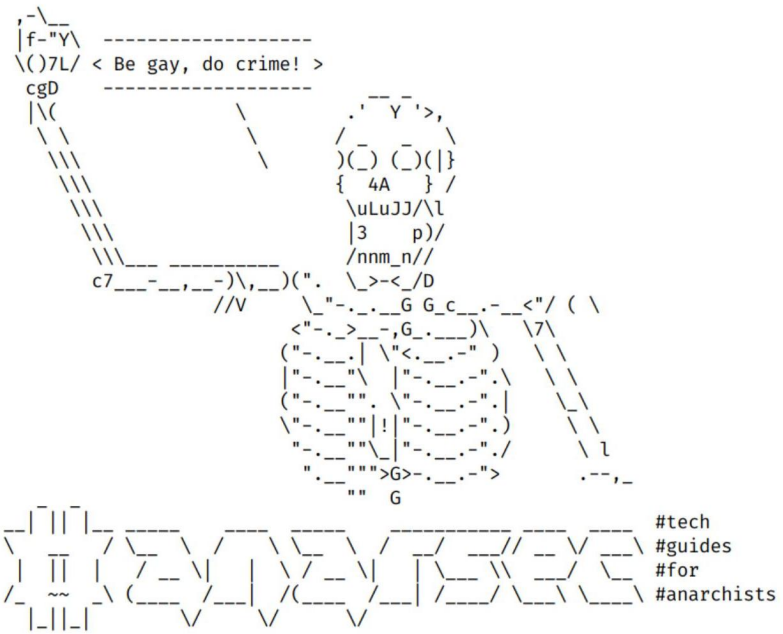
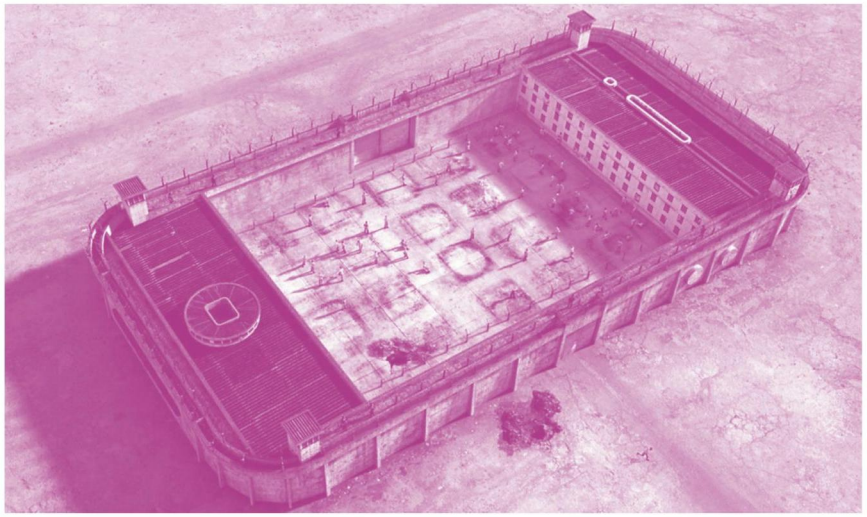
Tue le flic dans ta poche

La culture de la sécurité et la sécurité opérationnelle, quand elles sont efficaces, empêchent les forces répressives de se renseigner sur nos activités criminelles, mais aussi sur nos vies, nos relations, nos déplacements, et ainsi de suite. Ces renseignements sont un énorme atout pour préciser une liste de suspects et mettre en place de la surveillance ciblée. Cet article va présenter quelques stratégies pour tuer le flic dans ta poche.





Série: Défensif

Cette version de la brochure a été modifiée pour la dernière fois le 2024-04-23. Visitez anarsec.guide/fr pour savoir si elle a été mise à jour depuis.

Le symbole de dague † près d'un mot indique qu'une entrée existe dans le glossaire pour ce mot. Ai ferri corti.

AnarSec est une ressource conçue pour aider les anarchistes à se frayer un chemin à travers le terrain hostile de la technologie — des guides défensifs sur la sécurité numérique et l'anonymat, et des guides offensifs sur le piratage informatique. Tous les guides sont disponibles sous forme de brochures à imprimer et seront maintenus à jour.

Défensif

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Téléphonie

- **Tue le flic dans ta poche**
- GrapheneOS for Anarchists

Général

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Offensif

À venir

Table des matières

La culture de la sécurité et la sécurité opérationnelle[1], quand elles sont efficaces, empêchent les forces répressives de se renseigner sur nos activités criminelles, mais aussi sur nos vies, nos relations[2], nos déplacements, et ainsi de suite. Ces renseignements sont un énorme atout pour préciser une liste de suspects et mettre en place de la surveillance ciblée. Cet article va présenter quelques stratégies pour tuer le flic dans ta poche.

La localisation de ton téléphone est pistée en permanence[3], et ces données de localisation sont récoltées par des entreprises privées, ce qui permet à la police de les obtenir sans avoir besoin de mandat. Les identifiants matériels d'un téléphone et le nom lié à l'abonnement téléphonique[4] sont enregistrés par chaque antenne à laquelle il se connecte. Grâce à des services de piratage à distance comme Pegasus[5], même des unités de police locales peuvent prendre le contrôle d'un téléphone, et ces services sont « zero-click, » ce qui veut dire qu'il n'y a pas besoin que tu cliques sur un lien ou ouvres un fichier pour que ton téléphone soit piraté. D'un autre côté, après avoir échoué dans leur enquête sur plus d'une trentaine d'incendies volontaires dans une petite ville en France, des enquêteurs se sont plaint[6] que « l'exploitation de la téléphonie ou des immatriculations de véhicules est impossible puisqu'ils opèrent sans téléphone et sans voiture ! »

Chiffrement et géolocalisation

Dans une opération répressive récente[7] contre un anarchiste, les flics ont pisté la localisation du téléphone du suspect en temps réel et établi

[1] notrace.how/fr/blog/a-base-to-stand-on/une-base-sur-laquelle-s-appuyer.html
[2] notrace.how/threat-library/fr/techniques/network-mapping.html
[3] vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon
[4] anonymousplanet.org/guide.html#your-imei-and-imsi-and-by-extension-your-phone-number
[5] amnesty.org/fr/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus
[6] sansnom.noblogs.org/archives/11527
[7] notrace.how/resources/fr/#ivan

Voix sur IP (VoIP, Voice over Internet Protocol)

Google Voice est un service de voix sur IP bien connu et peu sécurisé ; cette technologie fait passer tes appels par Internet (tout comme Signal par exemple) au lieu d'utiliser la transmission classique par les antennes téléphoniques. Contrairement à Signal, la voix sur IP te permet de recevoir des appels de n'importe qui, pas juste d'autres utilisateurs de Signal. L'avantage d'utiliser la voix sur IP pour des appels par rapport à un abonnement téléphonique est que tu peux créer des numéros différents pour différentes activités (un pour les factures, un autre pour créer un compte Signal, etc.) et que tu n'as jamais besoin de désactiver le mode avion. L'avantage d'un abonnement téléphonique est que tu peux l'utiliser loin d'un accès au Wi-Fi, au prix d'être géolocalisé (c'est-à-dire qu'il est possible pour ton opérateur téléphonique et possiblement d'autres acteurs de savoir à tout moment où est ton appareil).

une liste de toutes les personnes qu'il avait appelé. On sait bien que ce type de surveillance est courante, et pourtant nombre de camarades trimballent un téléphone où qu'iels aillent, ou appellent d'autres anarchistes « en clair ». On pense qu'il faudrait mettre un terme à ces deux pratiques. Ne facilitons pas à ce point le travail des flics et des agences de renseignement en leur offrant nos relations sociales et nos données de localisation sur un plateau d'argent.

Si tu ne sors pas de chez toi avec un téléphone, les flics vont devoir recourir à la surveillance physique pour te localiser, ce qui leur demande beaucoup de ressources et peut être détecté. Et si jamais tu es placé·e sous surveillance physique, l'enquêteur va commencer par chercher à comprendre à quoi ressemblent tes déplacements habituels, et les données de localisation de ton téléphone offrent justement un aperçu détaillé de tes déplacements quotidiens.

Certain·e·s anarchistes pallient aux problèmes des smartphones en utilisant des bigos ou des téléphones fixes pour communiquer entre elleux, mais ce n'est pas une bonne solution. Les bigos et les téléphones fixes ne permettent pas de communiquer de manière chiffrée†, et donc l'État sait qui parle avec qui et ce qui est discuté. Un but premier de la surveillance ciblée est de cartographier les relations sociales de la cible pour identifier d'autres cibles. Le seul moyen d'empêcher nos ennemis de cartographier nos relations est d'utiliser exclusivement des moyens de communication chiffrés[8] quand on communique avec d'autres anarchistes par l'intermédiaire de la technologie.

Motifs de métadonnées

La normalisation de la connectivité permanente au sein de la société dominante a mené certain·e·s anarchistes à noter que les métadonnées† téléphoniques sont utiles aux enquêteurs. Mais à partir de cette constatation, certain·e·s arrivent à la conclusion qu'on ne devrait « jamais

[8] anarsec.guide/posts/e2ee/

éteindre son téléphone, »[9] ce qui nous mène dans la mauvaise direction. Leur logique est que nos interactions avec la technologie forment un motif de métadonnées de base, et que les moments qui dévient de ce motif ont l'air suspects s'ils coïncident avec le moment où une action se produit, ce qui peut être utilisé par des enquêteurs pour préciser une liste de suspects. Même si c'est vrai, la conclusion opposée est bien plus sensée : les anarchistes devraient minimiser la création de motifs de métadonnées auxquels des enquêteurs pourraient avoir accès.

Nos connexions aux infrastructures de la domination doivent rester opaques et imprévisibles si on veut pouvoir continuer à frapper l'ennemi. Et si les repérages préalables à une action impliquent de passer un week-end entier sans appareils électroniques ? Il y a aussi le simple fait que les téléphones doivent être laissés chez soi pendant une action — cela ne dévie d'un motif que si on a habituellement toujours un téléphone avec soi. Dans une vie « toujours connectée », ces deux changements dans nos métadonnées feraient tâche, mais ce n'est pas le cas si l'on refuse d'être connecté en permanence. **Pour minimiser l'empreinte laissée par tes métadonnées, tu dois laisser ton téléphone chez toi par défaut.**

As-tu vraiment besoin d'un téléphone ?

Les téléphones ont colonisé notre vie quotidienne parce qu'on nous a fait croire qu'on a besoin à tout moment de communication *synchrone*. La communication *synchrone*† c'est quand deux personnes communiquent en temps réel, à l'opposé d'une communication *asynchrone*† comme les emails, où les messages sont envoyés à des moments différents. Ce « besoin » a été normalisé, mais cela vaut le coup d'y résister

[9] attaque.noblogs.org/post/2018/12/11/jamais-eteindre-son-telephone-une-nouvelle-approche-a-la-culture-de-la-securite

Réseau Tor

Tor[43] (acronyme pour The Onion Router) est un réseau ouvert et décentralisé qui aide à se protéger des analyses de traffic réseau. Tor te protège en faisant passer tes communications à travers un réseau de relais maintenus par des volontaires à travers le monde : cela empêche une personne qui surveillerait ta connexion Internet de savoir quels sites web tu visites, et cela empêche les administrateurs des sites que tu visites de découvrir ta position géographique.

Chaque visite d'un site web via Tor fait passer par trois relais. Les relais sont des serveurs hébergés par différentes personnes et organisations à travers le monde. Un relai donné ne sait jamais à la fois d'où vient la communication chiffrée ni où elle va. Un extrait d'une évaluation top-secrète de la NSA désigne Tor comme « le roi de l'anonymat sécurisé sur Internet pour des usages en temps réel », « sans concurrents au trône en vue ». On peut accéder au réseau Tor sur n'importe quel système d'exploitation grâce au Navigateur Tor. Le système d'exploitation Tails† force tous les logiciels à passer par le réseau Tor pour accéder à Internet.

Pour plus d'informations, voir Tails for Anarchists[44] et Privacy Guides[45]. Pour comprendre les limites de Tor, voir la documentation de Whonix[46].

Système d'exploitation (OS)

Le logiciel système qui s'exécute sur ton appareil avant tout autre logiciel. Par exemple Windows, macOS, Linux, Android, et iOS. Linux et certaines versions d'Android sont les seules options open-source de cette liste.

[43] torproject.org/
[44] anarsec.guide/posts/tails/#tor
[45] privacyguides.org/fr/advanced/tor-overview/
[46] whonix.org/wiki/Warning

même (données) mais peut aussi contenir des métadonnées comme la date à laquelle le fichier a été créé, le type d'appareil photo, des coordonnées GPS, etc. Les métadonnées peuvent être précieuses pour le piratage (pour trouver des failles dans des logiciels obsolètes utilisés par une cible), pour des agences gouvernementales (pour récolter des informations sur des gens et les relations entre elleux), et d'autres acteurs (pour de la publicité ciblée). Quand tu utilises un ordinateur, tu laisses généralement des métadonnées derrière toi.

Pour plus d'informations, voir Remove Identifying Metadata From Files[38] et Defend Dissent: Metadata[39] (Défendre la contestation : Métadonnées).

Modèle de menaces

La modélisation de menaces est un ensemble d'activités pour améliorer sa sécurité en identifiant un ensemble d'adversaires, d'objectifs de sécurité[35], et de vulnérabilités[35], puis en définissant des contre-mesures pour prévenir ou remédier aux effets des menaces envers un système. Une menace est un évènement possiblement ou assurément non désiré qui peut être malveillant (comme une attaque par déni de service[35]) ou accidentel (comme un disque dur qui meurt). La modélisation de menaces est l'activité délibérée d'identification et d'évaluation des menaces et vulnérabilités.

Pour plus d'informations, voir la Bibliothèque de menaces du No Trace Project[40], Defend Dissent: Digital Threats to Social Movements[41] (Défendre la contestation : Menaces numériques contre les mouvements sociaux) et Defending against Surveillance and Suppression[42] (Se défendre contre la surveillance et la répression).

[38] anarsec.guide/posts/metadata

[39] open.oregonstate.education/defenddissent/chapter/metadata/

[40] notrace.how/threat-library/fr

[41] open.oregonstate.education/defenddissent/chapter/digital-threats/

[42] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/

dans les réseaux anarchistes. L'anarchie ne peut être qu'anti-industrielle[10]. On doit apprendre à vivre sans les commodités qui nous sont vendues par les entreprises de télécommunications, on doit défendre (ou raviver) notre capacité à vivre sans être connecté en permanence à Internet, sans les itinéraires en temps réel d'un GPS, et sans la possibilité de pouvoir toujours changer de plans à la dernière minute.

Si tu décides d'utiliser un téléphone, pour que ce soit aussi difficile que possible pour un adversaire de le localiser, d'intercepter ses messages, ou de le pirater, utilise GrapheneOS[11]. Si on se met d'accord **d'utiliser uniquement des moyens de communication chiffrés[12] pour communiquer avec d'autres anarchistes**, cela exclut les bigos et les téléphones fixes. GrapheneOS est le seul système d'exploitation pour smartphones qui offre un respect de la vie privée et une sécurité raisonnables.

Pour empêcher tes déplacements d'être pistés, considère le smartphone comme un téléphone fixe et laisse le chez toi quand tu sors. Même si tu utilises une carte SIM achetée anonymement, si elle est un jour reliée à ton identité, l'opérateur de téléphonie mobile peut rétroactivement obtenir l'historique de ses données de localisation. Si tu utilises un téléphone en suivant nos recommendations (en le connectant uniquement au Wi-Fi[13] et en le laissant en permanence en mode avion), il ne se connectera pas aux antennes téléphoniques. Cela ne suffit pas de laisser le téléphone chez toi quand tu vas à une réunion, une manif ou une action parce que cela dévierait du motif formé par tes comportements habituels et serait un indice qu'une activité suspecte est en cours sur cette période.

Tu peux choisir de vivre entièrement sans téléphone, si tu penses ne pas avoir besoin d'une « ligne fixe chiffrée ». Les stratégies qui suivent visent à minimiser la dépendance aux téléphones en utilisant des ordi-

[10] theanarchistlibrary.org/library/bismuto-beyond-the-moment#toc1

[11] anarsec.guide/posts/grapheneos/

[12] anarsec.guide/posts/e2ee/

[13] anarsec.guide/posts/grapheneos/#what-is-grapheneos

nateurs à la place (qui permettent aussi des formes de communication synchrone, bien que plus limitées).

Bureaucratie

Il y a beaucoup d'institutions bureaucratiques avec lesquelles on est obligé de communiquer par téléphone : institutions de santé, banques, etc. Il n'y a pas besoin de chiffrer ces communications, donc tu peux utiliser une application de voix sur IP (VoIP)†. Cela te permet de passer des coups de fil par Internet plutôt que par les antennes téléphoniques.

Les applications VoIP disponibles sur ordinateur sont asynchrones car elles ne sonnent pas quand l'ordinateur est éteint — quand tu loupes un appel il faut consulter la boîte vocale. Par exemple, un service comme jmp.chat[14] te donne un numéro VoIP, que tu peux payer en Bitcoin, et tu peux passer des appels avec une application XMPP — par exemple Cheogram[15].

Un numéro VoIP fonctionne généralement pour l'authentification à deux facteurs† (quand un service te demande de recevoir un code aléatoire par SMS pour te connecter). Pour ça, les numéros de téléphone en ligne[16] sont une autre option.

Bien que ce soit souvent plus cher qu'un numéro VoIP, un bigo ou téléphone fixe dédié fonctionne bien aussi pour passer et recevoir des appels « bureaucratiques » depuis chez soi.

Communication

Ne pas avoir de téléphone sur toi en permanence nécessite de changer la manière dont tu sociabilises si tu es déjà pris·e dans la toile[17]. Mini-

[14] kicksecure.com/wiki/Mobile_Phone_Security#Phone_Number_Registration_Unlinked_to_SIM_Card

[15] cheogram.com/

[16] anonymousplanet.org/guide.html#online-phone-number

[17] returnfire.noblogs.org/en-francais/pris-e-s-dans-la-toile

Chiffrement de bout en bout

Les données sont chiffrées[35] lors de leur trajet d'un appareil à un autre — de bout en bout — et ne peuvent être déchiffrées par aucun intermédiaire. Elles ne peuvent être déchiffrées qu'au niveau des deux bouts. Cela diffère du « chiffrement au repos » tel que chiffrement complet du disque[35], où les données stockées sur ton appareil sont chiffrées lorsque l'appareil est éteint. Les deux sont importants !

Pour plus d'informations, voir Encrypted Messaging for Anarchists[36], et Defend Dissent: Protecting Your Communications[37] (Défendre la contestation : Protéger nos communications).

Communication asynchrone

Au contraire de la communication synchrone†, les deux participant·e·s n'ont pas besoin d'être connecté·e·s au même moment. Cela grâce à un serveur qui stocke les messages jusqu'à ce que les destinataires des messages se connectent. C'est le type de communication le plus courant (email, etc.)

Communication synchrone

Contrairement à la communication asynchrone†, les deux participant·e·s doivent être connecté·e·s au même moment. Il n'y a pas besoin de serveurs pour la communication, on dit souvent que c'est « de pair à pair » (*peer to peer*).

Métadonnées

Les métadonnées sont des données qui donnent des informations sur d'autres données. Par exemple, un fichier JPG contient l'image en elle-

[35] anarsec.guide/glossary

[36] anarsec.guide/posts/e2ee/

[37] open.oregonstate.education/defenddissent/chapter/protecting-your-communications

mais de manière bien plus sécurisée qu'un ordinateur Windows classique. Voir Qubes OS for Anarchists[31].

Voir When to Use Tails vs. Qubes OS[32]. Nous ne proposons pas de conseils de « réduction des risques » pour des ordinateurs Windows ou macOS, parce que de tels conseils sont déjà facilement disponibles ailleurs et donnent une fausse impression de vie privée et de sécurité.

Applications de messagerie chiffrées

Voir Encrypted Messaging for Anarchists[33]

Stockage des appareils électroniques

Voir Make Your Electronics Tamper-Evident[34].

Annexe: Glossaire

Authentification à deux facteurs (2FA)

L'authentification à deux facteurs (ou « 2FA ») est une manière pour un utilisateur de s'authentifier auprès d'un fournisseur de services qui impose la combinaison de deux méthodes d'authentification différentes. Ces méthodes peuvent être quelque chose que l'utilisateur sait (comme un mot de passe ou un code PIN) ou que l'utilisateur a (comme une clé matérielle ou un téléphone portable).

[31] anarsec.guide/posts/qubes/
[32] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[33] anarsec.guide/posts/e2ee/
[34] anarsec.guide/posts/tamper/

miser intentionnellement la médiation des écrans dans nos relations sociales est un but précieux en soi.

Utiliser une « ligne fixe chiffrée » pour passer des coups de fil et un ordinateur pour nos communications chiffrées nous permet d'éviter le flot sans fin des notifications sur un appareil toujours à portée de main.

Cela nous ferait beaucoup de bien d'examiner attentivement la monoculture des groupes Signal qui ont remplacé les rencontres en face-à-face dans certains réseaux anarchistes. La culture du smartphone capture nos relations d'organisation et nous force à participer à une longue réunion sans fin relativement facile à surveiller.

Ceci dit, les communications chiffrées peuvent être utiles pour décider d'une date et d'un lieu où se rencontrer, ou pour s'organiser quand on habite loin les un·e·s des autres. Voir Encrypted Messaging for Anarchists[18] (*Applications de messagerie chiffrées pour anarchistes*) pour des options adaptées à un modèle de menace† anarchiste.

Appels d'urgence

C'est souvent possible d'emprunter le téléphone d'un passant dans la rue pour passer un appel d'urgence si on lui dit que notre téléphone n'a plus de batterie. Si on ne peut pas recevoir d'appels d'urgence, on peut prévoir de passer les un·e·s chez les autres ou de s'envoyer des messages chiffrés à des moments convenus à l'avance. Quels scénarios nécessitent vraiment que tu sois disponible pour recevoir un appel à tout moment ? Si c'est le cas dans ta vie, tu peux t'organiser en fonction de ça sans projeter cette urgence sur tous les aspects et moments de ta vie.

[18] anarsec.guide/posts/e2ee/

Itinéraires

Achète une carte papier de la zone et prends-la avec toi. Pour des trajets plus longs ou des trajets pour lesquels tu as besoin d'un itinéraire, note les itinéraires à l'avance avec OpenStreetMap[19].

Musique et podcasts

Ils font toujours des lecteurs MP3 ! Pour un prix bien moindre qu'un téléphone, tu peux écouter de la musique et des podcasts, mais l'appareil n'a ni GPS ni module radio. Ceci dit, ça ne veut pas dire que tu ne peux pas être géolocalisé·e via un lecteur MP3. S'il se connecte au Wi-Fi, la position approximative de ton lecteur MP3 peut être déterminée à partir de son adresse IP.

Annexe : Contre le smartphone

De Fernweh (#24)[20]

Il est toujours avec nous, toujours allumé, peu importe où on est ou ce qu'on fait. Il nous tient informé de tout et de tout le monde : ce que font nos ami·e·s, l'horaire du prochain métro, quel temps il fera demain. Il prend soin de nous, nous réveille le matin, nous rappelle nos rendez-vous importants, et est toujours à notre écoute. Il sait tout sur nous, quand est-ce qu'on se couche, où on est et quand, avec qui on communique, qui sont nos meilleur·e·s ami·e·s, quelle musique on écoute, quels sont nos hobbies. Et tout ce qu'il demande c'est un peu d'électricité de temps en temps ?

Quand je me promène ou que je prends le métro, tout le monde en a un, et personne ne tient plus de quelques secondes sans aller frénétiquement le chercher dans sa poche, le téléphone est sorti, un message est envoyé, un email lu, une photo likée. Il est rangé, petite pause, et

[19] openstreetmap.org/
[20] fernweh.noblogs.org/texte/24-ausgabe/gegen-das-smartphone/

Ton téléphone

Système d'exploitation† : **GrapheneOS** est le seul choix suffisamment sécurisé pour les téléphones portables. Voir GrapheneOS for Anarchists[26]. Si tu décides d'avoir un téléphone, traite-le comme une « ligne fixe chiffrée » et laisse-le chez toi quand tu sors. Voir Tue le flic dans ta poche[27].

Ton ordinateur

Système d'exploitation† : **Tails** est hors pair pour un usage sensible des ordinateurs (écrire et envoyer des communiqués, administrer un site web sensible, faire des recherches pour des actions, lire des articles qui peuvent être criminalisés, etc.) Tails démarre depuis une clé USB et est conçu pour ne pas laisser de traces sur l'ordinateur sur lequel tu l'utilises, ainsi que pour forcer toutes les connexions Internet via le réseau Tor†. Voir Tails for Anarchists[28] et Tails Best Practices[29].

Système d'exploitation† : **Qubes OS** est plus sécursé que Tails pour de nombreuses utilisations, mais a une courbe d'apprentissage plus raide et n'est pas conçu pour ne pas laisser de traces sur l'ordinateur. Ceci dit, il est quand même utilisable par des journalistes et autres personnes sans connaissances techniques poussées. Savoir à peu près utiliser Linux est nécessaire — voir Linux Essentials[30]. Qubes OS peut même faire tourner des logiciels Windows comme Adobe InDesign,

[26] anarsec.guide/posts/grapheneos/
[27] anarsec.guide/fr/posts/nophones/
[28] anarsec.guide/posts/tails
[29] anarsec.guide/posts/tails-best/
[30] anarsec.guide/posts/linux

La communication directe entre individus autonomes est la base de toute rébellion partagée, c'est le point de départ de rêves partagés et de luttes communes. Sans communication directe, toute lutte contre ce monde et pour la liberté est impossible.

Donc débarrassons-nous du smartphone et rencontrons-nous en face-à-face dans une insurrection contre ce monde ! Devenons incontrôlables !

Annexe: Recommendations

En tant qu'anarchistes, nous devons nous défendre contre la police et les agences de renseignement qui utilisent la surveillance numérique ciblée[21] pour nous incriminer[22] et cartographier nos réseaux[23]. Notre but est de dissimuler nos vies et projets à l'État. Ces recommendations sont destinées à tous les anarchistes, et sont accompagnées de guides permettant de les mettre en pratique.

Nous sommes d'accord avec la conclusion d'une revue de mesures de surveillance ciblées en France[24] : « Que chacun se le tienne donc pour dit en termes de responsabilités : lorsqu'on introduit volontairement un tel objet connecté doté de micro et/ou caméra (téléphone portable, babyphone, ordinateur, GPS de voiture, montre connectée, etc.), même éteint, près d'une conversation où des »paroles sont prononcées à titre privé ou confidentiel" et doivent le rester, on devient soi-même un potentiel mouchard d'État…"

Sur le même sujet, on pourra également lire les « Bonnes pratiques numériques »[25] de la Bibliothèque de menaces.

[21] notrace.how/threat-library/fr/techniques/targeted-digital-surveillance.html
[22] notrace.how/threat-library/fr/tactics/incrimination.html
[23] notrace.how/threat-library/fr/techniques/network-mapping.html
[24] sansnom.noblogs.org/archives/16942
[25] notrace.how/threat-library/fr/mitigations/digital-best-practices.html

on recommence, consultant les nouvelles du jour et ce que font nos ami·e·s…

Il est avec nous aux toilettes, au travail ou à l'école, et il aide apparemment à surmonter l'ennui quand on attend, on travaille, etc. Serait-ce peut-être une raison du succès de tous ces appareils technologiques, que la vraie vie est si ennuyeuse et monotone que quelques centimètres carrés d'écran sont presque toujours plus excitants que le monde et les personnes qui nous entourent ? Est-ce qu'il est comme une addiction (les gens ont clairement des symptômes de manque…) ou est-ce qu'il fait désormais partie de notre corps ? Sans lui, on perd nos repères et on a l'impression que quelque chose manque ? Donc ce n'est plus juste un outil ou un jouet, mais une partie de nous qui exerce aussi un certain contrôle sur nous, à laquelle on s'adapte, par exemple, en ne sortant pas de chez soi sans une batterie pleine ? Est-ce que le smartphone est la première étape qui brouillera la frontière entre humain et machine ?

Quand on voit ce que les technocrates en tout genres prophétisent (lunettes connectées Google, puces implantées, etc.), on dirait presque qu'on est en voie de devenir des cyborgs, des gens avec des smartphones implantés qu'on contrôle par la pensée (jusqu'à ce que nos pensées elles-même soient enfin contrôlées). Ce n'est pas surprenant que les médias, porte-paroles de la domination, ne nous montrent que les aspects positifs de cette évolution, mais c'est choquant que presque personne ne questionne cette vision. C'est probablement le rêve de tout chef d'État : pouvoir contrôler les pensées et actions de chacun et intervenir immédiatement en cas de problème. Des abeilles ouvrières complètement contrôlées et surveillées qu'on récompense par un peu de fun (virtuel) pendant que quelques-uns profitent.

Avec les immenses quantités de données facilement accessibles à propos de tout et de tout le monde à tout moment, le contrôle social et la surveillance ont atteint de nouveaux sommets. Cela va bien plus loin que la surveillance des téléphones et des SMS (comme on a pu voir pendant les émeutes de 2011 au Royaume-Uni). L'accès à une telle

quantité d'informations permet aux agences de renseignement de définir ce qui est « normal ». Ils peuvent déterminer quels endroits sont « normaux » pour nous, quels contacts sont « normaux », etc. En bref, ils peuvent repérer rapidement et presque en temps réel si des gens dévient de leur comportement « normal ». Cela donne un immense pouvoir à certaines personnes, qui est utilisé à chaque opportunité (pour surveiller les gens). La technologie fait partie du pouvoir, provient du pouvoir et a besoin du pouvoir. Il faut un monde dans lequel des individus ont un pouvoir extrême pour permettre la production de quelque chose comme le smartphone. Toute technologie est un produit du monde oppressif actuel, fait partie de lui, et le renforce.

Dans le monde d'aujourd'hui, rien n'est neutre. À ce jour, tout ce qui a été ou est développé est conçu pour étendre le contrôle et faire de l'argent. De nombreuses innovations de ces dernières décennies (comme le GPS, l'énergie nucléaire, ou Internet) proviennent même directement de l'armée. La plupart du temps ces deux aspects vont main dans la main, mais le « bien-être de l'humanité » n'est certainement pas une motivation, surtout dans ce qui est développé par l'armée.

Peut-être que prendre l'exemple de l'architecture peut mieux illustrer quelque chose d'aussi complexe que la technologie : prenons une prison vide et désaffectée, que peut-on faire de cette structure sinon la détruire ? Son architecture même, ses murs, ses miradors, ses cellules, contiennent déjà la raison du bâtiment : emprisonner des gens et les détruire psychologiquement. Cela serait impossible pour moi de vivre là, parce que le bâtiment même est oppressif.

De la même manière, les technologies d'aujourd'hui nous sont présentées comme un progrès visant à nous faciliter la vie. Elles ont été conçues dans le but de faire de l'argent et de nous contrôler, et auront toujours cela en elles. Peu importe les bénéfices supposés que tu retires de ton smartphone, ceux qui s'enrichissent en collectant tes données et en te surveillant vont toujours retirer plus de bénéfices.

Si par le passé on disait que « la connaissance c'est le pouvoir », aujourd'hui on pourrait dire que « l'information c'est le pouvoir ».

Plus les chefs en savent sur leurs troupeaux, mieux ils peuvent les dominer — ainsi, la technologie dans son ensemble est un outil de contrôle puissant pour prévoir et donc empêcher les gens d'attaquer ensemble ce qui les oppresse.

Ces smartphones ont l'air d'avoir besoin d'un peu plus que juste un peu d'électricité… Au sein de notre génération, qui a au moins connu un monde sans smartphones, il y a peut-être encore quelques personnes qui comprennent ce dont je parle, qui savent encore ce que c'est que d'avoir une conversation sans vérifier son téléphone toutes les trente secondes, de se perdre et découvrir de nouveaux endroits, ou de débattre sans demander immédiatement la réponse à Google. Mais je ne veux pas revenir au passé, même si ce ne serait de toute façon pas possible. Mais plus la technologie pénètre nos vies, plus cela semble difficile de la détruire. Et si nous étions une des dernières générations à pouvoir empêcher l'évolution des êtres humains en machines entièrement contrôlées ?

Et si à un moment on devient incapables d'inverser cette évolution ? L'humanité a atteint une nouvelle étape historique dans le domaine de la technologie. Une étape où elle est capable d'annihiler toute vie humaine (énergie nucléaire) ou de la modifier (manipulation génétique). Ce fait démontre une fois de plus la nécessité d'agir aujourd'hui pour détruire cette société. Pour ça, on a besoin de se rencontrer les un·e·s les autres et d'échanger des idées.

N'est-ce pas évident que si, au lieu de se parler les un·e·s aux autres, on communique uniquement par messages de cinq phrases ou moins, cela aura des effets sur le long terme ? Apparemment non. Tout d'abord, la manière dont on pense influence la manière dont on parle, et inversement — la manière dont on parle et communique influence la manière dont on pense. Si on est seulement capable d'échanger des messages courts et concis, comment peut-on discuter d'un monde complètement différent ? Et si on ne peut même pas discuter d'un autre monde, comment l'atteindre ?