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.

No Trace Project / No trace, no case. Eine Sammlung von Werkzeugen um Anarchist:innen und anderen Rebell:innen zu helfen, die Fähigkeiten ihrer Feinde zu **verstehen**, Überwachungsanstrenungen zu **unterlaufen**, und letztlich zu **handeln** ohne geschnappt zu werden.

Abhängig von deinem Kontext, kann es sein, dass der Besitz bestimmter Dokumente kriminalisiert wird oder ungewollte Aufmerksamkeit auf sich zieht—sei bedacht bezüglich der Broschüren, die du druckst und wo du sie lagerst.

Eine Grundlage, auf der wir stehen können

Die Unterscheidung zwischen OpSec und Sicherheitskultur

Eine Grundlage, auf der wir stehen können: Die Unterscheidung zwischen OpSec und Sicherheitskultur

Originaltext auf Englisch

A Base to Stand On: Distinguishing OpSec and Security Culture

No Trace Project

23. März 2023

Übersetzung und Layout

No Trace Project

notrace.how/de/blog/a-base-to-stand-on/eine-grundlage-auf-der-wir-stehen-konnen.html

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.

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.

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 Risi-

[1] https://notrace.how/resources/de/#confidence-courage-connection-trust

ken, 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)