on a confirmation que l'un des terroristes du Bataclan a envoyé le message "On est parti on commence" avant la mortelle fusillade. C'était un SMS en clair.

Amandine Schmitt



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

The New York Times
The New York Times
Late Edition - Final
Sports, Thursday, June 18, 2015, p. B 11

# Traces of Hacking Found Despite Efforts at Secrecy

**By JAMES GLANZ**

The F.B.I.'s route to the St. Louis Cardinals' front office in pursuit of an apparent hacker, or hackers, involved a trip through a shrouded corner of the Internet.

The website Deadspin pointed out last June that internal documents from the Houston Astros had been posted anonymously on a site called Anonbin. Alarmed, the Major League Baseball commissioner's office notified law enforcement officials. From the Anonbin posting, those officials worked backward to find the perpetrator, who had tried to leave no tracks.

The person or people who penetrated the Astros' network apparently used a network of servers called Tor to hide the source of the documents that found their way to the site.

"Tor is among the best anonymizing services out there, but it is not a silver bullet," said Sascha Meinrath, director of X-Lab, a technology policy organization in Washington. Tor is most effective in the hands of an experienced hacker, Mr. Meinrath said. The hacking, though, seems to have left traces somewhere in the welter of Tor servers.

"What this tells me is that whoever leaked this is not very tech savvy," he said.

The Tor network functions as a sort of Internet maze to throw off anyone who tries to trace the origin of an electronic message, Mr. Meinrath said. When the network receives a message, it bounces from server to server. The ordinary Internet pastes a series of addresses onto a message, allowing it to be traced back to the sender. In contrast, the Tor network strips that information out.

When the message emerges from the network, the source is, in theory, untraceable. Even so, it has long been known that intelligence and law enforcement agencies have made extensive efforts to infiltrate the Tor network and trace those who use it.

Many of the servers on the Tor network are run by volunteers. Mr. Meinrath said that if the F.B.I. explored the network, it was possible that investigators were not able to infiltrate enough servers on their own to trace the origin of the documents.

"Probably the F.B.I. had some of that information but not all of it," Mr. Meinrath said.

Another possibility, he said, was that the volunteer was not operating a server properly and kept information about the routes taken by the messages passing through it.

A skilled hacker, Mr. Meinrath said, would take into account all of these possibilities and add one or two additional layers of security to the communication -- for example, using software to cloak the identity of the computer that sent the message and connecting to the Internet somewhere that could not be linked to its source. Those measures seem to have eluded those who did the hacking.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Rue89 (site web)
Twitter, vendredi 21 mars 2014

# Twitter coupé en Turquie : trois façons simples de contourner la censure

**Gurvan Kristanadjaja**

La version turque du mode d'emploiGrâce à l'aide d'un traducteur, ce mode d'emploi est disponible en turc, à cette adresse. **Rue89**

Le Premier ministre Erdogan l'avait annoncé, il l'a fait. Jeudi soir, le gouvernement conservateur turc a fermé l'accès à Twitter depuis la Turquie pour « des raisons de sécurité ». Une mesure qui provoque le courroux des utilisateurs du réseau social, et des pays de l'Union européenne. La commissaire européenne en charge des Nouvelles technologies a tweeté :

**« L'interdiction de Twitter en Turquie est sans fondement, inutile et lâche. Les Turcs et la communauté internationale verront cela comme de la censure. C'en est. »**

The Twitter ban in #Turkey is groundless, pointless, cowardly. Turkish people and intl community will see this as censorship. It is.- Neelie Kroes (@NeelieKroesEU) March 20, 2014

Une censure symbolique certes, mais peu efficace en réalité au regard des moyens qui existent pour contourner une telle interdiction, développés par les communautés d'internautes confrontés aux censures chinoise et nord-coréenne.

Erdogan veut « éradiquer » Twitter en Turquie. Joli dessin via @klustout pic.twitter.com/QOUs6wsgLJ- pierrehaski (@pierrehaski) 21 Mars 2014

Si vous nous lisez depuis la Turquie, soyez rassurés : quand il y a deux ans encore, il aurait fallu être un utilisateur aguerri pour outrepasser cette prohibition, aujourd'hui trois clics suffisent.

1

Tor Browser

Tor (The Onion Router) est un réseau informatique mondial « parallèle ». De ce fait, il est utilisés par certains réseaux illégaux, mais sert aussi à contourner les censures.

Téléchargez le « Tor Browser » sur la page dédiée. C'est l'équivalent de Chrome, Firefox, Safari ou Internet Explorer, sauf qu'il est entièrement dédié à l'utilisation du réseau parallèle.

La page de téléchargement de Tor Browser

Installez le programme et exécutez-le, simplement. Utilisateurs de Mac, vous pourriez avoir un message notifiant « Impossible d'ouvrir Tor Browser ». Ne paniquez pas, faites un clic droit sur l'icône puis sélectionnez « ouvrir ».

Vous accédez à la fenêtre de paramètres du réseau Tor. Choisissez « se connecter ».

Paramètres de connexion de Tor Browser

Vous pouvez maintenant vous connecter à Twitter en utilisant la barre de navigation.

Attention néanmoins, si Tor permet d'accéder au réseau social, il ne garantit pas pour autant l'anonymat. Et soyez conscients que vous mettez vos données personnelles à disposition. Aller ailleurs que sur Twitter via Tor est à vos risques et périls.

2

VPN Gate

C'est un service qui permet de se connecter facilement à un réseau privé virtuel en Corée du Sud ou au Japon par exemple, et de contourner ainsi les interdiction en vigueur.

Accédez dans votre panneau de configuration au centre de réseau et de partage

Le centre de réseau et partage sous Windows

Choisissez « configurer une nouvelle connexion ou un nouveau réseau »

Configurer une nouvelle connexion

Sélectionnez ensuite « Connexion à votre espace de travail », puis « Utiliser ma connexion Internet (VPN) ».

Configurer ma connexion VPN

C'est à ce moment là que vous allez utiliser VPN Gate. Dans la colonne « MS-SSTP Windows Vista, 7, 8, RT No client required », copiez une des adresses disponibles (par exemple vpn747065236.opengw.net : 1956).

Les adresses VPN qui peuvent être utilisées

Entrez l'adresse choisie, avec pour destination « VPN Gate », pour nom d'utilisateur « vpn » et pour mot de passe « vpn ».

Les champs adresse et nom doivent être remplis

Ouvrez votre navigateur et rendez-vous sur Twitter. Vous êtes désormais connecté à une passerelle qui permet de contourner l'interdiction.

Comme sur Tor, soyez prudents.

3

Twitter par SMS

Pour ceux qui veulent accéder à Twitter via leurs téléphones et qui ne disposent pas d'une connexion internet, le réseau a rapidement mis en place un service pour tweeter par SMS. Sous Avea et Vodafone, envoyez « START » au 2444. Si vous disposez d'un réseau Turkcell, faites la même manipulation mais au 2555.

Turkish users : you can send Tweets using SMS. Avea and Vodafone text START to 2444. Turkcell text START to 2555.- Policy (@policy) March 20, 2014



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

LEFIGARO.fr

Le Figaro.fr
dimanche 13 décembre 2015 - 13:02 UTC +01:00

Tech & Web

# Twitter prévient ses utilisateurs lorsqu'un État veut espionner leur compte

**Ronfaut, Lucie**

**Au moins une quinzaine de personnes dans le monde ont été prévenues vendredi d'une intrusion venant potentiellement d'un gouvernement, dont deux comptes français.**

«Nous souhaitons vous informer que votre compte Twitter fait partie d'un petit groupe de comptes ayant peut-être fait l'objet d'un ciblage de la part d'agents commandités par un État.» C'est le message angoissant qu'ont reçu au moins des utilisateurs de Twitter vendredi soir. Pour la première fois, le réseau social a décidé d'informer par un mail des personnes qui auraient pu faire l'objet d'une attaque informatique de la part d'internautes associés à des gouvernements. «Nous pensons que ces agents ont éventuellement essayé d'obtenir certaines informations telles que des courriels, des adresses IP, et/ou des numéros de téléphone», précise Twitter. «À l'heure actuelle, nous n'avons pas de preuve qu'ils aient eu accès à vos données, mais nous poursuivons notre enquête.»

## Participants au projet Tor

On ignore combien de personnes ont été prévenues de cette intrusion, ou même si elles ont toutes été attaquées par le même État. Contacté par *Le Figaro*, Twitter n'a pas souhaité faire de commentaires. En France, au moins trois comptes ont affirmé avoir reçu ce mail. C'est le cas de @chiffrofete, une organisation qui organise des évènements autour de la cryptographie, et de l'un de ses fondateurs. Un autre utilisateur visé tweete régulièrement sur les libertés en ligne et utilise Tor, un réseau informatique qui permet de naviguer sur Internet de manière anonyme. Il indique néanmoins ne faire partie d'aucune organisation militante. «Pour le citoyen lambda que je suis et qui aspire à rester le plus anonyme possible, ce mail m'a un peu remué», a-t-il commenté.

À l'étranger, les profils des comptes ciblés sont similaires. Certaines personnes militent pour les libertés en ligne, font des recherches en sécurité informatique ou ou sont connectées au projet Tor. Ce dernier fait régulièrement l'objet de critiques de la part des autorités pour son utilisation supposée par des organisations criminelles. Le ministère de l'Intérieur aurait même envisagé de demander son interdiction dans le cadre de la lutte contre le terrorisme, d'après le journal *Le Monde* .Manuel Valls avait néanmoins affirmé que le gouvernement n'examinerait pas cette option. Twitter, lui, n'hésite pas à recommander l'utilisation de Tor à ses victimes d'une attaque étatique, afin de mieux protéger leur identité. Hasard du calendrier, le réseau social a envoyé ces avertissements le jour même de la nomination de la nouvelle directrice du Tor Project, Shari Steele.

C'est la première fois que Twitter prévient de telles attaques. Il rejoint dans cet effort Facebook, qui avait annoncé en octobre qu'il allait lui aussi prévenir ses utilisateurs dont le compte aurait été compromis par des agents «soutenus par un État». C'est aussi le cas de Google, qui le fait depuis 2012. Toutes ces entreprises collaborent par ailleurs régulièrement avec les autorités: il s'agit néanmoins de demandes spécifiques, prononcées dans le cadre d'enquêtes. Twitter, Facebook et Google communiquent tous sur le nombre de demandes d'informations qu'ils reçoivent de la part d'État, au travers de rapports de transparence.

**Voir aussi:**

http://www.lefigaro.fr/secteur/high-tech/2015/12/13/32001-20151213ARTFIG00052-twitter-previent-ses-utilisateurs-lorsqu-un-etat-veut-espionner-leur-compte.php

**Note(s) :**

Mise à jour : 2015-12-13 17:34 UTC +01:00

***PUBLI-Cnews·20151213·LFF·20151213ARTFIG00052*** *- Date d'émission : 2016-04-04*



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **5 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Point.fr
Le Point.fr
Société, dimanche 1 juin 2014

# Paris et Bruxelles pour un renforcement de la lutte européenne contre les djihadistes

## Source AFP

**Après la fusillade de Bruxelles, les Européens s'inquiètent du retour des jeunes djihadistes partis combattre en Syrie et veulent renforcer la lutte au niveau du continent.**

Le ministre de l'Intérieur Bernard Cazeneuve et son homologue belge Joëlle Milquet ont souhaité dimanche un renforcement de la surveillance européenne des candidats au djihad, notamment en Syrie, après l'arrestation du suspect de la tuerie du Musée juif de Bruxelles.

Si l'implication de Mehdi Nemmouche, un Français de 29 ans, se confirme, ce sera en Europe le "premier attentat commis par une personne qui aurait séjourné en Syrie", a déclaré Mme Milquet lors d'une déclaration commune avec son homologue français, qui l'avait invitée à Paris. Le suspect a en effet passé plus d'un an en Syrie en 2013-2014, vraisemblablement auprès de groupes djihadistes.

"Phénomène inquiétant"

La ministre belge a souligné le "phénomène (...) inquiétant pour l'ensemble de nos pays européens" des "ressortissants nationaux européens" qui "partent en Syrie et peuvent incarner une menace terroriste pour les pays dont ils sont issus". Un phénomène "qui prouve à quel point la mobilisation, les mesures qui ont été prises sont indispensables, doivent être renforcées et sont de véritables priorités", a-t-elle poursuivi, mettant l'accent sur la "prévention" et la "coopération entre nos différents services".

M. Cazeneuve a souligné que les ministres de l'UE chargés du secteur devaient évoquer ces questions mercredi et jeudi à Luxembourg, appelant à une "lutte sans merci face aux prêcheurs de haine et aux assassins fanatisés". Il a rappelé qu'il avait présenté fin avril un plan pour "accentuer la détection et la surveillance" des candidats au djihad, visant à endiguer la hausse de départs.

**Étendre les mesures à l'espace Schengen**

"Je souhaite à très brève échéance faire voter les mesures législatives indispensables à un meilleur contrôle des candidats au djihad sur le territoire national", a-t-il réaffirmé, avec le souhait de voir "étendre ces mesures à l'ensemble de l'espace Schengen".

Il a affiché une "détermination sans faille à combattre ensemble avec nos partenaires de l'UE et hors de l'Union ces nouvelles formes de terrorisme insidieuses, diffuses et d'autant plus dangereuses qu'elles ne sont pas facilement détectables".

M. Cazeneuve a ainsi souligné le "défi considérable" de la propagande djihadiste sur internet et dit porter une "attention particulière au discours de prosélytisme en milieu carcéral". Selon le procureur de Paris, Mehdi Nemmouche, délinquant multirécidiviste, s'était radicalisé lors de son dernier séjour en prison.



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

La Recherche
La Recherche, no. 505
fondamentaux, dimanche 1 novembre 2015, p. 61

Numérique

# Les failles de la loi sur le renseignement

**Claude Castelluccia et Daniel Le Métayer**

**Les attentats de janvier ont intensifié la nécessité de détecter les terroristes potentiels. Mais les mesures prévues par la récente loi sur le renseignement risquent de conduire à suspecter des citoyens innocents.**

« Renforcer la lutte contre le terrorisme en dotant les services de renseignement de capacités d'action accrues », tel est l'objectif de la loi sur le renseignement élaborée à la suite des attentats de janvier dernier et votée en juin. Cette loi repose avant tout sur la collecte d'informations sur Internet puisque le réseau mondial est considéré comme un vecteur essentiel de l'embrigadement extrémiste.

Si le besoin d'un encadrement juridique des activités de renseignement n'est guère contesté, le périmètre de la loi (en réalité bien plus large que la lutte contre le terrorisme) ainsi que nombre de ses dispositions font l'objet de sévères critiques. Un article propose notamment un changement radical de modèle : il entérine le passage d'une surveillance ciblée à une surveillance de masse. Concrètement, cela signifie qu'à l'avenir, il ne s'agit plus seulement de confirmer ou d'infirmer les soupçons qui pèsent sur une personne mais de faire émerger des suspects en analysant les comportements de tout un chacun. Pour reprendre un exemple abondamment cité par les défenseurs du projet de loi, l'analyse des connexions à un site hébergeant une vidéo de décapitation permettra de désigner des suspects potentiels. Le principe général consiste donc à pointer des personnes correspondant à des profils particuliers liés à leurs relations sociales, leurs comportements ou leurs centres d'intérêt. Cette surveillance de masse soulève des questions de fond.

Le premier écueil concerne les libertés individuelles et la protection de la vie privée. En effet, afin d'identifier de potentiels suspects, la loi autorise la collecte des données de connexion des internautes ou des données techniques, également appelées métadonnées. Il ne s'agit pas des contenus eux-mêmes, mais des informations contextuelles : dates, heures, lieux, durées des communications.

Ces métadonnées sont les données de surveillance par excellence et leur collecte s'apparente à l'action du détective à la recherche d'indices sur les rencontres entre personnes, les lieux fréquentés, les parcours... Par exemple, il est plus instructif de savoir qu'un appel téléphonique est destiné au bureau des alcooliques anonymes (les métadonnées) que d'écouter la conversation de prise de rendez-vous correspondant à cet appel (les données).

Très utilisées par les publicitaires pour catégoriser les internautes, ces métadonnées peuvent donc être très intrusives, parfois plus que les données elles-mêmes. Ainsi, c'est à partir de l'analyse de métadonnées que la liaison de l'ex-directeur de la CIA David Petraeus a été découverte. Plus précisément, il a pu être établi que différentes connexions à un compte de messagerie avaient été effectuées via les réseaux wifi d'hôtels à partir de chambres dont l'occupante s'est avérée être la maîtresse de Petraeus !

Plus globalement, la nouvelle loi autorise l'analyse des métadonnées collectées en masse, afin d'identifier des terroristes potentiels à partir des « signaux de faible intensité ». Ces signaux correspondent, par exemple, au fait d'accéder à des sites web suspects ou de regarder un type de vidéos. Mais en analysant des métadonnées aussi riches que la liste des sites visités par un utilisateur, on peut aussi en inférer ses centres d'intérêt ou son orientation politique. Pour déterminer si un individu est suspect ou pas, l'analyse va vraisemblablement reposer sur des algorithmes de classification binaire. Comme leur nom l'indique, ils permettent de classifier un ensemble de points en deux catégories à partir de critères et de modèles, qui sont soit spécifiés par le programmeur, soit automatiquement découverts par

l'algorithme dans une phase d'apprentissage à partir de données existantes. Or, pour être efficaces, ces algorithmes nécessitent d'être entraînés sur une quantité importante de données (mais dont le nombre varie en fonction des cas) ou d'avoir défini des modèles, c'est-à-dire des profils types de suspects, précis et distinctifs. Le problème, c'est qu'il existe très peu de données disponibles sur les « profils internet » de terroristes. Ont-ils des comportements vraiment différents des autres utilisateurs ? Et si tel est le cas, est-il possible de définir des profils ? Cela reste à démontrer et ce point est loin de faire l'unanimité **(1)**. Par ailleurs, cette collecte systématique et automatique de métadonnées peut être source de discriminations. Nous pourrions assister par exemple à une multiplication du nombre de personnes interdites de vol sur des bases infondées (et opaques) simplement parce qu'un système informatique l'aura décidé.

**PARADOXE DES FAUX POSITIFS**

Deuxième point, la surveillance de masse peut se révéler très inefficace dans la lutte contre le terrorisme. Car même si l'on arrivait à établir des profils précis, le nombre d'erreurs, c'est-à-dire d'innocents suspectés à tort, serait considérable ! En effet, dès lors que l'événement à identifier est rare - ce qui est le cas ici puisqu'il s'agit de retrouver quelques milliers de personnes dans une population de plusieurs millions d'individus -surgit le « paradoxe des faux positifs » **(2)**. Le phénomène est bien connu des mathématiciens. Pour l'expliquer, il faut savoir que les performances d'un algorithme de classification binaire sont caractérisées par deux paramètres calculés indépendamment : le taux de vrais positifs ou d'identifications correctes (la probabilité qu'un terroriste soit effectivement détecté comme terroriste par le système), et le taux de faux positifs ou d'identifications incorrectes (la probabilité qu'un innocent soit détecté comme terroriste).

Considérons un algorithme de classification binaire présentant un taux de vrais positifs de 99 % et un taux de faux positifs de 0,5 %, qui serait utilisé pour identifier 3 000 terroristes potentiels parmi 30 millions de personnes. Cet algorithme détecterait correctement 3 000 x 0,99 = 2 970 terroristes, mais ferait environ (30 000 000 - 3 000) x 0,5/100 = 149 985 erreurs ! 150 000 innocents en moyenne seraient donc suspectés à tort. En d'autres termes, un individu identifié comme terroriste par notre système n'aurait qu'une probabilité de 1,9 % [2 970/(2 970+149 985)] d'être réellement un terroriste, malgré un algorithme très performant !

Troisième problème inhérent à cette surveillance de masse, le contournement. En clair, qui veut éviter de se faire repérer peut contourner le système à l'aide de connexions chiffrées. Le jeu consiste à chiffrer toutes ses communications avec un logiciel gratuit, à télécharger légalement, par exemple PGP (Pretty Good Privacy, « assez bonne intimité »). Ce système de chiffrement à clé publique repose sur l'utilisation d'une double clé, l'une publique pour le chiffrement et largement diffusée, l'autre privée pour le déchiffrement et donc confidentielle. En résumé, celui qui ne dispose pas de la clé privée ne peut accéder qu'à du bruit. Pour contourner le système, une autre parade consiste à passer par un réseau dit « d'anonymisation », comme TOR (lire p. 65), où l'anonymat est la règle, et qui protège contre l'analyse des métadonnées.

Dans tous les cas, ces contournements techniques sont faciles à mettre en oeuvre et la seule information exploitable serait l'établissement d'une connexion chiffrée entre une machine et un ou plusieurs serveurs (en France ou à l'étranger). En particulier, aucune information sur le destinataire final de l'information ou le contenu du message ne serait exploitable. Il y a fort à parier que nombre de terroristes utilisent ou utiliseront ces techniques de contournement, ce qui aura comme conséquence de diminuer considérablement le taux de vrais positifs défini précédemment, et donc les performances du système de détection.

Que peut faire la technique pour réduire les dangers posés par ces systèmes de détection ? La loi ne précise pas les moyens qui seront mis en place pour réaliser l'analyse de trafic, ni qui va s'en charger. Par exemple, une cellule dépendant du ministère de l'Intérieur ou un sous-traitant privé.

Une première mesure de précaution consisterait à éviter la centralisation des données collectées par le système. La centralisation est généralement vue comme une faiblesse en sécurité informatique car elle introduit un point de vulnérabilité unique. En d'autres termes, un acteur malveillant capable de casser la sécurité du site aura accès à la totalité des données. Par ailleurs, il est préférable de séparer les données collectées par différents organismes pour des buts distincts. Par exemple, les données

collectées pour lutter contre le terrorisme ne devraient pas être utilisées pour détecter la fraude aux allocations familiales.

## CONFIDENTIALITÉ DES DONNÉES

De manière générale, toute donnée personnelle doit être stockée de façon chiffrée et leur accès doit être contrôlé. On peut aller plus loin en assurant dans certains cas la protection des données, aussi pendant les calculs. On citera par exemple le chiffrement homomorphe, qui permet d'effectuer des calculs sur les données chiffrées sans avoir besoin de les déchiffrer. Par exemple, si on note CK l'algorithme de chiffrement avec une clé K et DK l'algorithme de déchiffrement correspondant, si DK (CK ( n ) x CK ( m )) = n x m , on pourra dire que le schéma de chiffrement est homomorphe pour la multiplication. En d'autres termes, il est possible de calculer le produit sur les valeurs chiffrées elles-mêmes. De ce fait, la confidentialité des valeurs à protéger (ici n et m ) peut être préservée vis-à-vis de l'agent réalisant le calcul (ici la multiplication). On notera cependant que, même s'il est applicable en théorie à tout calcul, le principe du chiffrement homomorphe ne peut actuellement être effectué avec des temps de calcul raisonnables que pour certaines opérations (comme la multiplication ci-dessus).

L'utilisation des données de renseignement pose aussi des questions complexes en matière de contrôle d'accès. Tout d'abord, les règles d'utilisation des données ne sont pas de simples associations entre types de données et agents autorisés. De façon plus subtile, on peut vouloir exprimer, par exemple, le fait qu'un agent de renseignement d'un service donné peut utiliser les coordonnées téléphoniques des personnes avec qui un suspect désigné est entré en contact pendant les trois derniers mois (et peut-être aussi les contacts de ses contacts, etc.). En d'autres termes, mener son enquête ne doit pas lui permettre d'accéder à la totalité de la base de données du service mais uniquement à la partie en rapport avec son enquête. On peut aussi vouloir restreindre l'accès à certaines finalités et dans certaines conditions (par exemple avec l'autorisation d'un supérieur et à des fins de recherche de complicités d'acte de terrorisme).

Dans ces conditions, la difficulté consiste à exprimer des règles qui traduisent des obligations juridiques ou réglementaires, dans un langage qui soit à la fois traitable par une machine et compréhensible par des humains. Quand un tel langage est muni d'une sémantique claire (par exemple sur la base d'un modèle mathématique) il présente l'avantage de lever toute ambiguïté sur le sens des règles à appliquer, concernant notamment l'obligation d'effacement des données ou les autorisations d'accès **(3)**.

Reste le contrôle a posteriori, une forme de contrôle essentielle en matière de renseignement, qui relève de l'audit. Il peut consister par exemple à vérifier, après les faits, que les traitements effectués sur les données personnelles sont conformes aux exigences légales et réglementaires. Ces vérifications pourraient être largement automatisées à l'aide d'analyseurs de logs **(Fig. 1)**. Les logs sont les fichiers informatiques qui stockent l'historique des événements du système. Les analyseurs sont eux-mêmes des logiciels qui intègrent les règles à vérifier et parcourent les fichiers logs pour déterminer si ces règles ont été respectées, fournissant ainsi une aide précieuse aux auditeurs. Cependant, pour que ce type de contrôle soit probant, il faut que tous les moyens soient mis en oeuvre pour assurer la sincérité et la sécurité des logs : il est crucial en effet que ceux-ci reflètent l'ensemble des opérations pertinentes sur les données et qu'ils ne puissent être altérés (par exemple pour masquer des activités non conformes).

Il va de soi que la confidentialité de ces logs doit également être préservée, faute de quoi ceux-ci pourraient représenter un risque accru de divulgation de données personnelles. Ces contrôles a posteriori ne peuvent pas, par définition, apporter de garantie absolue. Ils relèvent de ce qu'on appelle parfois l' accountability, c'est-à-dire la responsabilisation, le mot accountability étant à prendre au sens de « rendre des comptes ». En d'autres termes, il s'agit d'une démarche de surveillance des surveillants, nécessaire pour assurer aux citoyens que les pouvoirs accordés aux services en matière de collecte et de traitement de données personnelles ne sont pas dévoyés.

## UN CONTRE-POUVOIR INDÉPENDANT

Cependant, les défis en la matière ne sont pas seulement techniques. Ce contrôle devrait être effectué par une entité véritablement indépendante, disposant des moyens suffisants, tant sur le plan financier qu'en matière d'expertise technique. On peut donc regretter que la Commission nationale de contrôle des techniques de

renseignement prévue par la loi sur le renseignement n'apporte pas les garanties suffisantes, notamment en matière d'expertise technique (une seule personnalité qualifiée parmi les neuf membres de la commission). Cette commission devra donner son avis avant toute autorisation de mise en oeuvre d'une technique de renseignement. Elle sera aussi informée de leurs modalités d'exécution et disposera des transcriptions des renseignements collectés de façon à pouvoir vérifier leur « caractère nécessaire et proportionné » .

Même si les recherches doivent être amplifiées sur ces sujets **(4)**, les techniques existantes peuvent déjà contribuer à concilier renseignement et protection de la vie privée dans le cadre d'une démarche d' accountability qui accorderait de véritables contre-pouvoirs à une entité tierce indépendante. Cette démarche inspire également le futur règlement européen sur les données personnelles, réforme globale des règles adoptées par l'Union européenne en 1995 en matière de protection des données personnelles, et qui devrait être adopté définitivement en 2015. Cependant, ce règlement ne concerne pas les activités de police et de justice qui seront régies par une directive spécifique. Idéalement, ce principe d' accountability, qui pourrait contribuer à renforcer la confiance des citoyens, devrait s'imposer à tous les acteurs, privés comme publics, qui traitent des données personnelles, la surveillance par des sociétés privées méritant tout autant d'attention que la surveillance d'État.

**N.B. :** Cet article reflète exclusivement l'opinion de ses auteurs et n'engage en aucune façon Inria.

**Encadré(s) :**

**Repères**

**Votée à la suite des attentats contre l'hebdomadaire Charlie Hebdo et l'Hyper Cacher porte de Vincennes, début 2015, la loi sur le renseignement valide le principe d'une surveillance de masse par l'analyse des métadonnées.**

**Les algorithmes programmés à cet effet risquent d'identifier comme suspects nombre d'innocents.**

**Pour le moins, des mesures devraient être prises pour mieux contrôler les usages des données par les services de renseignement.**

**TOR, UN LOGICIEL POUR ÉCHAPPER À LA SURVEILLANCE**

**TOR, qui peut être téléchargé librement (www.torproject.org), est un logiciel qui permet d'anonymiser les communications sur Internet. Avec lui, un utilisateur peut se connecter sur un site sans révéler au site ou à un observateur du réseau son adresse IP. TOR protège ainsi de la surveillance grâce aux fameuses « boîtes noires ». Il utilise un routage décentralisé qui repose sur des relais intermédiaires déployés par des volontaires à travers le monde. Chaque message est transporté par trois relais distincts, R1, R2 et R3, choisis par le système. Chaque message est ainsi chiffré trois fois successivement et donc enveloppé de trois couches de chiffrement, un peu comme un oignon (d'où le nom TOR pour The Onion Router). Le déchiffrement du message est également réalisé en trois étapes successives, par les trois relais, pour être envoyé au destinataire final. Aucun observateur ne peut identifier la source et la destination d'une connexion. Néanmoins, TOR ne cache pas forcément le contenu des communications. C'est un simple transporteur d'information au sens de l'article 12 de la directive européenne 2000/31/CE du 8 juin 2000. Comme La Poste, il n'est pas responsable des informations qu'il transporte.**

**Note(s) :**

Claude Castelluccia et Daniel Le Métayer, directeurs de recherche chez Inria

**(1)** Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique de l'Assemblée nationale, « Recommandation sur le projet de loi relatif au renseignement », 1er avril 2015.

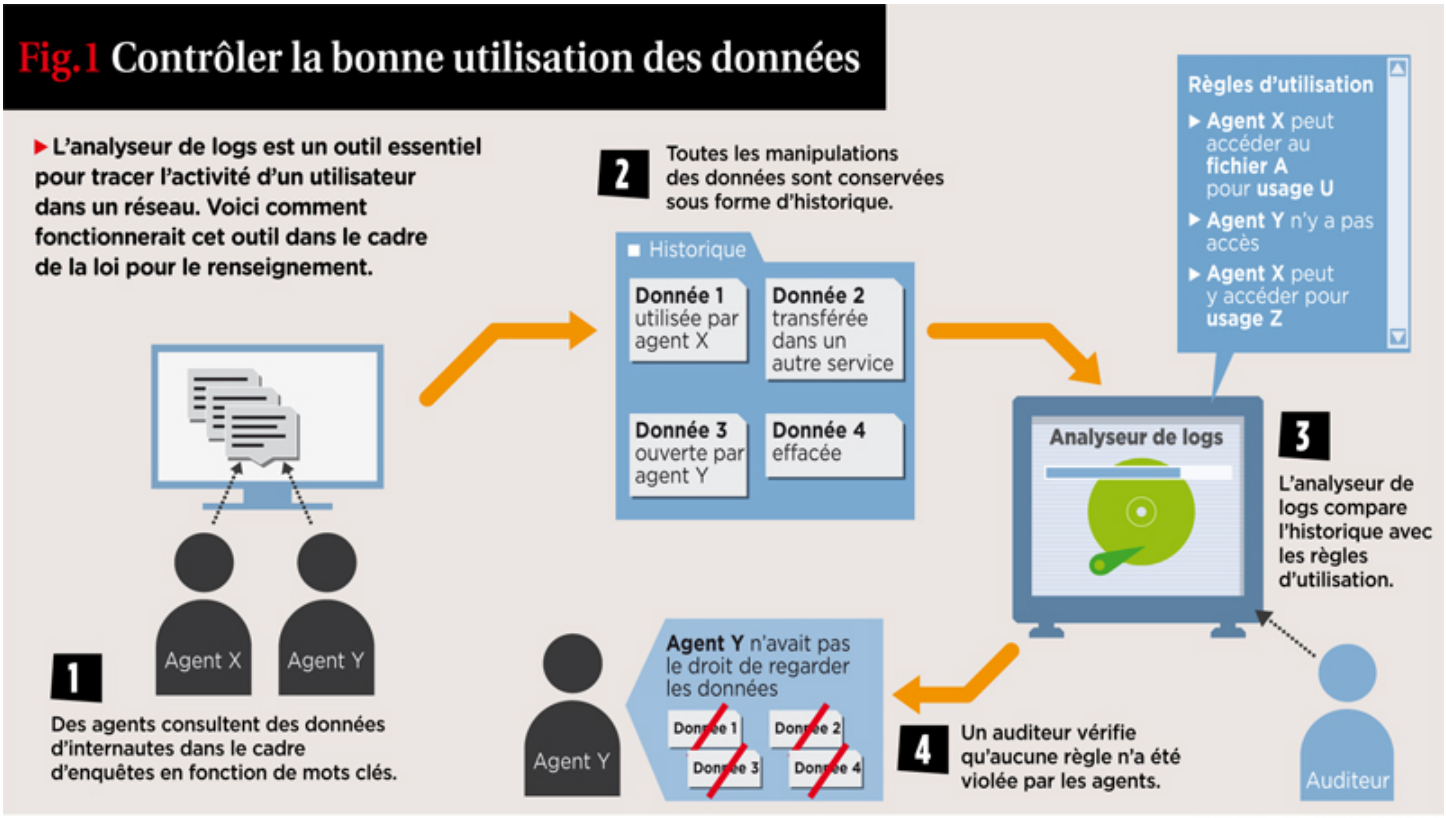
**(2)** J. Parra-Arnau, C. Castelluccia. « Dataveillance and the False-Positive Paradox », HAL, mai 2015.

**(3)** D. Butin, D. Le Métayer, « Log Analysis for Data Protection Accountability », *Formal Methods, LNCS 8442*, 63, Springer, 2014.

**(4)** National Research Council of the National Academies, « Bulk collection of signals intelligence : technical options », The National Academies Press, 2015.

http://tinyurl.com/homelandsecuritynewswire « Terrorists' personality traits indistinguishable from traits of the general population: Experts »

**Illustration(s) :**






**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

La Tribune (France), no. 5693
Territoires, mardi 21 avril 2015, p. 100

Opinions

# Pourquoi la loi sur le renseignement pourrait renforcer le terrorisme

**Acteurs de l'économie**

**Au-delà de l'inefficacité du système des "boîtes noires" démontrée par les chercheurs en informatique, l'effet de cette surveillance généralisée risque d'être le contraire que celui escompté. Car pour contourner cet éventuel dispositif législatif, des outils existent déjà. L'auteur, un expert en sécurité informatique, a souhaité resté anonyme.**

Le projet de loi sur le renseignement est en cours d'examen à l'Assemblée nationale en procédure accélérée. Il est actuellement très médiatisé par les technophiles, défenseurs de la vie privée et de nombreux organismes (ONU, Amnesty International, RSF, la LDH, syndicat de la magistrature, etc).

L'un des points les plus critiqués est l'article deux qui consiste à mettre en place des "boîtes noires" chez les opérateurs (Orange, Free, Numéricable/SFR ...) et hébergeurs (qui hébergent les sites web) afin de pouvoir surveiller tout le trafic transitant par l'Internet français. Le contenu des communications ne serait pas surveillé, mais uniquement les métadonnées : origine ou destinataire d'un message, adresse IP d'un site visité et de son visiteur, etc.

**Des données noyées**

D'après le gouvernement, ce dispositif servirait uniquement à détecter les projets d'actions terroristes grâce à de puissants algorithmes. Deux éléments montrent que les arguments avancés par le gouvernement manquent d'expertise technique.

L'inefficacité d'un tel système a été démontrée par les chercheurs en informatique. En effet, il n'y a pas d'algorithme magique qui permette de repérer facilement les comportements qui pourraient présager la préparation d'un attentat terroriste. De plus, un algorithme, aussi performant soit-il, donnerait en résultat une quantité très importante de faux-positif. Ainsi les données recherchées se retrouveraient comme une goutte dans l'océan, noyées dans un flot de données. Cependant, tout défenseur du texte de loi indiquera que cet argument est aussi incertain que le sera l'efficacité de ces "boîtes noires" : tant qu'on ne les a pas essayées, on ne peut pas le vérifier.

**Des terroristes plus vigilants....**

Mais le second élément est beaucoup plus pertinent. L'effet de la surveillance généralisée risque d'être le contraire que celui escompté. Jusqu'à présent, un apprenti terroriste savait qu'il avait peu de chances d'être surveillé, et ne faisait pas forcément attention à protéger ses échanges sur Internet.

Si ces "boîtes noires" étaient bien mises en place, tout le monde serait surveillé, terroriste compris. Ainsi ces derniers, sachant que leurs échanges les feraient potentiellement repérer, feraient en sorte de protéger leurs communications. Et pour ceci rien de plus simple, les outils existent déjà.

**...avec des outils déjà disponibles**

A la base, ces outils n'ont pas été développés dans un but terroriste ou illicite, mais pour préserver les libertés individuelles de chacun et notamment des journalistes et dissidents politiques en disgrâce dans leurs pays, comme en Chine, anciennement en Libye, en Syrie, et tant d'autres. Les lanceurs d'alertes tels qu'Edward Snowden, Mickael Manning, Julian Assange, qui nous informent sur les pratiques des gouvernements, les utilisent pour se protéger.

Parmi ces outils, on retrouve le réseau Tor. Il permet de sortir par différents noeuds du réseau et de protéger son identité. Pour l'utiliser, rien de plus simple. Vous téléchargez un système gratuit, puis vous l'installez sur une clé USB avant de démarrer votre ordinateur avec. Le réseau Tor a cependant deux inconvénients : il est plus lent que le réseau Internet classique et le fait d'utiliser ce système est repérable (on ne sait pas ce que vous y faites, mais on sait que vous l'utilisez). Ainsi, les "boîtes noires" pourraient catégoriser chaque utilisateur de Tor comme terroriste.

**L'arroseur arrosé**

L'autre moyen est de souscrire à un service VPN (Virtual Private Network, de l'anglais réseau privé virtuel). Ce service vous permet de vous connecter à un serveur et de sortir sur Internet depuis celui-ci. Ainsi, il suffit à un individu de souscrire à un de ces services à l'étranger (il en existe des dizaines pour quelques euros par mois) et les fameuses "boîtes noires" ne verraient qu'un trafic chiffré entre la connexion Internet de l'utilisateur et le serveur à l'étranger. Ce trafic se retrouve noyé dans la masse de trafic, également chiffré, comme il en existe une quantité considérable. En effet depuis peu, vos échanges avec Google et Facebook sont chiffrés d'office.

Ainsi les échanges tant recherchés par les fameuses "boîtes noires" seraient hors de portée, car leur point de sortie serait un serveur hors de France. C'est l'arroseur arrosé...

**Illustration(s) :**


reuters.com

***PUBLI-Cnews·20150421·TR·908984*** *- Date d'émission : 2016-04-07*



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Le Monde.fr
Le Monde.fr
jeudi 15 août 2013

# Bitcoin, BitTorrent, TOR : un Internet décentralisé pour des usages centralisés ?

**20130814**

20130814

The Pirate Bay a dix ans, et certains des fondateurs du site voudraient le voir fermer. L'annuaire de fichiers, qui se veut le plus gros site mondial d'indexation de contenus et de partage libre de films, de jeux, de séries TV et de musiques sur Internet, est devenu l'un des principaux carrefours du réseau BitTorrent. Devenu indispensable à nombre d'utilisateurs, il catalyse l'ire des ayants droit dont il participe à distribuer les oeuvres.

Pour quatre de ses créateurs, interrogés par le site spécialisé TorrentFreak , le service empêche le partage de fichiers d'évoluer, en étant justement devenu un symbole de la bataille contre les ayants droit. Pour eux, The Pirate Bay devrait laisser sa place à un système décentralisé, impossible à détruire, alors qu'il s'appuie lui-même sur un réseau de partage sans centre : BitTorrent.

Plusieurs autres réseaux Internet se sont développés autour de la décentralisation : l'échange de fichiers d'internaute à internaute sur BitTorrent, l'échange sécurisé d'argent par bitcoin ou la navigation anonyme par le réseau TOR. Pourtant, tous ces systèmes sont attaqués depuis plusieurs mois par la suppression de sites et de maillons devenus centraux : annuaires BitTorrent, points d'échange de monnaie bitcoin ou maillons TOR connus. Quand la protection de réseaux décentralisés, en théorie invulnérables, rencontre l'habitude des utilisateurs de concentrer leurs activités.

Jeudi 8 août, le service de mails sécurisés Lavabit a fermé ses portes , pour éviter de confier ses données aux services de renseignement américains. Le lanceur d'alerte à l'origine des révélations sur la surveillance américaine, Edward Snowden, aurait ainsi utilisé ce service, comme 350 000 autres personnes. Répondre à une requête des autorités pour un utilisateur aurait sûrement compromis la sécurité des données de l'ensemble des membres, qui ont perdu leur service de messagerie sans préavis. Le lendemain, c'était le service concurrent Silent Mail de Silent Circle qui fermait ses portes.

## UN SURF ANONYME, GRÂCE À DES POINTS IDENTIFIÉS

Quelques jours auparavant, le système de navigation anonyme TOR perdait son principal hébergeur de sites. Avec TOR, la connexion de l'internaute passe par un réseau sécurisé et ressort par l'un des milliers de "noeuds" qui le composent et gèrent les connexions. Pour les sites Internet consultés, seul le noeud utilisé apparaît, et non l'utilisateur. Ce réseau permet aussi d'accéder à des sites normalement inatteignables, dont l'adresse finit en .onion. Au-delà de contenus et services classiques, ces sites contiennent des sites spécialisés dans la pédopornographie ou la vente de drogue et d'armes. Début août, Freedom Hosting, le premier hébergeur de sites .onion, a été mis hors-ligne. Son fondateur a été arrêté et les sites hébergés distribuent désormais silencieusement un logiciel destiné à identifier les utilisateurs. Pour certains spécialistes dans la sécurité, cette action est l'oeuvre du FBI, qui a exploité la concentration de ces sites dans les mains d'une seule entreprise, qui avait leur confiance.

**<< Lire : "Les techniques pirates exploitées par le FBI pour surveiller les criminels"**

Mais TOR n'est pas utilisé que par les criminels : ce réseau est l'un des meilleurs moyens de contourner la censure d'Internet dans certains pays. Il est virtuellement impossible pour un Etat de cibler une entreprise ou un point d'Internet à bloquer, d'autres prenant automatiquement le relais. Ce n'est pas le cas des réseaux privés virtuels (VPN), souvent gérés par des entreprises, qui permettent aussi d'accéder anonymement à des sites normalement bloqués. Plusieurs pays, dont la Chine , bloquent ces réseaux privés ou s'assurent de pouvoir les surveiller. Malgré son indépendance, TOR n'est pas à l'abri des blocages : la grande majorité des "noeuds" (plus de 3 400) qui font le pont entre l'Internet classique et le réseau anonyme sont répertoriés, donc identifiables et blocables par les autorités. La police japonaise, notamment, souhaite interdire l'accès à TOR à cause de son usage par des criminels... qui pourraient tout de

même s'appuyer sur le millier d'autres "noeuds" non répertoriés restants.

## ÉCHANGES ENTRE INTERNAUTES ET RECHERCHES CENTRALISÉES

Sans possibilité de cibler les utilisateurs de ces réseaux eux-mêmes, le plus simple est d'attaquer ce qui les regroupe. Sur le réseau pair-à-pair BitTorrent, les points faibles sont les annuaires et moteurs de recherche comme The Pirate Bay et IsoHunt, étapes habituelles pour tout utilisateur souhaitant télécharger des contenus détenus par d'autres utilisateurs. Si chaque internaute peut directement fournir un fichier à un autre, l'habitude de passer par un moteur de recherche s'est très vite installée, rendant ces sites indispensables.

Les administrateurs de The Pirate Bay ont ainsi affaire à la justice de plusieurs pays, notamment leur Suède natale, pour le manque à gagner clamé par les ayants droit des oeuvres partagées. Depuis 2012, ils multiplient les actions pour rendre leurs utilisateurs moins dépendants de leur service, qui est lui-même travaillé pour être facilement transportable d'un prestataire technique à un autre ou d'un pays à un autre. Pour Tobias Andersson, l'un de ses fondateurs, le navire devrait s'autosaborder , afin de laisser place à une solution réellement décentralisée. Pendant ce temps, le moteur de recherche spécialisé IsoHunt fournit une version filtrée aux Etats-Unis et est menacé de fermeture, son fondateur enchaînant les défaites judiciaires face aux ayants droit depuis plusieurs années.

**<< Lire : "'TPB : AFK', The Pirate Bay sous les projecteurs"**

Les sites, des points connus, sont également sujets à des blocages dans plusieurs Etats, dont le Royaume-Uni , qui a pris soin de filtrer également les outils de contournement (comme les réseaux privés virtuels) destinés à y accéder. Le partage de fichiers en lui-même, quant à lui, reste possible, mais devient bien moins pratique. La suppression de ces sites pourrait bouleverser les habitudes des internautes, pour lesquels ils sont synonymes du réseau de partage.

## DES POINTS D'ÉCHANGE DE MONNAIES VIRTUELLES FRAGILES

D'autres points centraux, financiers ceux-là, ont connu un début d'année 2013 difficile. Liberty Reserve était une plateforme de blanchiment d'argent destinée aux criminels, démantelée fin mai. Le site, grâce à sa propre monnaie virtuelle, aurait blanchi plus de 6 milliards de dollars en sept ans. Cette monnaie était échangeable avec des devises classiques et d'autres monnaies virtuelles, comme le bitcoin. Bitcoin est à la fois une monnaie et un réseau sécurisé, qui gère la production et l'échange de cette monnaie. Toutes les transactions sont chiffrées et stockées par l'ensemble des utilisateurs, qui gagnent des bitcoins en sécurisant automatiquement les transactions des autres internautes. La monnaie est utilisée pour toutes sortes d'activités, plus ou moins légales.

Si deux internautes peuvent s'échanger des bitcoins seuls, des points d'échange se sont constitués, notamment pour permettre l'échange avec des monnaies classiques, comme le dollar ou l'euro. Si Liberty Reserve était explicitement destiné au blanchiment d'argent, d'autres se veulent plus neutres. Mt Gox, l'un des principaux acteurs de l'échange de "bitcoin", a perdu à la mi-mai sa capacité d'échanger la monnaie virtuelle avec les monnaies classiques après que la police fédérale américaine a bloqué son compte sur la plateforme de change Dwolla. Le point d'échange est accusé d'avoir permis le blanchiment d'argent et le paiement de drogues.

Tor, BitTorrent, bitcoin, mais aussi Google ou Facebook : sur Internet, la perte d'un maillon n'empêche pas le fonctionnement des autres. Il existe pourtant des maillons qui ont acquis plus d'importance que d'autres : les moteurs de recherche, réseaux sociaux ou des magasins comme Amazon. Ces services sont devenus centraux dans les usages des internautes et dans la vie de nombreux autres sites. Cette habitude de concentrer les activités peut aisément se retourner contre les utilisateurs... qui en sont devenus dépendants.

**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

# table des matières

Libération
Futurs, mardi 22 septembre 2015, p. 20

Interview

# Cyberattaques: «Beaucoup de pays se font passer pour des Chinois»

## Bernard Barbier, ex-directeur technique du renseignement extérieur français, raconte la guerre qui se joue dans l'ombre entre Etats.

**Pierre-Olivier FRANÇOIS; Jean-Marc Manach; Recueilli par Pierre-Olivier François avec Jean-Marc Manach**

Sa parole publique est rare, Bernard Barbier est habitué au secret : pendant quinze ans, il a travaillé pour le service de renseignement extérieur français, la DGSE, dont il a dirigé la division technique, «les grandes oreilles». De ce poste clé, il a assisté (et pris part) à la militarisation croissante du cyberespace et à la mise en place de systèmes de collecte massive de données. Passé dans le privé en 2014, il a accepté de s'exprimer dans le documentaire *Cyberguerre, l'arme fatale ?* diffusé ce soir sur France 2. *Libération* publie la version longue de cet entretien.

Quand avez-vous pris conscience que la cyberguerre allait avoir de l'importance ?

J'étais directeur technique à la Direction générale de la sécurité extérieure (DGSE), l'équivalent de l'Agence nationale de sécurité (NSA) aux Etats-Unis. J'avais donc la responsabilité de tout le système d'écoute français, mais aussi de la cyberoffensive. Après la première guerre du Golfe, où la France s'est retrouvée totalement dépendante du renseignement américain, Michel Rocard et Pierre Joxe ont décidé de doter la France d'outils de renseignement forts. La direction technique de la DGSE a donc monté des équipes de cyberguerre en 1990-1991, quand on a eu la capacité de casser les mots de passe pour pouvoir accéder aux informations contenues dans les ordinateurs.

Jusqu'en 2007, l'objectif était de faire de l'espionnage, d'aller voler des informations. Traditionnellement, les services écoutaient les satellites : c'est assez simple à écouter. Avec le déploiement des réseaux en fibre optique, à partir des années 2000, c'est devenu beaucoup plus difficile : il fallait pouvoir être soi-même sur le chemin du réseau. Par contre, c'était beaucoup plus simple d'aller chercher l'information dans les *data centers*, sur les serveurs : au lieu d'écouter l'information qui circule sur un tuyau, on allait chercher l'information directement dans les ordinateurs (1).

A partir de 2007, on est passé du cyberespionnage à la cyberguerre. On s'est rendu compte que cette capacité pouvait avoir un vrai effet dans un conflit moderne, et qu'on avait les moyens de provoquer des dégâts chez l'adversaire. Le premier événement étatique important en la matière fut l'attaque lancée par des hackeurs russes qui, avec des moyens à très faibles coûts, ont quasiment bloqué un Etat, l'Estonie, en 2007. On n'était pas à proprement parler dans un conflit traditionnel, puisqu'il n'y avait pas de bombardements, pas de morts, et que les dégâts n'étaient que virtuels. Mais cette attaque introduisait une nouvelle dimension, un changement profond, un moyen d'action qui n'existait pas : une forme d'avant-guerre qu'un Etat peut ne pas revendiquer, puisque dans le domaine cyber, la détection de l'auteur d'une attaque est extrêmement complexe.

Pourquoi est-il aussi difficile d'identifier les auteurs d'une cyberattaque ?

Le fait qu'il soit quasiment impossible de savoir qui vous attaque reste l'un des gros problèmes. Mais c'est également un outil intéressant puisque cela permet d'attaquer un pays sans être identifié. Comment identifier et détecter l'attaquant puisque, pour attaquer, vous rebondissez sur des serveurs-relais qui sont partout dans le monde, des systèmes de type TOR, et que le serveur qui vous attaque a en général été hacké ? C'est devenu quelque chose de presque normal, et beaucoup de pays ont développé ou acquis des capacités de cyberattaque, d'autant que ces virus que les pays développent, vous pouvez les récupérer, les analyser et les réutiliser pour attaquer un autre pays. A ce titre, les Chinois ont bon dos : beaucoup de pays se font passer pour des Chinois !

Comment la France s'est-elle lancée dans cette nouvelle forme de guerre ?

A l'occasion du «livre blanc» sur la défense et la sécurité nationale, en 2007-2008, on a commencé à réfléchir à ce type d'armes informatiques. Et j'ai prévenu les militaires qu'on ne pouvait pas les comparer aux armes classiques. Traditionnellement, vous développez une arme, vous formez des militaires et vous l'utilisez pendant quarante ans. Là, on n'est pas du tout dans ce concept, parce que ces armes ont une action limitée dans le temps puisque l'adversaire peut les récupérer, les comprendre, les analyser, les réutiliser et vous, vous devez avoir toujours une longueur d'avance. Il n'y a pas d'un côté des gens qui conçoivent l'arme et de l'autre ceux qui l'utilisent : les ingénieurs qui conçoivent l'arme informatique sont ceux qui l'utilisent, et ils doivent être sur le champ de bataille pour l'adapter à la menace, être capables d'innover et de redévelopper des armes en permanence.

Ce concept a été très vite intégré par les militaires. Actuellement, dans toute opération militaire, il y a une étude de cyberguerre. Jean-Yves Le Drian lui-même a été extrêmement surpris. Quand il a vu l'ampleur de ce qu'on pouvait faire, il est devenu un grand fan de cette technologie. Et on voit bien d'ailleurs qu'il est extrêmement moteur dans ce domaine.

Peut-on rester en dehors de cette course aux cyberarmements ?

Non. Parce que c'est une technologie duale accessible à tout le monde. Je pense qu'on est face à un dilemme. Tous les pays considèrent que c'est une arme au potentiel de développement technologique exponentiel et incroyable. Quand on regarde ce qui existait en 2000 par rapport à maintenant, c'est gigantesque. Mais en 2030, avec l'Internet des objets, on en sera où ? Ce concept de cyberguerre est issu de l'Académie militaire chinoise qui a compris, à la fin des années 90, que le cyber était le point faible des Etats-Unis. Depuis, toutes les économies occidentales reposent sur le numérique, et sont donc extrêmement vulnérables. Mais ce sont les pays occidentaux qui ont vraiment ouvert la boîte de Pandore.

Les Américains considèrent qu'ils ont dix-quinze ans d'avance par rapport à nous, et opposent les Gafa *[Google, Apple, Facebook, Amazon, ndlr]* et la vieille Europe. Ils ont mis des vulnérabilités dans un certain nombre d'outils afin de pouvoir en faire des cyberarmes, et cette vulnérabilité se retourne contre nous. Les Américains n'ont aucunement l'intention de lâcher leur suprématie et leur avance. Pour eux, le cyberespace sera le cyberespace des Gafa. Et les Gafa sont associés avec la NSA.

On ne peut pas se permettre d'avoir des failles dans nos systèmes, a fortiori des failles provoquées par des Etats qui les utilisent contre d'autres Etats. Le directeur du FBI dit qu'il faut absolument être capable de continuer à pouvoir décrypter les algorithmes de cryptographie. Maintenant, pour l'évolution de l'industrie, ne faut-il pas rendre ces algorithmes incassables ? C'est un problème d'indépendance technologique fondamental pour l'Europe et les industriels. J'ai beaucoup discuté avec Microsoft là-dessus, qui est en train de faire un lobbying gigantesque pour que les agences américaines aient l'interdiction d'affaiblir ses produits : pour Microsoft, c'est un enjeu absolument majeur pour le futur.

Avec la collecte de masse, que devient la présomption d'innocence ?

Keith Alexander *[l'ancien directeur de la NSA]* était venu nous voir parce qu'on a vraiment développé une relation forte avec la NSA, à partir de 2006. A la fin d'un très bon repas avec Pierre Brochand *[directeur de la DGSE de 2002 à 2008]*, entre le dessert et le café, il nous dit : *«Moi, mon objectif, c'est d'écouter tout l'Internet mondial.»* Je me souviens, on l'avait regardé en lui demandant : *«Comment ça ?»* Aujourd'hui, on voit bien avec Edward Snowden que c'était une volonté en 2007, que la NSA avait depuis acquis cette capacité d'écouter tout le monde, que les Américains ont mis en place une écoute généralisée et qu'ils ont des centaines de milliers de suspects. Mais le problème de fond, c'est de savoir quelles sont les limitations potentielles ? Qu'est-ce que cela veut dire être suspect ? Est-ce qu'on va être arrêté en voulant sortir du territoire français parce qu'un robot de la NSA a décidé qu'on était suspect ? Il faut qu'il y ait des limites, et c'est aux hommes politiques de définir où sont ces limitations.

En tant qu'Européens, Français, on s'était mis des limites déontologiques, puisque la loi de 1991 *[sur les écoutes téléphoniques]* était totalement floue sur ces technologies modernes. En particulier, on avait décidé de ne pas s'espionner entre pays européens et entre grands alliés, en particulier sur des thèmes politiques et autres. Et ça a été un choc assez violent de découvrir que les Américains ne respectaient pas ces limites

déontologiques et qu'ils avaient piraté l'Elysée en 2012.

C'est pour ça que la France ne fait pas partie des Five Eyes (2) ?

J'étais personnellement plutôt favorable à ce qu'on soit le sixième oeil, notamment parce qu'il y a un *«no spy agreement»* entre ses signataires : normalement, ils ne s'espionnent pas entre eux. Mais la France, au niveau politique, n'accepte pas cet engagement. Donc on est le sixième oeil sans l'être vraiment : on est un allié assez particulier par rapport aux Américains, parce que les Allemands sont en retrait maintenant dans ce domaine, et que la capacité technique de la France est quand même la première dans l'Europe continentale.

Un des documents Snowden parle d'un logiciel espion qui serait français et s'appellerait Snowglobe. Ça vous dit quelque chose ?

*(Rires)* Les informaticiens aiment bien donner des noms de code. Donc les Français ont donné des noms de code, il pouvait y avoir Babar, Titi, etc. Ce que montre Snowden, c'est que la NSA et ses alliés ont surveillé l'action de la France (et d'autres) dans ce domaine-là, et je pense que ce qui est intéressant, c'est que ces documents montrent que l'action de la France a été jugée assez efficace finalement.

*(1) Les dispositifs de collecte de masse déployés par la France à partir de 2008 sur les câbles sous-marins n'avaient pas été entièrement révélés lors de l'interview.*

*(2) Accord de coopération qui réunit, autour de la NSA, les services de renseignement électroniques britanniques, canadiens, australiens et néo-zélandais.*



**Retour à la table des matières**

Nombre de document(s) : **1**

Date de création : **8 avril 2016**

Créé par : **TELECOM-PARISTECH**

table des matières

Les Echos
Les Echos, no. 21990
High-Tech & Médias, jeudi 30 juillet 2015, p. 20

Internet

# Hornet, le nouveau réseau anonyme

**Le nouveau venu entend marcher sur les platesbandes de Tor .**

Voilà un projet qui risque fort de faire grincer des dents les défenseurs de la loi sur le renseignement, votée au Parlement le 24 juin. Nom de code : Hornet. Ce nouveau réseau Internet, dévoilé par cinq chercheurs de l'Institut fédéral de technologie de Zurich et de l'University College de Londres, promet une navigation anonyme, sécurisée et aussi rapide qu'une connexion très haut débit.

Pour le moment, les internautes désireux de surfer gratuitement et anonymement peuvent se tourner vers Tor, un réseau Internet anonyme. En téléchargeant le navigateur Tor, n'importe qui peut aller sur Internet sans trop de craintes d'être espionné. Problème, la connexion est lente. Ce à quoi Hornet veut mettre fin en simplifiant le trajet des informations. Conséquence, en conservant une très bonne vitesse de connexion, ce réseau pourrait accueillir plus d'utilisateurs que Tor.

## Sécurité améliorée

*« Du point de vue de l'utilisateur, il n'y aurait quasiment pas de différence entre utiliser Hornet et utiliser une connexion "normale" »* , confirme un informaticien répondant au pseudonyme d'Aeris. Le débit pourrait donc être celui d'une connexion fibre optique actuelle, soit la meilleure technologie existante. En ce qui concerne la sécurité, les chercheurs à l'origine d'Hornet ont un peu amélioré le principe de fonctionnement de Tor. A savoir le système du réseau « onion » permettant de protéger les données transmises à travers plusieurs couches de chiffrement.

Mais le réseau est encore à l'état de projet et rien ne dit qu'il verra le jour en l'état. *« Ca semble prometteur, mais la question qui se pose est celle des machines composant le réseau »* , continue Aeris. Avec Tor, les connexions passent souvent par de petits serveurs appartenant à des bénévoles. Pour Hornet, les serveurs supportant le réseau devront être plus puissants, sans quoi la vitesse de connexion pourrait baisser fortement. A l'heure actuelle, Tor est utilisé par environ 2 millions de personnes. Si le projet Hornet se concrétise, le nombre d'internautes anonymes pourrait bien augmenter.

Romain Duriez



**Retour à la table des matières**