Camouflage dans l'infosphère

Quelques bases d'autodéfense numérique

Anonyme
Texte rédigé pour le recueil
juillet 2020

et un jour les centres nous suivront
et ce jour nous casserons les prisons

À l'échelle de la biosphère, on est une espèce particulièrement facile à surveiller. Durant notre processus évolutif, comme des grosses quiches qui croient dominer le monde et n'ont plus peur de rien, on a abandonné toutes nos aptitudes au camouflage.

On est même l'espèce qui a inventé les dispositifs de contrôle les plus sophistiqués.

Avant, les luttes étaient en papier, en barricades, en armes à feu. Il n'y avait qu'un combat pour l'organisation du territoire physique. Le temps passe et on observe l'obsolescence programmée de la matière.

Aujourd'hui, on roule joyeusement, avec les freins franchement sabotés, sur l'autoroute de la numérisation. Chacune de nos actions, chacune de nos interactions avec notre environnement peut devenir une donnée : l'endroit qu'on habite, ce qu'on achète, avec qui on parle, ce qu'on mange, etc[1]. Ce sont des milliers d'informations que l'on donne chaque jour à l'infosphère, qui chaque jour sont *données*.

1. *La piraterie n'est jamais finie* [n° 5] décrit ce phénomène et comment il réduit la liberté d'action des hacktivistes.

Si vous posez votre oreille contre le coquillage de la domination, vous n'entendrez pas le bruit de la mer, vous entendrez une voix qui murmure : « donner ses données, reprendre, c'est voler ». Enlevez le coquillage, approchez-vous de la fenêtre, vous entendrez une autre voix — des milliers de voix en fait — qui chantent : « Tout est à nous, rien n'est à eux, et ce qu'ils ont ils l'ont volé ».

Alors, on répond à l'appel de la rue, on organise le contre-braconnage de nos existences, la réappropriation de ce qu'on nous carotte, l'invisibilisation des zones numériques de nos combats.

Donc, l'infosphère est un nouveau territoire de la lutte, avec un nouveau papier, de nouvelles barricades, de nouvelles armes. Parler de « territoire », c'est un peu abusif. C'est un ensemble de machines qui s'envoient des signaux et des stimuli, un genre de truc orgiaque mais version minérale, un immense réseau tissé d'information : le plus formidable outil de contrôle jamais inventé par le camp autoritaire et le plus formidable outil d'organisation et de partage dont le camp libertaire n'ait jamais disposé. Nouveau paradoxe : une prison qui porte en elle le potentiel de l'émancipation générale. La question de fond, c'est qui va gagner ? Mais ça, ça nous dépasse, la question qui nous occupe ici, c'est comment rester invisible quand on fait voyager nos informations dans le réseau de machines ?

On trouve sur le net beaucoup de très bons guides sur l'autodéfense et la légitime attaque numérique. Seulement, ils sont le plus souvent très longs, rarement francophones, globalement peu vulgarisés. Alors on s'est demandéexs comment fournir une synthèse efficace, suffisamment courte et détaillée, simple et la plus inclusive possible, pour sortir un peu du champ de vision des machines, des États et des entreprises. On va se concentrer sur les pratiques militantes et laisser de côté ce qui relève des situations de sécurité de la vie quotidienne.

En gros, comment s'assurer une protection numérique minimale, quand on y connaît que dalle ? Mais attention, c'est une base, forcément incomplète, qui donne des pistes, sans remplacer un vrai temps d'autoéducation en ligne. De plus, le temps passe vite et, contrairement au vin, les tutos sur le numérique vieillissent mal. On insiste : explorez tout vous-mêmes, informez-vous autant que possible. Ceci est une introduction.

Pour commencer, on va se poser une question simple et une question complexe : c'est qui l'ennemi ? c'est quoi l'information ?

C'est qui l'ennemi ?

- *L'État*, comme d'hab, avec sa horde de clowns bleu fluo qui jouit du monopole de la violence légitime et les quelques iClowns spécialisés qui organisent la surveillance de l'infosphère. Iels peuvent enquêter sur des groupes ou sur des individus, construire les dossiers soumis à la justice pénale et activer l'ensemble de la machine répressive juridique via des enquêtes numériques commanditées par des juges. C'est un ennemi particulièrement tenace, parce que ses moyens sont immenses, mais pour qui les enquêtes numériques sont lentes et coûteuses. Si le flic n'arrive pas à forcer une personne à déverrouiller son téléphone en garde à vue, il est peu probable que toute l'administration nécessaire pour forcer un téléphone se mette en place rapidement. Rappel : *don't talk to the police*.
- *Le Capital*, comme d'hab, et les différentes milices bariolées qu'il peut se payer : départements internes de surveillance, hackeureuxses mercenaires, détectives privéexs, geeks traîtres à leur classe qui écrivent des programmes contre-révolutionnaires pour cracker des mots de passe, etc. Les

mises sur écoute et autres enquêtes numériques illégales commanditées par des entreprises sont bien moins rares qu'on pourrait le croire. Et bien sûr, on n'oublie pas que l'infosphère est essentiellement propriétaire, c'est-à-dire que c'est le Capital qui nous ouvre la porte du réseau et qui nous lâche pas pendant toute la durée de notre visite (en nous fournissant un accès à internet et la majorité des serveurs et des canaux sur lesquels on peut naviguer). Souvent mandatées par des groupes d'intérêts financiers, les entreprises sont plus difficiles à cerner et pratiquent plus facilement la surveillance illégale, puisqu'elles ne sont pas assujetties aux lois censées encadrer le travail de la police.

- *La merveilleuse assemblée hétéroclite qui porte le doux nom de fachosphère* et parmi laquelle certains individus d'exception ont appris à se brancher au réseau. L'essentiel de la menace fasciste numérique (et de la lutte antifasciste) se présente comme une guerre d'information qui nécessite rarement des compétences techniques (*doxxing*°, enquêtes sur les réseaux sociaux, dénonciation de militanxtes à leurs employeureuxses, menaces physiques et morales via les canaux de communication traditionnels, etc.).

C'est quoi l'information ?

Ça, c'est plus complexe. Ici, on propose de présenter trois points principaux :

- le stockage (sur des machines physiques comme un ordinateur) ;
- la requête (la navigation sur internet) ;
- la communication (s'envoyer des données).

On essaiera de toujours décrire brièvement la situation, puis de donner le meilleur conseil de sécurité possible. Par souci de synthèse, on vous laissera approfondir en ligne votre autoéducation sur certains logiciels, sans les présenter en détail.

Le stockage

Rappel : contrairement aux corps de police, les machines ne sont pas biodégradables, donc ne les jetez pas dans la nature[2] !

Rappel : contrairement aux corps de police, les machines respirent encore quand on les débranche du réseau, donc une première routine de sécurité concerne l'ensemble des manières dont on stocke les données en dehors de toute connexion sur le Net.

La plupart de ces conseils visent à se défendre si notre ordinateur est saisi par des ennemis dans le cas d'un cambriolage par exemple (parfois appelé « perquisition » lorsque décrété par unex juge), mais aussi à se prémunir contre différentes infiltrations pouvant venir du Net : des virus, des *spywares*°, etc.

Un ordinateur hors-ligne

L'infosphère est une drogue dure, dès qu'on y branche un ordinateur, il devient accro et toute connexion au réseau laisse des traces dans son disque dur. Certaines activités numériques, comme rédiger des textes, préparer des visuels ou monter des vidéos, peuvent se faire de manière sûre sur une machine *offline*. Un ordinateur qui ne s'est jamais connecté ne peut pas être infiltré depuis le net. On peut aussi démonter sa carte réseau (le bidule qui permet à la machine de se mettre en réseau), comme on peut démonter ses

2. Pour quelques recettes de compost, consulter *Le compost généralisé* [nº 41].

émetteurs wifi et bluetooth.

Conseil de sécurité : avoir un ordinateur secondaire qui ne se connecte jamais pour travailler des documents (textes, images, vidéos). N'y faire entrer et sortir des données qu'avec des périphériques non connectés, comme des clés USB, surtout jamais de smartphone. C'est une solution onéreuse, mais si on se détend un peu avec le concept de propriété privée, ça peut se trouver gratuitement un ordinateur (pourquoi pas en empruntant les ordinateurs de personnes qui ont les moyens de s'en repayer).

Conseil de sécurité : il n'est pas rare que votre ordinateur soit infecté par un périphérique externe. On peut copier une quantité considérable de données en laissant une clé USB spécifique branchée quelques minutes. Ne branchez une clé USB à votre appareil que si vous êtes absolument certainexs de sa provenance. En cas de doute, transférez vos fichiers via OnionShare (voir ci-dessous).

Conseil de sécurité : Si vous transformez un ordinateur connecté en ordinateur non connecté, n'oubliez pas de détruire l'ensemble de vos traces, puis de le reformater aux paramètres d'usine.

Un disque dur interne chiffré

Quels que soient vos choix en matière de sécurité, protégez vos ordinateurs avec un mot de passe long et que vous n'utilisez que pour cela. Cela permet de chiffrer le disque dur de votre machine.

On ne parle pas ici du mot de passe qui vous permet couramment d'accéder à votre session, mais d'un chiffrement disque. Renseignez-vous sur des applications qui permettent de le faire simplement : Filevault (Mac), BitLocker (Windows), LUKS/VeraCrypt (Linux), simple code (IOS).

Des disques externes chiffrés

La corbeille, même vidée, reste à moitié pleine. Chaque fois que l'on importe, crée ou modifie un document (texte, image, vidéo, etc.) directement sur son ordinateur, des données s'écrivent et on laisse des traces qui peuvent être récupérables. Sur les systèmes d'exploitation principaux, comme ceux d'apple ou de microsoft, il est même parfois impossible d'effacer complètement la présence de ces informations. C'est encore mieux, bien sûr, si les disques externes sont chiffrés. Cela veut dire que leurs données ne sont pas écrites de manière lisible et qu'il faut entrer un mot de passe pour les déchiffrer.

Conseil de sécurité : Créez, stockez, travaillez et supprimez vos documents sensibles sur des clés USB ou des disques durs externes chiffrés sans jamais les faire transiter par votre ordinateur.

Privilégiez un disque dur externe protégé par un mot de passe et cachez-le en choisissant intelligemment la cachette (il arrive que la cheminée de vos grands-parents soit plus sûre que le coffre-fort de votre bar anarchiste préféré).

Mots de passe

Utilisez des mots de passe longs, aussi aléatoires que possible et uniques pour chaque service. Pour éviter de devoir se le rappeler, utilisez un gestionnaire de mots de passe : on conseille KeePass. Ce logiciel permet de stocker de manière sécurisée vos mots de passe et vous évite de devoir vous en souvenir. Ce logiciel est aussi équipé d'un générateur qui permet de créer des mots de passe forts. Ne réutilisez jamais deux fois le même mot de passe.

Logiciels et métadonnées

Un document est un ensemble de données (le texte d'un fichier word, les pixels d'une image, etc.). Mais tout document contient aussi des métadonnées. Les métadonnées sont l'ensemble des informations circonstancielles, comme l'auteurixe d'un document, sa date de création, de modification, les ordinateurs par lesquels il a transité, etc. Elles ne sont pas visibles, mais inscrites dans le code du document et accessibles pour qui sait où chercher. Certaines personnes ont été identifiées puis condamnées sur la seule base de ces métadonnées. Le type et la quantité de métadonnées dépendent du format de document (.doc, .txt, .jpg, .png, .pdf, .mp4, etc.) et des logiciels utilisés pour les traiter (Word, LibreOffice, Adobe, etc.). Dans certains formats d'image, certaines métadonnées indiquent même le lieu et l'heure où se situait l'appareil qui a pris la photo.

Conseils de sécurité :

- pour travailler le texte : LibreOffice, des fichiers au format .txt ;
- pour travailler l'image : sur un ordinateur connecté au net, préférez Gimp et Inkscape. Des anciennes versions de la suite adobe (qui ne nécessitent pas un cloud et un compte lié à une adresse email), si possible sur un ordinateur *offline* ;
- pour travailler la vidéo : privilégiez Kdenlive, Openshot, Blender(3D). Des anciennes versions de la suite adobe (qui ne nécessitent pas un cloud et un compte lié à une adresse email), si possible sur un ordinateur *offline*.

On peut aussi recevoir des documents de l'extérieur et vouloir en « nettoyer » les métadonnées.

Conseil de sécurité : Pour nettoyer les métadonnées des fichiers standards, utilisez la petite application facile d'utilisation

Metadata Anonymization Tool (MAT). Faites ce nettoyage juste avant l'envoi ou la mise en ligne du document (image, texte, etc.) : le rouvrir sur votre ordinateur (dans un traitement de texte ou d'images) réécrira de nouvelles métadonnées.

Les systèmes d'exploitations : un ordinateur de combat

Comme l'État et le Capital, l'ordinateur repose sur un système d'exploitation (OS), soit un ensemble de programmes qui régulent, contrôlent et permettent l'activité de l'utilisateurixe sur la machine. Les plus connus sont évidemment macOS ou windows, équipant respectivement les macs et les PC. En termes de sécurité tous les OS sont égaux, mais certains sont plus égaux que d'autres : comprendre, certains sont de vrais flics. Par principe et en pratique, il faut absolument éviter les OS privés, dont le code n'est pas accessible à touxtes et qui tendent à collecter une quantité immense de données contre la volonté de leurs utilisateurixes. Il est conseillé de se procurer une machine prête au combat dans son fonctionnement même, et d'adopter un OS sécurisé, en plus de tous les conseils de sécurité qui précèdent et qui suivent. On en propose deux : Debian et Tails.

Conseil de sécurité : on peut changer le système d'exploitation de n'importe quel ordinateur, même d'un mac, même si ce n'est pas toujours facile. Avant cela, regardez sur internet comment le reformater aux paramètres d'usine.

Tails

Tails est un « ordinateur » (en fait, un système d'exploitation) qui tient sur un disque externe comme une clé USB ou une carte SD. Le principe est simple : on branche la clé USB sur n'importe

quel ordinateur et on travaille uniquement sur la clé, ce qui ne laisse aucune trace d'activité sur la machine principale. Selon les paramètres de Tails, la clé peut même redémarrer intégralement à chaque fois qu'elle est débranchée. C'est ce qui fait de Tails un « système live » qui autorise une vraie double vie : on peut avoir un ordinateur personnel consacré à la gloire de la vie capitaliste pour brouiller les pistes et, quand vient la nuit, on y branche une clé USB pour travailler anonymement à la révolution sociale.

De plus Tails a l'avantage d'être équipé par défaut de logiciels n'utilisant que les connexions les plus sécurisées (via le réseau Tor, voir ci-dessous) et de bloquer toute connexion non anonyme. Son fonctionnement est largement décrit dans des guides qui lui sont consacrés et qu'on conseille vivement. Tails est un apprentissage qui demande un peu de temps, mais ça en vaut vraiment la peine.

Debian

Debian est un système d'exploitation Linux particulièrement sécurisé si vous ne voulez pas vous lancer dans Tails. Il fonctionne globalement comme n'importe quel OS et après quelques heures à lire des tutos, vous vous y retrouverez rapidement.

Installez Debian sur un ordinateur reformaté aux « paramètres d'usine », cela permet de supprimer l'ensemble des données liées à votre usage précédent de cette machine (effacer votre ancienne vie quoi). Ensuite, effectuez l'ensemble de l'installation sans jamais indiquer d'information qui permettrait de remonter à votre identité réelle (nom, adresse, numéro de téléphone, etc.). Si, à n'importe quelle étape de l'utilisation de votre ordinateur de combat (installation d'une nouvelle appli, paramétrage d'un compte en ligne, etc.), on vous demande ce type d'informations, fuyez absolument ou trouvez une alternative. N'oubliez pas d'activer le chiffrement

complet du disque.

Si possible, essayez d'éviter :

- tout ce qui est lié à apple : le système d'exploitation macOS, ses logiciels et ses formats ;
- tout ce qui est lié à microsoft : le système d'exploitation windows, la suite office, ses logiciels (word, excel, powerpoint, etc.) et ses formats (.doc, etc.), skype, etc ;
- le PDF, qui est un format particulièrement transparent en termes de métadonnées, même s'il est possible de l'utiliser de manière sécurisée.

La requête

Pour naviguer sur le réseau de machines, mieux vaut abandonner cette fiction bourgeoise qu'est l'identité et rester fluide. Lorsqu'on navigue sur internet, notre ordinateur envoie une requête à un ensemble d'autres ordinateurs sur lesquels sont hébergées des informations, comme les sites. L'ensemble de ces interconnexions laisse des traces chez différentes entités. La requête est une trajectoire dans ce réseau que l'on doit essayer d'anonymiser : il faut adopter dès l'origine une identité numérique qui ne pourra être retracée jusqu'à notre identité physique. Le plus souvent, l'identité numérique désigne le numéro d'identification de votre ordinateur et celui de votre point d'accès wifi, ce sont les deux principales informations qui permettent de remonter jusqu'à vous.

Si vous vous connectez avec un ordinateur qui n'est pas le vôtre depuis un wifi public, il sera très difficile de relier votre activité en ligne (ce que vous ferez sur cet ordinateur) à la personne que vous êtes : votre identité numérique du moment est difficile à lier à votre identité administrative. C'est pour cette raison que les cybercafés apportaient une certaine protection (même si ce n'est

plus vrai aujourd'hui, puisqu'on demande souvent une identité administrative dans ces endroits).

En revanche, et on part du principe dans ce texte que ce sera la situation la plus fréquente pour vous, si vous vous connectez depuis un ordinateur qui vous appartient sur le wifi de votre maison : votre identité administrative est très facile à lier à cette identité numérique (qui est en fait votre identité numérique la plus fréquente). On sait très bien que ce wifi est utilisé par un très petit nombre de personnes, qui sont en général celles qui paient la facture, et idem pour l'ordinateur.

Tor

Tor est un réseau accessible à travers un navigateur qui cherche à empêcher quiconque de déterminer avec certitude les pages que vous avez visitées. Pour ce faire, il fait en sorte que chaque requête passe par trois relais intermédiaires avant d'arriver au site de destination. Il est assez simple de trouver en ligne des descriptions techniques du fonctionnement de Tor. Pour dire l'essentiel, si vous naviguez en utilisant Tor, les personnes qui administrent votre accès à internet ne connaissent que l'adresse du premier relai (en gros, iels savent que vous utilisez Tor, mais pas quelle page vous consultez) et les personnes qui administrent la page que vous consultez ne savent pas d'où vous arrivez, elles voient seulement que la troisième destination (un relai Tor quelque part sur la planète) s'est connectée à leur site. Si vous consultez facebook depuis la box d'un opérateur, comme swisscom par exemple : swisscom sait que vous naviguez sur Tor, mais pas sur quel site, et facebook sait qu'une personne est connectée depuis le réseau Tor, mais sans savoir depuis quelle box ni quel ordinateur (donc sans avoir aucun élément qui permette

de remonter à votre identité administrative).

Conseils de sécurité :

- n'utilisez que Tor pour naviguer sur internet ;
- la prudence reste de mise durant l'ensemble de la navigation. Si vous consultez facebook depuis Tor en vous connectant à votre compte avec votre adresse email privée (*jeanne.dupont@gmail.com*), Tor ou pas, facebook saura que Jeanne Dupont s'est connectée. Cela est valable pour l'ensemble des situations : n'entrez jamais aucune information privée durant votre navigation ;
- n'hésitez pas à relancer Tor fréquemment pour refabriquer une nouvelle identité numérique (un nouveau circuit de connexion Tor) ;
- prenez l'habitude d'utiliser Tor, même dans les navigations qui ne sont pas particulièrement risquées, pour multiplier les connexions et brouiller les pistes ;
- ne modifiez pas les paramètres par défaut du navigateur ;
- n'utilisez pas Tor pour télécharger en *torrent*°.

VPN

Un réseau privé est un réseau d'appareils connectés les uns avec les autres, parfois à internet. Votre imprimante et votre ordinateur forment un réseau privé connecté à votre wifi, ce qui vous permet d'imprimer directement sans avoir à relier physiquement les appareils. Les VPN (*Virtual Private Network*) sont des applications qui permettent de simuler un réseau privé et d'accéder à internet à travers lui. Les VPN prennent la forme d'une application à installer sur votre ordinateur. Une fois activée, vous appartenez virtuellement à un réseau, vous pouvez parfois choisir le pays où est situé ce réseau. Dès lors, vous vous connectez et naviguez sur internet

avec l'identité de ce réseau et non plus l'identité de votre ordinateur. Votre fournisseur d'accès à internet voit seulement que vous vous connectez à un VPN.

Attention, la plupart des applications de VPN sont privées et payantes. La plupart des sociétés sur le marché conservent des *logs* de connexion, soit l'historique des pages que vous avez visitées depuis leur VPN. Ne faites confiance à aucune société privée de VPN, la plupart disposent de votre identité administrative et ont déjà montré qu'elles collaborent avec la police.

Conseil de sécurité :

- utilisez Riseup VPN, et faites-leur un don, entretenir un VPN coûte cher ;
- utiliser un VPN en plus de Tor est un débat non résolu de la sécurité informatique. Ici, on est plutôt contre. S'il faut choisir l'un ou l'autre, utilisez Tor et ne vous posez pas trop la question du VPN.

Moteurs de recherche

Vous savez sans doute ce que sont les moteurs de recherche, ces algorithmes propriétaires que les individus postmodernes utilisent à la place de leur mémoire. Les moteurs de recherche sont de sacrés flics et vous êtes autant leur produit que leur client. Bannissez tous les moteurs propriétaires pour éviter de laisser des petits cailloux partout où vous passez.

Conseil de sécurité : utilisez DuckDuckGo, sur Tor. Réglez Tor comme votre navigateur par défaut, et DuckDuckGo comme votre moteur de recherche par défaut (ça évitera les boulettes en cliquant sur un lien sensible qui s'ouvrira par défaut dans google chrome par exemple).

Réseaux sociaux

Bon alors, on incendie tout ça ? Il faudrait un texte entier, qui arriverait probablement à la conclusion que ça brûlera avec le reste, mais qu'en attendant ça peut servir. Il existe des réseaux sociaux plus sûrs, comme Mastodon, mais comme ils sont assez peu fréquentés, ça leur enlève une bonne partie de leur intérêt.

Sur twitter, facebook ou instagram, le truc essentiel, c'est de se créer un compte anonyme, mais anonyme de fond en comble. Sortez vos dispositifs d'identification anonyme : une adresse email Riseup créée pour l'occasion (voir ci-dessous), avec un nom débile et jamais utilisé ; un numéro de téléphone prépayé et anonyme ; comme pseudo un Prénom et un Nom vraisemblables mais pas les vôtres, une photo vraisemblable (une bonne vieille image gratuite de clownettex en costard). Peut-être qu'un jour facebook demandera une carte d'identité pour vérifier l'authenticité du compte, et il faudra recommencer. C'est plus facile pour twitter (pas besoin de numéro de téléphone). Faites toute cette procédure, bien sûr en respectant toutes les consignes de sécurité (ordinateur de combat, Tor, etc.). À partir de ce compte, on peut ensuite créer des pages ou des groupes et publier du contenu.

Pour instagram, pas besoin de numéro de téléphone, mais la galère c'est qu'on peut difficilement publier du contenu depuis un ordinateur. On peut se créer un compte et visiter d'autres pages en respectant les consignes.

Pour publier du contenu, passez par un smartphone équipé d'un VPN.

Pour publier sur instagram depuis un ordinateur (idéalement pas celui sur lequel des choses sensibles se passent) :

- installez le navigateur Brave ;

- ouvrez Brave, ouvrez une nouvelle page de navigation privée avec Tor ;
- allez sur instagram.com ;
- authentifiez-vous ;
- sur la page faites un clic droit et sélectionnez Inspecter ;
- cliquez sur l'icône de téléphone/tablette en haut à gauche du panneau qui s'ouvre ;
- sélectionnez *iphone X* dans le menu déroulant le plus à gauche du bandeau qui vient d'apparaître en haut de la page ;
- rafraîchissez ;
- vous pouvez (presque) tout faire comme si vous étiez connecté depuis un smartphone, mais sur votre ordinateur sécurisé (Tor, etc.).

Conseil de sécurité : quel que soit le réseau social, créez un compte anonyme de bout en bout (aucune étape de la création du compte ne permet de remonter à votre identité administrative ou numérique). Essayez de ne pas publier du contenu sensible sur les réseaux depuis votre smartphone.

Publier des données sur internet

On a souvent besoin de publier des données sur internet en tout anonymat, par exemple pour revendiquer une action que la morale bourgeoise réprouve. La publication peut se faire via les réseaux sociaux, des forums ou des journaux *open-source*.

Si vous respectez tous les conseils ci-dessus, vous êtes déjà bien. Faites particulièrement attention :

- à naviguer sur Tor, pour que votre fournisseur d'accès et le site ignorent tous deux que vous vous êtes connecté ;

- à effacer les métadonnées de vos textes et images pour éviter de mettre en ligne la photo d'une action qui contiendrait dans son code l'auteurixe, la date et l'heure où l'image a été prise, etc ;
- à ne pas réutiliser un compte qui vous a déjà servi : sur les forums, créer un profil sécurisé qui ne servira qu'à revendiquer l'action (ce qui évitera de pouvoir remonter jusqu'à vous en consultant les autres messages postés, idem sur les réseaux sociaux).

Il est parfois plus sûr d'envoyer un mail à un média autonome ou révolutionnaire de confiance et de les laisser s'occuper de la publication.

Si vous le pouvez, essayez d'éviter :

- tous les navigateurs qui ne sont pas Tor (chrome, firefox, safari, etc.) ;
- tous les moteurs de recherche qui ne sont pas DuckDuckGo (google, yahoo et même cette daube d'ecosia parce que écologie libérale = mensonge du Capital) ;
- un même mot de passe partout, des mots de passe trop simples, des mots de passe qui n'utilisent ni chiffres ni caractères spéciaux, des mots de passe qui utilisent des mots du dictionnaire ;
- les sociétés privées de VPN.

La communication

Le plus sûr, c'est souvent de n'avoir rien à déclarer. Mais pour s'organiser, il faut pouvoir communiquer. On détaille ici quatre types d'échange d'informations : les mails, la discussion en temps réel (tchat), l'écriture collective en ligne et l'envoi de fichiers de grande taille (images, vidéos).

Mail

L'ensemble du trafic d'informations qui permet l'envoi d'un mail présente de très nombreuses failles de sécurité possibles.

Quand vous envoyez un mail, votre ordinateur envoie une requête qui passe par :

- le routeur wifi ;
- puis la société privée qui vous fournit l'accès (p. ex. swisscom) ;
- puis à un serveur DNS ;
- puis au serveur sur lequel est hébergée votre boîte mail (p. ex. outlook) ;
- vous écrivez votre mail ;
- et ça repart en sens inverse.

Chaque serveur (chaque machine) par laquelle transite l'information en garde des traces dans des registres qui peuvent être consultés par les sociétés privées ou les États. Même si cela peut paraître étonnant, sans précaution de votre part, de très nombreux intermédiaires peuvent lire le contenu de vos mails aussi facilement que lae facteurixe pourrait ouvrir votre courrier. Vous pensiez vraiment que gmail et les autres pouvaient définir ce qui va dans la boîte « spam » sans lire le contenu du mail ? (ce travail est sous-traité à des robots qui ne sont pas syndiqués et bossent 24 h sur 24 h, indignez-vous).

Pour envoyer un mail de manière sécurisé :

- créez une adresse dont l'intitulé est sûr (pas d'information personnelle, ou de pseudos connus, etc.) ;
- cette adresse, ouvrez-la chez un hébergeur sûr. On conseille le collectif Riseup, basé à Seattle et œuvrant depuis des années à la sécurité numérique des militanxtes. Notez bien qu'aucun collectif n'est absolument sûr, n'écrivez dans

vos mails que le strict nécessaire et gardez vos envolées lyriques révolutionnaires pour les réunions en face à face. Pour ouvrir une adresse @riseup.net, il vous faut un compte Riseup. Pour obtenir un compte, il vous faudra être parrainé par des personnes disposant déjà d'un compte Riseup. Débrouillez-vous (traînez dans les coins anarcho-louches de votre bled, vous finirez bien par tomber sur une personne capable de vous fourguer ce genre de came). Un mail qui reste sur les serveurs Riseup (envoyé d'une adresse @riseup.net à une autre) est complètement chiffré de bout en bout : seules les personnes qui envoient et reçoivent le mail peuvent le lire. Les administrateurixes de Riseup ne le peuvent pas ;

- n'envoyez aucune information sensible à des adresses qui ne soient pas des adresses @riseup.net. Faites à la personne en question un petit cours de sécurité, maintenant que vous êtes dans la team, envoyez-leur une clé d'accès Riseup et attendez qu'elles se soient créé une adresse *safe* pour échanger vos meilleures recettes de tofu[3] ;
- renseignez-vous sur ce qu'est le chiffrement PGP, pour un peu d'autoéducation et une couche de sécurité supplémentaire.

Discussion en temps réel (tchat)

Le smartphone n'est jamais votre ami. Oubliez d'emblée toutes les applications de cette chère Silicon Valley (whatsapp, facebook messenger, etc.). Il existe d'autres applications qui proposent un tchat chiffré de bout en bout (*end-to-end encryption*), ce qui

3. Pour d'autres excellentes recettes, consulter *Le Grand Midi* [nº 47].

empêche même les administrateurixes de connaître le contenu de vos échanges. Deux solutions viables existent : Signal et Telegram. Les deux sont très faciles d'accès et d'utilisation. En revanche, ces applications sont liées à votre numéro de téléphone, ce qui signifie que TOUT LE MONDE déteste la… que TOUT LE MONDE peut savoir facilement qui parle à qui et quand. Selon la situation, cette seule information peut être très précieuse pour les ennemis.

Signal :

- est *open-source* (cela signifie que son code est public, donc que de nombreuses personnes ont collectivement vérifié que les messages étaient bel et bien chiffrés) ;
- permet de régler un délai d'autodestruction des messages qui peut s'avérer bien pratique ;
- ne stocke pas les échanges sur ses serveurs (désinstaller l'application les supprime, mais de votre côté seulement) ;
- est basé aux USA, ce qui signifie que la NSA a probablement accès à vos échanges.

Telegram :

- n'est pas *open-source* ;
- permet de supprimer vos messages sur votre téléphone et ceux de tous les destinateurixes ;
- permet de créer des *bots*, soit des canaux de discussion où tout le monde peut discuter de manière privée avec le collectif de personnes qui a créé le *bot* ;
- permet de créer des canaux (un collectif gère un fil d'information auquel on peut s'abonner, sans pouvoir interagir, un peu comme twitter mais sans les commentaires) ;
- est basé en Russie, donc probablement accessible par le FSB, le successeur du KGB wesh.

Conseil de sécurité : n'installez jamais la version desktop de

Signal ou telegram sur votre ordinateur de combat : ces applications sont liées à votre numéro de téléphone (qui permet de remonter facilement à votre identité), cela mettrait en danger l'ensemble de vos routines de défense. Signal a annoncé en 2020 que l'application ne sera bientôt plus reliée à un numéro de téléphone, ce qui mériterait une grande fête collective.

Pads

Les pads sont des outils collaboratifs en ligne qui permettent d'écrire un fichier en collectif (une alternative aux google docs par exemple). Si l'on y accède exclusivement par Tor, ils peuvent difficilement être reliés à des utilisateurixes.

Là encore, on conseille vivement les pads proposés par Riseup. Attention toutefois, ils ne sont pas protégés par un mot de passe. Cela permet à toute personne possédant le lien d'accès de les modifier : n'y mettez jamais d'informations personnelles ou compromettantes.

Conseil de sécurité : utilisez des Riseup pads.

Partager des documents

Le problème des mails, c'est qu'on peut difficilement s'en servir pour s'envoyer des trucs lourds, surtout en respectant les consignes de sécurité exposées ici. L'internet sécurisé est beaucoup plus lent, parce que l'argent permet d'acheter la vitesse.

Pour pallier cela, Tor est de nouveau une solution viable. Le collectif a développé un outil de partage nommé OnionShare qui divise votre fichier en petits paquets qui circulent sur les points relais Tor. Il vous suffit d'installer le logiciel sur votre ordinateur de combat, puis d'y glisser le document lourd que vous souhaitez

partager. Le logiciel génère un lien de partage que vous pouvez envoyer au destinataire (en respectant les consignes de sécurité). Le transfert ne fonctionnera que tant que l'application est ouverte sur votre ordinateur. Vous verrez le nombre de personnes qui téléchargent le fichier, si ce nombre est anormal, fermez l'application immédiatement.

Conseil de sécurité : utilisez OnionShare et assurez-vous que toutes les personnes concernées sont connectées en même temps en discutant sur Telegram/Signal.

Niquez tout, brûlez le reste et n'utilisez pas ça :

- les services mail privés. Les applications mail installées sur ton ordinateur ;
- les services de transfert de documents privés, tout ce qui n'est pas OnionShare ;
- les applications de messagerie privées qui ne sont pas Signal ou telegram (whatsapp, messenger, etc.) ;
- les pads et *clouds* privés (google docs, google drive, dropbox, etc.) ;
- tout ce qui passe par le réseau téléphonique standard (appels, SMS, MMS, etc.).

Téléphone portable

Dumb phones

On pense parfois à tort que les *dumb phones*° sont plus sûrs que des smartphones. Il est vrai qu'ils sont dépourvus des trackers modernes de google, apple, samsung, huawei et les autres, mais, en réalité ils n'offrent presque aucune sécurité :

- rien n'est chiffré sur l'appareil, quiconque a un accès physique à votre appareil peut en extraire le contenu ;

- l'antenne étant vieille, aucune sécurité n'est garantie lors des communications (appels, sms, mms) ce qui permet à toute personne à proximité de se faire passer pour votre opérateur téléphonique et d'avoir accès à toutes vos communications (les kits qui permettent de le faire se trouvent pour moins d'une centaine de francs suisses) ;
- la triangulation de votre téléphone par les antennes cellulaires auxquelles vous vous connectez permet votre localisation. Aux yeux de la police, qui collabore avec les opérateurs téléphoniques, il n'y a aucune différence entre un vieux téléphone et une puce gps que vous auriez directement dans la poche, ce qui n'est pas le cas avec un smartphone bien protégé.

Smartphones

Évitez un usage sensible du smartphone autant que possible. Il existe des solutions pour se créer un téléphone portable de combat, mais elles exigent des développements techniques qui excèdent ce texte. En gros, android et iOS contiennent du code « propriétaire » inaccessible (non *open-source*) et il est impossible de vérifier ce que les entreprises affirment en termes de sécurité ni de savoir ce à quoi elles ont effectivement accès. Si vous n'avez pas le choix, quelques conseils cependant :

- chiffrez le contenu de son disque avec un bon mot de passe (voir ci-dessous) ;
- faites toujours les dernières mises à jour ;
- ne *rootez*° pas votre Android et ne *jailbreakez*° pas votre iphone ;
- gardez le moins d'informations possible sur votre téléphone et faites y transiter le moins de choses possible ;

- réinitialisez régulièrement le téléphone pour en effacer le contenu. N'utilisez ni les sms ni les appels téléphoniques pour les choses sensibles : utilisez Signal/telegram (voir ci-dessus) ;
- n'activez jamais le déverrouillage par reconnaissance faciale ou digitale ;
- désactivez les notifications sur l'écran verrouillé ;
- désactivez la localisation (dans les paramètres de l'appareil) ;
- ne reliez pas l'appareil à un compte (par exemple un compte Apple). Ou alors, faites-le le temps de télécharger une application (les *stores* requièrent souvent une adresse email) et déconnectez ensuite ce compte de l'appareil ;
- de manière générale, ne laissez pas d'informations qui permettent de faire le lien entre vous et l'appareil. En cas de problème, vous pouvez toujours dire que vous l'avez trouvé par terre et que vous vouliez l'apporter aux objets trouvés (ce qui est d'ailleurs valable pour tous vos appareils sensibles) ;
- si vous devez absolument l'apporter dans un endroit risqué (manifestation, action, etc.), videz-en le contenu pour ne pas mettre d'autres personnes en danger. Quittez autant que possible les applications de discussions, ne laissez dessus aucune trace, sinon l'application et/ou le groupe de discussion dont vous auriez besoin pendant l'action ;
- n'utilisez pas les applications qui se réclament de Tor. Sur android, équipez plutôt votre smartphone d'un Riseup VPN (la marche à suivre est sur le site de Riseup).

Rappel : en Suisse, la police peut déverrouiller tous les smartphones, qu'ils soient ou non protégés par un mot de passe, via des programmes comme ceux de la société Cellebrite.

La continuité de cet antizine se fabrique librement sur le réseau.
https://www.noussommespartout.org

*

Nous sommes partout *collecte et partage des voix antifascistes, féministes, anticapitalistes, antiracistes, antispécistes, des paroles de hackeureuxses, des voix en lutte pour les droits des migranxtes, contre toutes les formes d'oppression de nos sociétés, pour les droits LGBTQIA+, contre les écocides, pour les droits des travailleureuxses du sexe, contre les violences policières et la répression juridique, pour les droits des sans-papièrexs, pour l'autodétermination et l'émancipation de touxtes les travailleureuxses, contre la précarisation, contre le système carcéral et pour les ZAD.*

*

La piraterie littéraire n'est jamais finie.
https://abrupt.cc/nsp/nous-sommes-partout

« l'infosphère est un nouveau territoire de la lutte »

CAMOUFLAGE·DANS·L'INFOSPHÈRE
QUELQUES·BASES·D'AUTODÉFENSE·NUMÉRIQUE
ANONYME·JUILLET·2020
TEXTE·RÉDIGÉ·POUR·LE·RECUEIL
WWW·NOUSSOMMESPARTOUT·ORG