CSRC *BULLETIN #1*

Ceci est le premier numéro d'une publication irrégulière du **Centre de documentation sur la contre-surveillance***, une base de données de ressources sur comment déjouer la surveillance ciblée. Une version de ce texte avec citations et hyperliens est disponible en ligne à l'adresse* **csrc.link/fr***, publié en mars 2023.*

CONTRE LA SURVEILLANCE CIBLÉE, COORDINATION INTERNATIONALE

On est des anarchistes. On croit en une coordination internationale de groupes anarchistes informels pour poursuivre la lutte contre toutes les formes de domination. On croit que le partage des connaissances sur les capacités et les tactiques de nos ennemis devrait être une partie importante de cette coordination. La connaissance n'est pas une fin en soi mais un moyen de limiter les risques de se faire prendre, afin de pouvoir continuer à attaquer.

Nos ennemis ont des capacités importantes et des tactiques perfectionnées. De leur côté, iels ont les institutions policières et judiciaires, les scientifiques et les technocrates, et dans certains cas, le soutien de la majorité de la population. Iels contrôlent de vastes réseaux d'infrastructures. Iels ont une mémoire infinie, des archives et des bases de données ADN.

De notre côté, on a la nature informelle et décentralisée de nos organisations, les ombres pour se cacher, et la solidarité pour s'entraider dans les moments difficiles, pour continuer les combats des camarades qui ne peuvent plus le faire.

"*Quoi qu'il arrive, nous faisons et continuerons à faire des erreurs dans la lutte contre des mécanismes d'oppression aussi puissants. Des erreurs qui "coûteront" toujours plus cher par rapport aux erreurs des flics qui sont "absorbées". Nous devons évaluer à nouveau les situations et veiller à ce que les erreurs commises une fois ne se reproduisent plus. Nous devons étudier et apprécier l'expérience accumulée depuis tant d'années et, en tenant compte de la tendance à se préparer pour les batailles qui ont déjà eu lieu et non pour celles qui viendront, soyons prêt.e.s et que la chance soit de notre côté...*"

—camarades anarchistes de Grèce, dans un texte détaillant la surveillance qui a conduit à leurs arrestations, 2013

Nos ennemis s'organisent déjà au niveau international ; iels partagent des informations, des tactiques et des développements technologiques et scientifiques. C'est regrettable, mais ça signifie aussi qu'un rapport rédigé par des camarades dans un pays—sur, par exemple, une bonne façon d'éliminer les traces ADN, ou un micro-espion trouvé dans un squat, ou un outil pas cher pour abattre les drones de la police—pourrait aider d'autres personnes n'importe où dans le monde.

Certes, tout ne doit pas être partagé publiquement. Parfois, des informations encore inconnues de nos ennemis doivent rester secrètes en fonction d'une stratégie ou d'un plan spécifique. Mais sinon : partageons nos connaissances et nos expériences, et organisons-nous !

UNE BASE SUR LAQUELLE S'APPUYER : DISTINGUER LA SÉCURITÉ OPÉRATIONNELLE (OPSEC) ET LA CULTURE DE LA SÉCURITÉ

Parfois, des termes apparentés deviennent des synonymes, et parfois ça peut être bien. Le français en est rempli, comme "super" et "génial"—la différence entre ces mots ne manque à personne.

Mais parfois, laisser s'estomper la différence entre les termes nous fait aussi perdre un élément de sens utile. La sécurité opérationnelle (OpSec) et la culture de la sécurité sont deux termes qui ont des significations similaires

ON PRÉSENTE : LA THREAT LIBRARY

L'objectif de la toute nouvelle Threat Library du CSRC est simple : examiner l'éventail des techniques répressives de l'État afin de mieux les déjouer. Cette "bibliothèque" documente deux douzaines de techniques de maintien de l'ordre différentes, les divisant en trois tactiques (dissuasion, incrimination et arrestation) et proposant pour chacune d'elles des mesures d'atténuation (*mitigations*) potentielles, c'est-à-dire des moyens de limiter les dégâts. Elle établit également un lien entre ces techniques et des opérations répressives spécifiques menées par les États contre des anarchistes au cours des deux dernières décennies.

La Threat Library est destinée à vous aider à "établir un modèle de menace", processus par lequel vous essayez de comprendre quels types de mesures l'État est susceptible de prendre contre vous afin de vous y préparer. Il est préférable de faire cet exercice en collaboration avec les camarades avec lesquel.le.s vous travaillez sur un projet spécifique. Un bon modèle de menace peut transformer la peur ou la paranoïa en courage, en nous donnant une idée précise de ce à quoi nous sommes confronté.e.s afin que nous puissions prendre des précautions. En d'autres termes, cela nous aide à décider de la sécurité opérationnelle (OpSec) appropriée. Le CSRC suggère d'utiliser la Threat Library pour créer des "arbres d'attaque" (*attack trees*). "Les arbres d'attaque sont un outil permettant de faciliter un brainstorming collectif sur les différentes façons dont un adversaire pourrait réussir à vous attaquer dans un contexte donné, en représentant les attaques sous la forme d'un arbre." Consultez le tutoriel de la Threat Library pour obtenir un guide étape par étape sur leur utilisation.

La Threat Library peut aussi être consultée en dehors de l'établissement d'un modèle de menace. Supposons que les anarchistes de ma région ont l'habitude de faire face à des infiltré.e.s ou des indics qui tentent de briser leur organisation. Dans l'onglet "Incrimination", je sélectionne "Infiltrators". En 300 mots, l'entrée liste cinq principaux types d'infiltré.e.s et propose trois mesures d'atténuation possibles (l'attaque, le principe *need-to-know*, et un exercice consistant à faire une carte de nos relations sociales). Si je clique sur le lien "infiltrators topic", j'obtiens une liste de 27 textes écrits par des anarchistes sur des infiltré.e.s dans leurs réseaux. Ma peur des infiltré.e.s est atténuée par la connaissance des signes spécifiques à rechercher et par des outils pratiques pour renforcer mes réseaux de confiance.

Avec des sujets allant des visites domicilaires (*Door knocks*) aux perquisitions (*House raids*) en passant par la criminalistique (*Forensics*), la Threat Library vise à être complète tout en restant brève et pertinente. Le CSRC dispose d'une énorme quantité d'informations sur la répression et la façon d'y faire face. La Threat Library résume et trie toutes ces informations pour qu'elles soient pratiques et faciles à analyser. La Threat Library est disponible en format brochure pour faciliter sa lecture et sa distribution.

Est-ce qu'il y a une technique, une mesure d'atténuation ou une opération répressive qui manque ? Est-ce que vous voulez modifier une technique actuellement répertoriée ? Pour agrandir, améliorer, critiquer ou commenter la Threat Library, contactez-nous.

mais distinctes, et les deux sont des éléments nécessaires de la pratique anarchiste de la sécurité contre la répression.

L'OpSec fait référence aux pratiques spécifiques utilisées pour éviter de se faire prendre pour une action ou un projet donné. Certaines pratiques d'OpSec incluent porter des gants et des masques, changer de chaussures, des mesures pour éviter de laisser de l'ADN, des vêtements de black bloc, l'utilisation de Tails pour un accès anonyme à Internet, et ainsi de suite. L'OpSec se situe au niveau de l'action ou du projet. Ces pratiques peuvent être enseignées, mais en fin de compte, seules les personnes qui réalisent ensemble un projet spécifique doivent se mettre d'accord sur les pratiques d'OpSec à utiliser.

Selon *Assurance, courage, lien, confiance*[1] : "La culture de sécurité fait référence à un ensemble de pratiques développées pour évaluer les risques, pour contrôler les flux d'informations dans nos réseaux et pour construire des relations fortes pour la lutte." La culture de la sécurité intervient au niveau de la relation ou du réseau. Pour être efficaces, ces pratiques doivent être partagées aussi largement que possible.

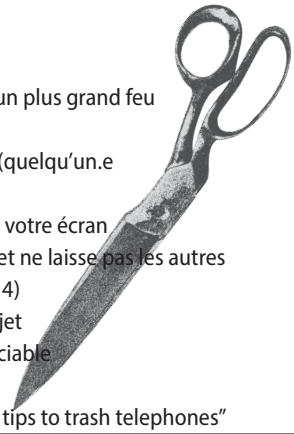
À première vue, l'OpSec peut sembler plus importante. Si nous avons les pratiques dont nous avons besoin pour être en sécurité, pense-t-on, alors qu'importe ce que font les autres personnes du milieu ? De nombreu.x.ses anarchistes sont (à juste titre) sceptiques à l'égard des milieux et ne se considèrent pas comme connecté.e.s ou dépendant.e.s de personnes avec lesquelles iels n'ont pas d'affinités. Beaucoup d'énergie dans l'espace anarchiste est consacrée au perfectionnement de l'OpSec, ce qui semble approprié, puisque si vous voulez mener une action offensive, il est préférable de ne pas se faire prendre. Cependant, la culture de la sécurité est également importante, et une bonne OpSec ne la remplace pas. Elle fournit le contexte social—la base—sur lequel repose toute notre activité. En effet, que nous le voulions ou non, nous sommes toutes intégré.e.s dans des réseaux, et le prix à payer pour s'en couper complètement est élevé. Sans une base stable, il est beaucoup plus difficile d'agir en toute sécurité.

Pour en revenir à *Assurance, courage, lien, confiance*, les auteur.ice.s écrivent que la culture de la sécurité ne consiste pas à se fermer, mais à trouver des moyens de rester ouvert aux connexions avec les autres en toute sécurité. Cela implique d'avoir des conversations honnêtes sur les risques et de définir des normes de base avec des réseaux plus larges que les seules personnes avec lesquelles nous avons l'intention d'agir. La culture de la sécurité n'est pas statique—il ne s'agit pas seulement d'un ensemble de règles que les membres des milieux "radicaux" doivent connaître. Elle doit être dynamique, fondée sur des conversations permanentes et sur notre meilleure analyse des modèles de répression actuels.

Des pratiques telles que le *vouching* (établir des réseaux de confiance en se cautionnant entre nous), cartographier nos relations sociales et se renseigner sur le passé des gens peuvent sembler relever de l'OpSec et constituer un élément important de la planification de certaines actions, mais elles sont issues de la culture de la sécurité. La culture de la sécurité consiste à se demander "ce qu'il faudrait pour que je te fasse confiance". Cela ne signifie pas que vous devez cautionner toutes les personnes que vous connaissez ou que vous ne passez pas de temps avec les personnes que vous ne cautionnez pas, mais simplement que vous savez clairement à qui vous faites confiance pour quoi et pourquoi, et que vous disposez de mécanismes pour apprendre à faire confiance à de nouvelles personnes en toute sécurité.

Aucune bonne habitude sur la façon de parler des actions qui se produisent dans votre ville (culture de la sécurité) ne vous protégera si vous laissez de l'ADN sur la scène de crime (OpSec), et aucune détection de la surveillance physique (OpSec) ne vous protégera du flic infiltré qui s'est lié d'amitié avec votre colocataire afin de se rapprocher de vous (culture de la sécurité). Les pratiques d'OpSec et de culture de sécurité sont distinctes et l'une ne remplace pas l'autre. En développant une compréhension plus approfondie des deux cadres, on peut essayer de se maintenir hors de prison tout en continuant à créer des liens et à étendre les réseaux informels d'affinité.

DIX ASTUCES POUR CASSER LES TÉLÉPHONES



1. mets le feu à ton téléphone
2. jette ton téléphone dans le canal
3. mets les téléphones de tes amis dans un plus grand feu
4. jette tous les téléphones dans le canal
5. n'apporte pas toujours ton téléphone (quelqu'un.e pourrait le jeter dans le feu)
6. parlez-vous les un.e.s aux autres, pas à votre écran
7. détruis les preuves (c.f. astuces 1 et 2) et ne laisse pas les autres fabriquer des preuves (c.f. astuces 3 et 4)
8. fais de l'utilisation du téléphone un sujet
9. sois injoignable par téléphone, sois sociable
10. nique la technologie

—*Rumoer n°5*, "Ten tips to trash telephones"

1. csrc.link/#confidence-courage-connection-trust

EXTRAITS CONTRE LA SURVEILLANCE

Dans cette section, on veut partager avec vous de courts extraits qui relèvent des sujets couverts par le CSRC, mais qui ne justifient pas une entrée distincte sur notre site web. Vous pouvez nous envoyer de tels extraits si vous souhaitez qu'ils soient publiées dans le prochain numéro.

• En 2021, plusieurs personnes ont été arrêtées en France suite à l'incendie de véhicules appartenant à Enedis et d'une importante antenne-relais. Un texte détaille l'éventail intéressant de techniques de surveillance qui ont précédé leurs arrestations : filature, prélèvement ADN sur la poignée d'une voiture pendant que son propriétaire faisait des courses, entrée dans un domicile la nuit pour installer un keylogger sur un ordinateur, demande à Enedis de fournir la liste des personnes qui ont refusé l'installation du compteur Linky, et demande à un journal local de fournir les adresses IP qui ont accédé à leur article sur l'incendie.

• En 2022, deux anarchistes ont été arrêté.e.s en Italie et accusé.e.s de fabrication et de possession de matériel explosif. Un texte explique que l'enquête qui a conduit aux arrestations a commencé lorsqu'un "inconnu" a trouvé du matériel explosif, du matériel électrique et d'autres dispositifs dans une forêt en juin 2021. Par la suite, les flics ont installé des pièges photo/vidéo pour "capturer" toute personne qui s'approchait de la zone. Une personne a ainsi été photographiée de dos près de l'endroit, et les flics ont prétendu l'avoir reconnue et identifiée.

• Pour terminer cette section, voici une citation pleine d'espoir d'un communiqué revendiquant la responsabilité de l'incendie d'un bâtiment de constructeurs de prisons en Allemagne : "*Afin de ne pas produire de bonnes images sur les caméras de surveillance, nous portions des K-ways pour dissimuler la forme de nos corps et nos démarches. Pour rendre la forme de nos têtes méconnaissable, nous avons utilisé des chapeaux. Le développement des techniques d'analyse vidéo inquiète de nombreu.x.ses camarades. Avec ces conseils nous voulons montrer les possibilités de résister contre cette technique de surveillance.*"

CONTRIBUEZ AU CSRC !

Nous proposons d'utiliser notre site web pour faciliter le partage de connaissances et d'expériences entre camarades sur le thème de la surveillance ciblée. Parcourez nos plus de 180 ressources sur **csrc.link**, également accessible dans le navigateur Tor via une adresse .onion. Imprimez nos tout nouveaux stickers et diffusez-les autour de vous. Contribuez en nous envoyant un email à **csrc@riseup.net**—si vous voulez chiffrer, notre clé PGP est disponible en ligne à l'adresse **csrc.link/csrc.asc**