CSRC *Bulletin Nr. 1*

Dies ist die erste Ausgabe einer unregelmäßig erscheinenden Publikation des **Counter-surveillance resource center***, eine Datenbank von Hilfsmitteln zur Umgehung zielgerichteter Überwachung. März 2023.* **csrc.link/de**

INTERNATIONALE KOORDINATION GEGEN ZIELGERICHTETE ÜBERWACHUNG

Wir sind Anarchist.innen. Wir glauben an eine internationale Koordination informeller anarchistischer Gruppen, um dem Kampf gegen jegliche Formen der Herrschaft nachzugehen. Wir glauben, dass das gegenseitige Teilen von Kenntnis über Fähigkeiten und Taktiken unserer Feind.innen einen bedeutenden Teil dieser Koordination bilden sollte. Die Kenntnis ist kein Selbstzweck, sondern ein Mittel zur Begrenzung der Aussichten gefasst zu werden, damit wir weiter angreifen können.

Unsere Feind.innen sind im Besitz von außerordentlichen Einsatzmöglichkeiten und perfektionierten Taktiken. Auf ihrer Seite steht die Polizei und das Justizsystem, die Wissenschaftler.innen und Technokrat.innen, und in manchen Fällen die Unterstützung der allgemeinen Bevölkerung. Sie kontrollieren riesige Infrastrukturnetze. Sie haben unendliche Erinnerungsvermögen, Archive und DNA-Datenbanken. Auf unserer Seite befindet sich das informelle und dezentrale Wesen unserer Organisationen, Schatten, in denen wir uns verstecken, und Solidarität, mit der wir einander in schwierigen Zeiten helfen, damit die Kämpfe von Gefährt.innen weitergeführt werden, wenn diese selbst es nicht mehr tun können.

"*Egal was passiert, wir machen Fehler und uns werden auch weiterhin im Kampf gegen solch starke unterdrückerische Mechanismen Fehler unterlaufen. Fehler, die uns immer mehr „kosten" werden, im Vergleich zu den Fehlern der Bullerei, die „neutralisiert" werden. Wir müssen geschehene Situationen wieder prüfen und sicherstellen, dass die Fehler, die einmal passiert sind, ganz einfach nicht wieder vorkommen können. Wir müssen die angesammelten Erfahrungen von so vielen Jahren studieren und wertschätzen, unter der Beachtung der Tendenz, sich für bereits stattgefundene Kämpfe vorzubereiten; anstatt für jene, die noch kommen werden. Seien wir vorbereitet und möge Glück auf unserer Seite sein...*"

—Anarchistische Gefährt.innen aus Griechenland, aus einem Text aus dem Jahr 2013, der ausführlich über die Überwachung berichtet, die zu ihren Verhaftungen geführt hatte.

Unsere Feind.innen organisieren sich bereits auf einem internationalen Niveau: Sie teilen Informationen, Taktiken, und technologische und wissenschaftliche Entwicklungen. Das ist bedauerlich, aber es bedeutet auch, dass ein Bericht von Gefährt.innen in einem Land – über, sagen wir mal, eine gute Art und Weise im Umgang mit DNA-Spuren, oder eine gefundene Wanze in einem besetzten Haus, oder ein billiges Werkzeug für das Abschießen einer Drohne der Polizei – anderen irgendwo sonst auf der Welt helfen könnte. Gewiss sollte nicht alles öffentlich geteilt werden. Manchmal sollten Informationen, die unseren Feind.innen noch unbekannt sind, mit der Grundlage einer spezifischen Strategie oder eines bestimmten Planes geheim bleiben. Aber im Übrigen: Lasst uns die Kenntnis und die Erfahrungen teilen, und uns selbst organisieren!

EINE GRUNDLAGE, AUF DER WIR STEHEN KÖNNEN: DIE UNTERSCHEIDUNG ZWISCHEN OPSEC UND SICHERHEITSKULTUR

Manchmal werden verwandte Begriffe zu Synonymen, und manchmal kann das auch in Ordnung sein. Aber manchmal, wenn wir es uns erlauben den Unterschied zwischen Begriffen zu verlieren, dann veranlasst dies uns auch dazu, ein nützliches Stück an Bedeutung zu verlieren. Operative Sicherheit (OpSec) und Sicherheitskultur sind zwei Begriffe, die ähnliche aber unterschiedliche Bedeutungen in sich tragen, und beide sind notwendige Teile einer anarchistischen Sicherheitspraxis gegen Repression.

ANKÜNDIGUNG: DIE BEDROHUNGSBIBLIOTHEK

Das Ziel der neulich herausgegebenen Bedrohungsbibliothek [Threat Library] des Counter-Surveillance Ressource Centers ist einfach: Den Blick auf die staatliche Aufstellung der repressiven Techniken richten, mit dem Zweck, diese durch geschicktes Manövrieren zu überlisten. Die Bibliothek dokumentiert zwei Dutzend verschiedene Überwachungs- und Kontrollmethoden, aufgeteilt in drei Taktiken (Abschreckung [Deterrence], Belastung [Incrimination] und Verhaftung [Arrest]) und offeriert potenzielle Abschwächung, das heißt, Arten und Weisen der Schadensbegrenzung, für jede.n Einzelne.n. Sie verbindet zudem Methoden mit spezifischen repressiven Operationen, die vom Staat gegen Anarchist.innen in den letzten paar Jahrzehnten ausgeführt wurden.

Die Bedrohungsbibliothek ist dafür gedacht, dir beim Erstellen eines Bedrohungsmodells Hilfe zu leisten, ein Prozess, durch den du versuchst zu verstehen, was für Arten von Maßnahmen der Staat voraussichtlich gegen dich ausführen wird, damit du dich auf diese vorbereiten kannst. Es wird am besten gemeinschaftlich mit den Gefährt.innen erstellt, mit denen du an einem bestimmten Projekt zusammenarbeitest. Ein gutes Bedrohungsmodell kann Angst oder Paranoia zu Mut umwandeln, indem es uns eine genaue Vorstellung über das liefert, was wir bekämpfen, und wir somit Schutzmaßnahmen treffen können. Mit anderen Worten hilft es uns, über angemessene Operative Sicherheit (OpSec) zu entscheiden. Das CSRC empfiehlt die Bedrohungsbibliothek auf eine Weise zu verwenden, mit der „Angriffsbäume" erstellt werden können. „Angriffsbäume sind ein Werkzeug, das eine kollektive Ideensammlung darüber vereinfacht, wie ein.e Gegner.in einen erfolgreichen Angriff auf dich innerhalb eines gegebenen Kontexts auf verschiedene Arten und Weisen ausführen könnte, indem die Angriffe mit der Struktur eines Baumes dargestellt werden". Schau in der Anleitung [Tutorial] zur Bedrohungsbibliothek für einen Schritt-für-Schritt-Leitfaden nach.

Die Bedrohungsbibliothek kann auch zur Navigation von Hilfsmitteln außerhalb der Erstellung eines Bedrohungsmodells verwendet werden. Nehmen wir an, dass Anarchist.innen in meiner Umgebung eine Geschichte von Spion.innen und Informant.innen teilen, die zur Zerschlagung unserer Organisierung zum Einsatz kommen. Auf der Webseite wähle ich in der Bedrohungsbibliothek in der Spalte „Belastungen" [Incrimination] das Thema „Spion.innen" [infiltrators] aus. Mit weniger als 300 Wörtern teilt der Eintrag in fünf hauptsächliche Typen von Spion.innen auf, und offeriert drei mögliche Formen der Abschwächung (Angriff [Attack], Need-to-know-Prinzip, d.h. „Kenntnis nur, wenn nötig", und Netzwerkvisualisierung [Network map exercise]). Wenn ich auf die Schaltfläche „Thema Spion.innen" [infiltrators topic] klicke, erhalte ich eine Liste von 27 Texten, geschrieben von Anarchist.innen, die von Spion.innen in deren Netzwerken handeln. Meine Angst vor Spion.innen wird gelindert, indem ich einerseits die genauen Anzeichen kenne, nach denen ich Ausschau halten sollte und andererseits praktische Werkzeuge zur Stärkung meiner Vertrauensnetzwerke kenne.

Mit Themen, die von Türeklopfen über Hausdurchsuchungen bis zu Spurensicherungen reichen, zielt die Bedrohungsbibliothek darauf ab, umfassend und zugleich kurz und prägnant zu sein. Das CSRC bietet eine riesige Menge an Informationen zu Repression und wie damit Umgegangen werden kann, und die Bedrohungsbibliothek fasst sie alle für dich zusammen und sortiert sie, damit diese auf praktische und einfache Art und Weise analysiert werden können. Die Bedrohungsbibliothek ist im Broschürenformat für einfaches lesen und verteilen erhältlich.

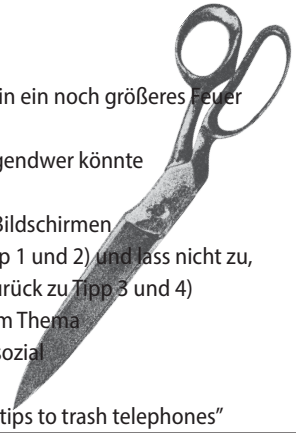
Gibt es eine Methode, eine Abwehrstrategie oder eine repressive Operation, von der du denkst, dass sie fehlt? Möchtest du einen derzeitig aufgelisteten Eintrag editieren? Um etwas hinzuzufügen, zu verbessern, und Kritik oder Feedback zur Bedrohungsbibliothek mit uns zu teilen, nimm mit uns Kontakt auf, via **csrc@riseup.net**

OpSec verweist auf die spezifische Praxis, die genutzt wird, um es zu vermeiden, bei einer bestimmten Aktion oder einem bestimmten Projekt erwischt zu werden. Einige OpSec-Vorgehensweisen beinhalten das Tragen von Handschuhen und Masken, die Verwendung von unterschiedlichen Schuhen, die Maßnahmen, die es verhindern DNA-Spuren zu hinterlassen, Schwarzerblock-Kleidung, die Verwendung von Tails für den anonymen Zugriff auf das Internet, und so weiter. OpSec bewegt sich auf dem Niveau der Aktion oder des Projekts. Diese Vorgehensweisen können beigebracht werden, aber letztlich müssen bloß die Menschen, die sich dazu entscheiden gemeinsam ein bestimmtes Projekt umzusetzen, sich darauf einigen, welche OpSec-Vorgehensweisen sie nutzen wollen.

Gemäss *Confidence Courage Connection Trust*[1] verweist die Sicherheitskultur „auf eine Reihe von entwickelten Vorgehensweisen, die zur Beurteilung von Risiken, zur Kontrolle des Informationsflusses durch deine Netzwerke, und zur Schaffung von soliden organisierenden Beziehungen dienen." Die Sicherheitskultur ereignet sich auf dem Niveau der Beziehung oder des Netzwerks. Damit sie effizient sind, sollten diese Vorgehensweisen so weit verbreitet werden, wie möglich. Auf den ersten Blick mag OpSec als wichtiger erscheinen. Wenn wir die Praxis haben, die wir zur Sicherheit benötigen, so die Überlegung, was spielt es dann für eine Rolle, was andere Menschen im Milieu anstellen? Viele Anarchist.innen stehen Milieus (zu Recht) skeptisch gegenüber, und verstehen sich selbst nicht damit verbunden oder angewiesen auf Menschen, mit denen sie keine enge Affinität teilen. Innerhalb des anarchistischen Raums geht viel Energie in die Perfektionierung von OpSec, was als angemessen erscheint, da es vorzuziehen ist, nicht erwischt zu werden, wenn du eine offensive Aktion umsetzen willst. Allerdings ist auch die Sicherheitskultur wichtig, und gutes OpSec ist kein Ersatz dafür. Sie stellt den sozialen Kontext zur Verfügung – die Grundlage – auf der all unsere Aktivitäten aufgebaut sind. Denn ob es dir nun gefällt oder nicht, wir sind alle in Netzwerke eingebettet, und der Preis, den du für das komplette Abtrennen davon bezahlst, ist hoch. Ohne eine stabile Grundlage ist es viel schwieriger auf sichere Art und Weise zu handeln.

Um auf „Confidence Courage Connection Trust" zurückzukommen: Die Autor.innen schreiben, dass es bei Sicherheitskultur nicht darum geht, sich zu verschließen, sondern Wege zu finden, die es erlauben auf sichere Art und Weise gegenüber Verbindungen mit anderen offen zu bleiben. Dies beinhaltet ehrliche Gespräche über Risiken und das Festlegen von grundsätzlichen Normen mit breiteren Netzwerken als bloß den Menschen, mit denen wir beabsichtigen zu handeln. Sicherheitskultur stagniert nicht – sie ist nicht bloß eine Reihe von Regeln, die Menschen in „radikalen" Subkulturen kennen sollten. Sie muss dynamisch sein, auf der Grundlage von andauernden Gesprächen und unseren besten Analysen über gegenwärtige Respressionsmuster. Vorgehensweisen wie das Bürgen für eine Person, die Netzwerkvisualisierung, und Hintergrundüberprüfungen könnten den Eindruck erwecken, sie seien Teil der OpSec, und sie mögen einen wichtigen Teil innerhalb einer Planung von bestimmten Aktionen darstellen, aber sie entspringen der Sicherheitskultur. Die Sicherheitskultur beinhaltet die Frage „Was würde es für mich bedeuten, dir zu vertrauen?". Das bedeutet nicht, dass du für alle, die du kennst bürgen musst oder dass du keine Zeit mit den Menschen verbringst, für die du nicht deine Hand ins Feuer legen würdest. Es geht darum, dass du dir dabei sicher bist, wem du wofür vertraust, und weshalb, und dass du Mechanismen hast, mit denen du lernst, neuen Menschen auf sichere Art und Weise zu vertrauen. Kein Maß an guten Gewohnheiten, wie du über Aktionen sprichst, die in deiner Stadt auftreten (Sicherheitskultur), werden dich schützen, wenn du deine DNA am Handlungsort hinterlässt (OpSec), und keine Anzahl an aufgedeckter physischer Überwachung (OpSec) wird dich vor einer verdeckt ermittelnden Bullenschaft schützen, wenn diese sich mit deiner mitbewohnenden Person anfreundet, um näher an dich heranzukommen (Sicherheitskultur). Die Vorgehensweisen von OpSec und Sicherheitskultur sind unterschiedlich, und das eine ist kein Ersatz für das andere. Mit dem Entwickeln von umfassenderen Verständnissen beider Rahmenbedingungen können wir versuchen uns selbst und einander aus dem Gefängnis herauszuhalten, während wir den Aufbau von Verbindungen fortführen und informelle Netzwerke und Affinität vergrößern.

ZEHN TIPPS FÜR DIE ZERSTÖRUNG EINES TELEFONS



1. Steck dein Telefon in Brand
2. Wirf dein Telefon in den Kanal
3. Wirf die Telefone deiner Freund.innen in ein noch größeres Feuer
4. Wirf alle Telefone in den Kanal
5. Bring nicht immer dein Telefon mit (irgendwer könnte es ins Feuer werfen)
6. Sprecht miteinander, nicht mit euren Bildschirmen
7. Zerstöre Beweismittel (zurück zum Tipp 1 und 2) und lass nicht zu, dass Andere Beweismittel erstellen (zurück zu Tipp 3 und 4)
8. Mach den Gebrauch von Telefonen zum Thema
9. Sei über das Telefon unerreichbar, sei sozial
10. Scheiß auf Technologie

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

BRUCHSTÜCKE GEGEN ÜBERWACHUNG

In diesem Abschnitt möchten wir kurze Notizen teilen, die sich innerhalb des Rahmens des CSRC bewegen aber nicht für einen eigenen Eintrag auf der Webseite genügten. Du kannst uns solche Notizen zuschicken, wenn du sie in der nächsten Ausgabe veröffentlicht haben möchtest.

• Im Zuge von Brandstiftung an Fahrzeugen von Enedis (verantwortlich für die Verwaltung des Elektrizitäts-Vertriebsnetzes in Frankreich) und an einem bedeutenden Füllsender, wurden 2021 mehrere Menschen in Frankreich verhaftet. Ein Text auf Französisch berichtet ausführlich über die interessante Reichweite von Überwachungsmethoden, die ihrer Verhaftung vorangingen: Beschattung, die DNA-Sicherung an einem Autotürgriff während dessen Besitzer.in einkaufen war, das nächtliche Eindringen in eine Wohnung, um einen Keylogger auf einem Computer zu installieren, die Aufforderung an Enedis, eine Liste jener Menschen bereitzustellen, die die Installation des neuen „smarten" Elektrizitätszählers verweigerten, den sie überall installieren, und die Aufforderung an eine lokale Zeitung, jene IP-Adressen zur Verfügung zu stellen, die sich Zugang zu ihrem Artikel zur Brandstiftung verschafft haben.
• Im Jahr 2022 wurden zwei Anarchist.innen in Italien verhaftet und mit dem Vorwurf der Herstellung und des Besitzes von Sprengstoff angeklagt. Ein Text erklärt, dass die Ermittlung, die zur Verhaftung führte, zu dem Zeitpunkt anfing, als eine „unbekannte Person" Sprengstoff, Elektromaterialien und andere Vorrichtungen im Juni 2021 in einem Wald gefunden hatte. Danach stellten die Bullen Foto/Video-Fallen auf, um all diejenigen zu „fangen", die sich in die Nähe des Gebietes bewegten. Später wurde eine Person von hinten, in der Nähe der Stelle fotografiert, und die Polizei behauptete anschließend diese erkannt und identifiziert zu haben.
• Zum Schluss dieses Abschnitts gibt es hier ein hoffnungsvolles Zitat aus einem Kommuniqué, das behauptet, für die Brandstiftung an einem Bürogebäude des Bauunternehmens eines Knastbaus in Deutschland verantwortlich zu sein: *„Um auf den Überwachungskameras keine guten Bilder zu produzieren, trugen wir Regenponchos, die für eine Verschleierung von Körperform und Gangart sorgen. Um unsere Kopfform unkenntlich zu machen, benutzten wir Hüte. Die Weiterentwicklung der Videoauswertung bereitet vielen Genoss.innen Sorge, wir wollen mit diesem Einblick Möglichkeiten aufzeigen, sich gegen diese Überwachungstechnik zu wehren."*

TRAG DEINEN TEIL ZU CSRC BEI!

Wir schlagen die Nutzung der CSRC-Webseite vor, um die Kenntnis und die Erfahrungen zu den Themen der zielgerichteten Überwachung unter Gefährt.innen auf erleichterte Art und Weise zu teilen. Schau dich innerhalb der 180+ Hilfsmittel auf **csrc.link** um, die Seite ist auch via Tor Browser mit einer .onion Adresse aufrufbar. Drucke unsere brandneuen Aufkleberaus und verteile sie. Wirke mit, indem du uns eine E-Mail an **csrc@riseup.net** – wenn du verschlüsseln möchtest, dann findest du unseren PGP key: **csrc.link/csrc.asc**

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