AKTUELLE METHODEN STAATLICHER :UBERWACHUNG

A-DRESDEN.ORG
ANARCHISTISCHES NETZWERK DRESDEN

Das Anarchistische Netzwerk Dresden besteht aus Gruppen und Einzelpersonen in Dresden. Wir teilen gemeinsame Prinzipien und beteiligen uns an verschiedenen Kämpfen in der Stadt. Wir möchten einen Raum für interessierte Menschen schaffen, um sich kennenzulernen und gemeinsam an für sie bedeutsamen Themen zu arbeiten.

A-DRESDEN.ORG
a-dresden@riseup.net

1. Ausgabe, Juni 2024

Inhalt

Einleitung

1. Einleitung

Dieses Zine ist ein Begleitheft zum Vortrag 'Aktuelle Methoden staatlicher Überwachung'. Es soll zum einen dazu dienen sich die Inhalte wieder ins Gedächtnis zu rufen, und zum anderen diese Inhalte auch für Personen zugänglich machen, die den Vortrag nicht besucht haben.

In diesem Heft werden einzelne Technologien vorgestellt, die gegen Aktivist:innen eingesetzt werden. Wir werden anhand jeder dieser Technologien

1. im Überblick die Funktionsweise erklären
2. reale Beispiele aus der Vergangenheit geben
3. Möglichkeiten der Gegenwehr aufzeigen.

Das Heft ist als Work-In-Progress zu verstehen. Falls du Fehler findest, oder denkst, dass gewisse Technologien fehlen, die hier aufgeführt werden sollten, schreib uns eine Mail. Die aktuelle Fassung wurde recht schnell runtergeschrieben, um als Infomaterial zum Talk verfügbar zu sein. Für Rechtschreibfehler wird keine Haftung übernommen, Korrekturvorschläge sind jedoch gerne gesehen.

1.1 Smartphones im Visier

Blogpost des ABC Dresdens, November 14, 2023[1]

Wir stellen fest, dass linke Gruppen in den letzten Wochen und Monaten mehr und mehr von Repression betroffen sind. Staatliche Akteur*innen scheinen

[1] https://abcdd.org/2023/11/14/smartphones-im-visier/

sehr bemüht zu sein, unsere Smartphones zu beschlagnahmen. Was sie damit vorhaben, ist noch unklar, die Vermutung liegt nahe, dass es aktuell Bestrebungen gibt, linke Netzwerke und Gruppen zu durchleuchten und Verbindungen zwischen Einzelpersonen herzustellen. In diesem Text wollen wir auf Geschehnisse der Vergangenheit eingehen und die Leser*innen auffordern, ihre Sicherheitsprinzipien zu prüfen.

Stand Überwachung & Gesetzeslage

Weltweit gibt es Bestrebungen, unsere Chatverläufe und Bewegungsprofile abzurufen. Polizeibehörden in den USA fragen zum Beispiel regelmäßig Google, welche Personen zu einem bestimmten Zeitpunkt an einem bestimmten Ort waren. Ein Fall, der öffentlich wurde, ist der von Zachary McCoy. Aus dem Nichts bekam er einen Brief von Google mit der Information, dass Google seine Accountinformationen an die Polizeibehörden aushändigen wird. Der Grund: Zum Zeitpunkt eines Überfalls war McCoy in der Nähe des Tatorts joggen und hatte sein Smartphone dabei. Dadurch wurde er Hauptverdächtiger im Ermittlungsverfahren.

Innerhalb Europas und in Deutschland gibt es genauso konkrete Gesetze und Methoden, welche darauf abzielen, mittels unserer Handys und Smartphones Informationen über uns zu sammeln. So wurden mit dem neuen sächsischen Polizeigesetz Möglichkeiten geschaffen, Daten nicht nur bei klassischen Providern wie Internet- oder Telefonanbietenden abzugreifen, sondern auch bei Online-Diensten wie Twitter, Google, Facebook und Co. Mit dem Anti-Terror-Paket wurde 2016 die **Ausweispflicht beim Kauf von Prepaidkarten** eingeführt. Das Ziel ist, die Benutzung von anonymen Telefonen zu erschweren. Somit sind die meisten Telefone nun direkt an den Personalausweis der betreibenden Person gekoppelt. Diese Tatsache wird auch aktiv genutzt: 2014 haben staatliche Stellen ganze 7 Millionen Mal abgefragt, wem eine Telefonnummer gehört. Mittlerweile passiert das 21 Millionen Mal pro Jahr. Also dreimal so oft. Im aktivistischen Umfelde betreiben Leute zwar weiterhin Telefone mit vorregestrierten Sim-Karten – sogenannte Burner Sims, welche nicht auf den eigenen Namen laufen – der Anteil scheint in unseren Augen aber zu sinken.

Eine andere Technik staatlicher Überwachung, welche sich direkt gegen unsere Telefone richtet, ist die sogenannte „Stille SMS“. Diese SMS wird, wenn man sie empfängt, nicht angezeigt: man bekommt es also nicht mit. Trotzdem generiert sie einen Kommunikationsvorgang, der vom jeweiligen Telefonanbieter

protokolliert wird und dann von Polizeibehörden abgefragt werden kann. Auf diese Weise und beim mehrfachen Senden von dieser Stillen SMS erhält die Polizei ein akkurates Bewegungsprofil in Echtzeit. Vermutungen legen nahe, dass diese Methode unter anderem für Festnahmen benutzt wird. So geht aus Statistiken hervor, dass 2019 in Schleswig-Holstein für gewisse Maßnahmen mitunter 400 Stille SMSen verschickt wurden. Bei dieser Technik reicht es, wenn ihr ein Telefon mit Sim-Karte einstecken habt, auch wenn es ein noch so alter Knochen ist.

Eine weitere Technologie im Einsatz sind sogenannte IMSI Catcher. Dies sind Fake-Mobilfunkmasten, die Cops mitunter in der Nähe von Demonstrationen aufstellen. Somit wählen sich Telefone der Demonstrierenden in diesen falschen Mobilfunkmast ein. Dadurch wissen Cops zum einen, wer vor Ort ist, zum anderen ist es ihnen möglich, Telefongespräche und SMSen abzufangen. Solche IMSI Catcher wurden unter anderem auf Pegida Demos in Dresden eingesetzt.

All diese Methoden richten sich konkret und zielstrebig gegen die Mobiltelefone in unseren Hosentaschen. Die klassische Telekommunikations-Überwachung haben wir noch gar nicht erwähnt. Aktuell müssen wir davon ausgehen, dass die Telefone von Aktivist*innen aus dem Umfeld der Letzten Generation abgehört werden und zwar auch in Dresden [2]. Ein solcher Lauschangriff zieht große Kreise: auch wenn ihr selbst nicht im direkten Kontakt mit Menschen der Letzten Generation steht, kann es dennoch gut sein, dass ihr aus welchen Gründen auch immer sogenannte ‚Drittbetroffene' seid und trotzdem ins Visier der Überwachungsmaßnahme fallt. Es ist wichtig, sich darüber im Klaren zu sein und keine Informationen über Strukturen, Aktionen oder ähnlichem am Telefon zu besprechen. Und wenn die Cops keine Genehmigung bekommen, unsere Geräte aus der Ferne auszuspähen, dann gibt es eine viel einfachere Methode, uns komplett zu durchleuchten und Vollzugriff auf unser privates und aktivistisches zu Leben bekommen: die Beschlagnahmung von unseren Smartphones!

Allein 300 Beschlagnahmte Handys am TagX

Der Staat beschlagnahmt technische Geräte nicht aus Spaß oder einfach, um uns die Geräte wegzunehmen, sondern um diese auszuwerten und Beweise gegen uns zu sammeln. Für diese Auswertungen kaufen Polizeibehörden Software von Privatunternehmen ein, so z.b. die Software „Celebrite" vom gleichnamigen Her-

[2] https://www.addn.me/news/saechsische-polizei-ermittelt-gegen-letzte-generation-grosser-lauschangriff-auf-den-dresdner-stadtrat/

steller. Das sind Firmen, die sich darauf spezialisieren, Smartphones auszuwerten. In der Vergangenheit kam es immer wieder zur Beschlagnahmung von Geräten aus dem aktivistischen Umfeld, vorallem von Smartphones. So wurde zum Beispiel am Anarchistischen 1. Mai in Dresden ein Telefon beschlagnahmt. Am TagX in Leipzig wurden alleine 300 Handys bzw. Smartphones beschlagnahmt und diese werden nun „als Beweismittel ausgewertet“ [3]. Aufgrund eines Tweets haben Cops einen Sozialarbeiter aus Sachsen aufgespürt und auch sein Telefon beschlagnahmt. Letzte Woche gab es Hausdurchsuchungen im Rahmen des 01.05. in Gera – auch dort wurden Smartphones beschlagnahmt.

Der Grund ist immer wieder der gleiche: man müsse Beweismittel sichern. Doch ein beschlagnahmtes Smartphone enthält Daten, die weit darüber hinausgehen. Absurd ist auch, dass Behörden keine Statistik darüber führen, wie viele Smartphones sie auslesen. Wir müssen davon ausgehen, dass das Auslesen unserer Geräte ohne Rücksicht auf die Privatsphäre zum Normalfall wird. Bei einer erfolgreichen Auswertung bekommen die Cops zugriff auf SMS, Kontakte, Anrufverläufe, alle Medien (Bilder, Videos, Audio Aufnahmen), App-Daten, Dateien sowie versteckte und gelöschte Dateien. Die Datenmenge, die wir dadurch an die Behörden übergeben, ist enorm groß. Sie können Bildschirmsperren umgehen und sich gemütlich Chatverläufe in diversen Messengern angucken. Dadurch ist es möglich, detaillierte Netzwerke aus Kontaktpersonen zu erstellen. Da heutzutage viele Chatmessenger an eine Telefonnummer gebunden sind, ist es ein Leichtes, die Identität der einzelnen Personen in verschiedenen Chatgruppen zu ermitteln und Mitglieder ganzer Politgruppen zu erschnüffeln.

Trotzdem ist es in linken Kreisen eine gängige Praxis sich über nummergebundene Messegner auf Smartphones zu organisieren – es drängt sich die Frage auf, ob wir perspektivisch nicht einen anderen Umgang finden müssen.

Prüft eure Sicherheitskonzepte !

Der Staat ist unser Feind und unsere tägliche politische Arbeit richtet sich voll und ganz gegen ihn. Genau deswegen ist es wichtig, diesem bürokratischen Unterdrückungsapparat keinen Meter Platz zu machen. Nicht nur auf der Straße, sondern auch im digitalen Raum. Aktivist*innen auf der ganzen Welt engagieren sich für die verschiedensten Kämpfe – und mögen ihre Herangehensweisen noch so unterschiedlich sein, eint sie doch immer wieder derselbe Punkt: sie

[3] https://www.mdr.de/nachrichten/sachsen/leipzig/leipzig-leipzig-land/leipzig-polizei-zu-fehlern-demo-tagx-kessel-dritter-juni-100.html#sprung2

setzen sich einem Repressionsrisiko aus und nehmen mitunter hohe Strafen in Kauf. Ein wichtiges Grundprinzip, um langfristig politisch aktiv bleiben zu können und nicht hinter Gittern zu landen, ist der Schutz der eigenen Anonymität. Die Handlungen und Aktionen, welche wir ausführen, dürfen nicht mit unserer „offiziellen“ Person in Verbindung gebracht werden. Deswegen müssen wir die Daten, die wir mit anderen Aktivist*innen austauschen, schützen. Wir müssen sicher und verschlüsselt kommunizieren, nicht aus Spaß, sondern zum Schutze unserer eigenen Sicherheit und der unserer Genoss*innen.

Bei der Wahrung unserer Anonymität sind wir auf die Hilfe unserer Mitmenschen angewiesen: sie müssen diese genauso respektieren und achten wie wir selbst. Hier greifen die Prinzipien der gegenseitigen Hilfe – Mutual Aid – wie in allen anderen Bereichen des Lebens. Es muss Teil einer solidarischen Praxis sein, die Anonymität unserer Mitmenschen zu erhalten. Die Sachen, die wir online besprechen, austauschen und organisieren, gehen nur uns etwas an. Und mit jedem Sicherheitsrisiko, das wir eingehen, mit jedem konfiszierten Smartphone, das sensible Informationen enthält, machen wir Platz für unseren politischen Gegner und verlieren ein Stück Freiheit. Deswegen möchten wir dazu aufrufen, die Sicherheitskonzepte innerhalb eurer Politgruppen zu checken. Prüft welche Informationen euer Handy preisgibt, welche Infos den Behörden durch eine Hausdurchsuchung in die Hände fallen würden und was sich davon vermeiden ließe.

II Methoden

2. Ortungsmethoden

2.1 Stille SMS

Stille SMS Nachrichten sind eine technologische Angriffsmethode, um unseren Standort über die Handys in unseren Hosentaschen ausfindig zu machen. Dazu versenden die staatlichen Behörden eine spezielle SMS an unsere Telefone, die bei uns aber gar nicht angezeigt wird. Die Nachricht ist quasi "still", weil wir davon nichts mitbekommen. Die Cops können dadurch unseren genauen Standort zu genau dem Zeitpunkt ermitteln, an dem sie die SMS abgeschickt haben.

2.1.1 Beispiele

In Schleswig-Holstein wurden 2019 in mehreren Maßnahmen (271) Stille SMS eingesetzt. Dort wurden pro Maßnahme rund 400 dieser Nachrichten verschickt[1]. Vermutlich werden Stille SMS Nachrichten für Festnahmen benutzt und innerhalb kürzester Zeit sehr oft verschickt, um die gesuchte Person ausfindig zu machen.

2.1.2 Verteidigung

Stille SMS Nachrichten funktionieren bei Smartphones genauso wie bei alten "Knochen". Es ist also komplett egal welche Art Telefon man besitzt - solange man es bei sich hat und eine SIM-Karte eingelegt ist, kann man mittels der Stillen SMS (sowie der Funkzellenabfrage) geortet werden. Um sich dagegen zu verteidigen, sollte man schlichtweg kein Telefon bei sich haben oder es ausschalten.

[1] https://netzpolitik.org/2020/viele-stille-sms-bei-bund-und-laendern/

Eine Möglichkeit um trotzdem kommunizieren zu können wäre ein Smartphone ohne SIM-Karte, das man nur über WLAN benutzt.

2.2 GPS Tracker

Wenn die Polizeibehörden an einem Bewegungsprofil interessiert sind, wird die Zielperson im Zuge des „kleinen Lauschangriffs“ nach § 100h Abs. 1 Nr. 2 StPO unter Umständen auch per GPS Tracker am Auto überwacht. Das passiert vor allem, wenn die Ortung auf anderem Wege erschwert wäre - d.h. wenn die Person kein Telefon bei sich hat, oder dieses regelmäßig wechselt.

2.2.1 Beispiele

Bild 2.1: GPS Tracker an Seitenschwelle vom Auto

Bild 2.2: Tracker der nach Fund entfernt wurde.

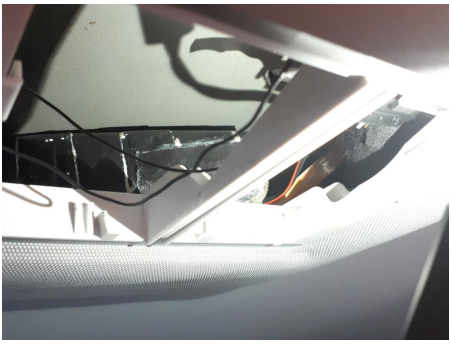

Bild 2.3: Tracker und Wanze im Fahrzeuginnenraum hinter der Deckenbeleuchtung.

Bild 2.4: Weiterer ausgebauter Tracker

Beispiele gibt es mehr als genug. In der Regel werden GPS Tracker an der Fahrzeugunterseite mit Magneten angebracht. Die Tracker haben einen Akku und senden die Daten über das Mobilfunknetz raus. Der Tracker in Bild 2.1 wurde 2022 in Berlin gefunden und dann entfernt, wie in Bild 2.2. zu sehen ist. 2 Wochen später haben die Aktivist:innen einen neuen Tracker an ihrem Auto gefunden und wieder entfernt[2].

In Bild 2.3. sehen wir die aufgeschraubte Deckenbeleuchtung im Fahrzeuginnenraum zwischen den beiden vorderen Sitzen. Dort wurde ein GPS Tracker sowie ein kleineres Audioaufnahmegerät verbaut. Die Geräte waren hinter einer Verkleidung der vorderen Deckenbeleuchtung versteckt. Sie waren durch ein Stromkabel miteinander verbunden und bezogen ihren Strom aus der Zuleitung zur hinteren Deckenleuchte[3].

2.2.2 Verteidigung

Checkt eure Autos und beobachtet sorgsam eure Umgebung! Falls ihr selbst überwacht wurdet, informiert potenzielle weitere Betroffene! Beteiligt euch nicht an Spekulationen und redet nicht mit den Cops. Anna und Arthur halten's Maul!

[2] https://de.indymedia.org/node/215986
[3] https://de.indymedia.org/node/160385

2.3 IMSI-Catcher

IMSI-Catcher sind ein technologisches Überwachungsinstrument, um Handys, bzw. die dort eingelegten SIM-Karten in der Umgebung ausfindig zu machen. Dazu wird eine Art "Fake Funkzelle" erstellt, in die sich die Handys in der Umgebung dann automatisch einwählen - als wäre es ein ganz normaler Funkmast vom Telefonanbieter eures Vertrauens. Sobald sich die Telefone dort eingewählt haben, können die Cops genau sehen welche Telefone und SIM-Karten sich eingewählt haben. Zusätzlich ist es möglich Telefonate sowie SMS Nachrichten abzuhören.

Zum einen werden solche IMSI-Catcher auf Demonstrationen eingesetzt, um einen Überblick über die anwesenden Personen zu bekommen, zum anderen kann man damit auch Personen observieren und rausfinden mit welchen anderen Personen sie sich treffen (indem sie sehen welche Handys sich in der näher der observierten Person befinden).

2.3.1 Beispiele

Bild 2.5: IMSI-Catcher auf PEGIDA Demo 10.02.2015 Dresden

Bild 2.6: IMSI-Catcher auf DÜGIDA/PEGIDA Demo 25.02.2015

Wie in Bild 2.5 und Bild 2.6 zu sehen kommen IMSI-Catcher auf Demonstrationen zum Einsatz, um einen Überblick über die anwesenden Personen (bzw. deren Telefone) zu bekommen. Des Weiteren werden sie aber auch zur Observation einzelner Personen benutzt. Dabei verfolgen die Cops die Person mit dem IMSI-Catcher und schauen welche Telefone anwesend sind. Darüber können sie zum einen bestimmen welches Telefon die Zielperson selber mit sich hat - also auch herausfinden welche "anonyme SIM-Karte" diese Person gerade benutzt. Des Weiteren sehen sie die Telefone anderer Personen, mit denen sich

die Zielperson trifft. Darüber können sie ein Netzwerk aller mobilen Geräte des sozialen Umfeldes erstellen und die Identitäten befreundeter Personen ermitteln oder Überwachungsmaßnahmen gegen die Telefone der Kontaktpersonen starten.

2.3.2 Verteidigung

Es gibt Apps um Imsi Catcher zu entdecken - zum Beispiel der Android IMSI-Catcher Detektor[4]. Des Weiteren funktionieren IMSI-Catcher nur wenn man ein Telefon dabei hat, sobald man kein Telefon einstecken hat, oder es ausgeschaltet, ist man immun. Da IMSI-Catcher auch die Kommunikation abhören können (Telefonate, SMS) sollte man über Ende zu Ende verschlüsselte Messenger wie Element oder Signal kommunizieren.

[4] https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector

3. Beweismittelsicherung

3.1 Digitale Forensik

Sicherheitsbehörden verfügen über Technologien zur Auswertung der Daten auf Handys sowie Laptops. Abhängig vom Betriebssystem und Verschlüsselung ist diese Auswertung mehr oder weniger erfolgreich. Es kommt regelmäßig dazu, dass Cops Handys beschlagnahmen. Das kann auch im Alltag passieren, in einer normalen Kontrolle. Sobald ein Gerät beschlagnahmt wurde, kann die forensische Untersuchung beginnen. Das bedeutet es wird spezielle Software benutzt, um die Geräte auszulesen. Diese Software kann in der Regel Displaysperren umgehen, versuchen verschlüsselte Geräte zu entschlüsseln, Passwörter zu cracken oder Sicherheitslücken ausnutzen, um das Gerät zu knacken.

Sobald ein Gerät erfolgreich ausgelesen wurde, können die Cops ALLE Nachrichten (egal ob Signal, Element oder SMS) einsehen, sie haben Zugriff auf alle Dateien und Apps. Mit diesen Daten und spezieller Analyse Software können sie dann nach Keywords in allen Nachrichten suchen und soziale Netzwerke mit den Kontaktpersonen erstellen. Sobald sie mehrere Geräte von verschiedenen Personen ausgelesen haben, können sie diese gemeinsam analysieren. D.h. sie können Überschneidungen von
Kontaktpersonen finden, sie können Orte finden, an denen man sich zeitgleich aufgehalten hat und vieles mehr. Wenn ein solches Gerät privat genutzt wurde, legt diese Software das komplette Privatleben der betroffenen Personen in die schmierigen Hände der Ermittlungsbehörden - eine wirklich unschöne Vorstellung.

Die deutsche Polizei hat 7 solcher Auslesetools im Einsatz, viele davon sind konkret auf das Knacken und Auswerten von Smartphones spezialisiert[1]. In Sachsen wurde zum Beispiel die Software "Cellebrite" eingesetzt, ein Tool das damit wirbt auch neuste Geräte und iPhones knacken zu können.

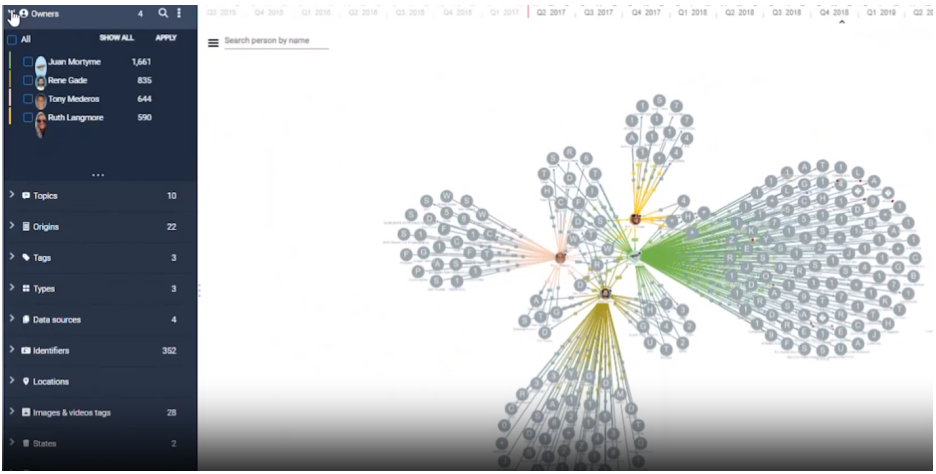

Bild 3.1: Screenshot der Software Cellebrite welche ein soziales Netzwerk verschiedener Personen generiert

3.1.1 Beispiele

Alle 3,5 Stunden durchsucht die Polizei ein Smartphone[2]. Auf der Demonstration zum Tag X (nach der Verurteilung von Lina) in Leipzig wurden 383 Telefone beschlagnahmt. Das ist eine unglaublich hohe Zahl. Beschlagnahmungen von Smartphones sind für Cops aktuell eines der effektivsten Ermittlungswerkzeuge. Einerseits sind sie rechtlich einfach durchzusetzen, andererseits geben diese Geräte extrem viele Informationen preis.

3.1.2 Verteidigung

Die Verteidigung gegen forensische Untersuchung der eigenen Geräte ist ein komplexes Themengebiet. Zuerst kannst du Maßnahmen ergreifen, um eine Beschlagnahme der Geräte zu erschweren - z.b. indem du keine Geräte mit

[1] https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/

[2] https://netzpolitik.org/2024/sachsen-anhalt-alle-35-stunden-durchsucht-die-polizei-ein-smartphone/

Chatverläufen oder anderen sensiblen Informationen mit auf Demos nimmt. Des Weiteren ist es wichtig die Geräte stetig zu aktualisieren. Bei Smartphones empfiehlt es sich LineageOS oder GrapheneOS zu verwenden, da diese Betriebssysteme einen hohen Sicherheitsstandard aufweisen und von Auslesetools wie Cellebrite nicht so leicht geknackt werden können.

Dann stellt sich noch die große Frage wie viele Daten man auf diesen Geräten haben muss. Wenn man das Gerät "privat" benutzt wäre es von Vorteil die Kommunikation bezüglich Aktionen, Gruppentreffen, ..., auf anderen anonymen Geräten zu betreiben. Sei es ein eigens dafür vorgesehenes Smartphone, oder ein verschlüsselter Rechner/Laptop. Die Wahrscheinlichkeit, dass ein ordentlich verschlüsselter Rechner/Laptop geknackt wird, ist geringer - eben weil moderne Unternehmen sich vorwiegend mit dem Knacken von Smartphones beschäftigen.

4. Observationsmethoden

4.1 Videoüberwachung

Videoüberwachung ist ein breites Feld staatlicher Ermittlungsarbeit. Es gibt tausende Überwachungskameras an öffentlichen Orten. Bei Demonstrationen oder ähnlichem installieren Cops temporäre Videokameras, um die Personen abzufilmen. Dies passiert alles öffentlich und mit dem Wissen der Beteiligten. Zusätzlich gibt es allerdings auch den verdeckten Einsatz von Videoüberwachung. Dazu installieren die Ermittlungsbehörden möglichst unbemerkt Videokameras an verschiedensten Orten, um so über einen gewissen Zeitraum einen bestimmten Ort (Hauseingang, alternatives Zentrum, Wagenplatz, ...) zu observieren.

Diese Installationen können sehr unterschiedlich sein. Häufig werden sie in leerstehenden Wohnung aufgebaut, um durch ein Fenster die gegenüberliegende Straßenseite oder Ähnliches zu filmen. Es gibt aber auch mobile Installationen die in Autos aufgebaut werden können. Das Auto wird dann vor dem zu observierenden Ort geparkt und nach einer Weile wieder abgeholt. Unter anderem können diese Systeme auch automatische Gesichtserkennung betreiben, und die vorbeigehenden Personen automatisch mit Gesichtern aus Datenbanken abgleichen[1]. Falls sich eine Person, nach der gesucht wird, an solch einer Installation vorbeibewegt, bekommen die Cops automatisch eine Meldung.

In manchen Fällen kommt es auch vor, dass verdeckte Videokameras direkt in den Wohnungen von betroffenen Personen installiert werden.

[1] Netzpolitik 03.05.2024 "Polizei observiert mit Gesichtserkennung": https://netzpolitik.org/2024/ueberwachungstechnik-polizei-observiert-mit-gesichtserkennung/

4.1.1 Beispiele

Bild 4.1: Verdeckte Kamerainstallation in Wohnung

Bild 4.2: Verdeckte Kamerainstallation in einem Auto

Beispiele solcher Installationen zeigen uns Erfahrungen von Aktivist*innen in der Vergangenheit.[2]. Hier abgebildet sehen wir Bild 4.1 - eine Installation, die in einer Leer stehenden Wohnung aufgebaut wurde und einen gegenüberliegenden Wagenplatz gefilmt hat[3]. Bild 4.2 - eine Installation in einem Auto. In dem Auto befand sich eine Videokamera, die einen Hauseingang abgefilmt hat. Nachdem sie entdeckt wurde, haben Aktivist:innen Zettel an dem Auto angebracht, um auf die Kamera aufmerksam zu machen.

4.1.2 Verteidigung

Beispiele verdeckter Videoüberwachungsinstallationen zeigen, dass diese in der Regel immer auf stationäre Ziele (Wagenplätze, Hauseingänge, Haltestellen, ...) gerichtet sind, um dort ein und ausgehende Personen zu identifizieren. Als Polit- oder Bezugsgruppe solltet ihr abwägen, ob es notwendig ist, die eigenen Treffen/Plena an solchen Orten abzuhalten. Es empfiehlt sich neutrale (politisch nicht vorbelastete) Orte für die Treffen zu wählen und diese Orte regelmäßig zu wechseln. Wenn es keine festen Treffpunkte gibt, ist es auch nicht möglich diese zu observieren.

Solche Kameras können auch filmen, was ihr auf euren Handys oder Laptops macht und eventuell aufzeichnen welche Nachrichten ihr schreibt. Daher empfiehlt es sich die Bildschirme so auszurichten, dass sie durch kein Fenster

[2] notrace.how - "Searchable database of cases of physical surveillance devices": https://www.notrace.how/earsandeyes/#type=video

[3] Indymedia 15.12.2022 "Versteckte staatliche Überwachungskamera in Bremen demontiert!": https://de.indymedia.org/node/245569

oder Eingang zu sehen sind. Setzt euch zum Beispiel mit dem Rücken zur Wand. Gegen automatische Gesichtserkennung können einfache Mittel wie Basecaps, hochgezogene Schals oder andere Taktiken der Vermummung helfen.

4.2 Super Recognizer

Super Recognizer (dt "Wiedererkenner:innen") sind Personen, die sich überdurchschnittlich gut Gesichter merken können. Man kann es sich wie ein fotografisches Gedächtnis für Gesichter vorstellen. Das ist eine Fähigkeit die rund 2% der Menschen besitzen[4]. In UK hat die Polizei angefangen sich diese Eigenschaft zu Nutze zu machen und unter den bereits angestellten Polizist:innen Tests durchgeführt, um eben solche Super Recognizer ausfindig zu machen. Iht täglicher Job ist es eine Vielzahl von Videoaufnahmen von Straftaten zu sichten und sich die Personen genau einzuprägen. Wenn sie diese Personen dann später wieder sehen, können sie sich daran erinnern auf welcher Videoaufnahme sie diese gesehen haben. Dem Ganzen liegt eine Pseudowissenschaft zugrunde, die behauptet das eben diese Super Recognizer niemals falsch liegen. Außerdem sollen diese, wenn sie denn eine Person wieder erkennen dann auch zu 100 % richtig liegen. Zeitgleich soll es ihnen möglich sein, Personen auch trotz Vermummung wiederzuerkennen. Zum Teil soll nur die Augenpartie ausreichen, um eine Person später wieder identifizieren zu können.

Entgegen wissenschaftlicher Erkenntnisse vertritt die Polizei die Einschätzung, dass Super Recognizer eine zuverlässige und sichere Ermittlungsmethodik darstellen. Die Polizei Sachsen setzt seit 2021 immer mehr auf den Einsatz von Super Recognizern. Es befinden sich aktuell verschiedene "Wiedererkenner:innen" in Chemnitz und Dresden[5] im Einsatz. Aktuell scheint es, als könnten super recognizer vermummte Personen sehr viel besser erkennen als die digitale Gesichtserkennung. So sind super recognizer auch häufiger auf Demos präsent, um Personen, die in der Vergangenheit auffällig geworden sind wieder zu erkennen. Falls sie jemanden sehen, Versuchen die Cops diese Person dann aus der Demonstration zu ziehen, um deren Identität feststellen zu können.

[4] Paper Super-recognizers: People with extraordinary face recognition ability: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3904192/

[5] https://www.polizei.sachsen.de/de/MI_2024_104685.htm

4.2.1 Beispiele

Am 16. Mai 2021 kam es nach einem Fußballspiel von Dynamo Dresden zu Ausschreitungen. Dort wurden Super Recognizer eingesetzt, um vermummte Personen zu identifizieren[6]. Laut Angaben der Polizei wurden 33 von 42 vermummten Personen mittels 80 Stunden Videomaterial identifiziert. Auf Demonstration in Anna-Berg-Buchholz wurde 2022 eine Person aus der Demo gezogen - ein Super Recognizer hat die Person von einer Monate zurückliegenden Straftat wiedererkannt.

4.2.2 Verteidigung

Super Recognizer können sich sehr gut Gesichter merken und bekommen diese meist mittels Videoaufnahmen zugespielt. Auch wenn sie Personen trotz Vermummung wiedererkennen können, hat das Grenzen. Es ist schwierig Empfehlungen auszusprechen aber eine Vollvermummung für Mund, Nase, Ohren und Sonnenbrille (sowie Mütze) sollte trotzdem noch einen gewissen Schutz bieten. Des Weiteren ist es umso wichtiger sich gegen Kameraaufnahmen der Cops abzuschirmen. D.h. klassische Mittel wie der Einsatz von Regenschirmen sollten stärker fokussiert werden.

[6] https://www.saechsische.de/dresden/krwalle-stadion-ausschreitungen-die-gewaltbereite-fanszene-dynamos-ist-nicht-erreichbar-5800249.html

5. Kommunikationsüberwachung

5.1 Telekommunikationsüberwachung

Die Telekommunikationsüberwachung (TKÜ) ist ein breites Feld polizeilicher Ermittlungsarbeit. Sie umfasst das Abhören von Telefonaten, E-Mail Überwachung, Mitschneiden von SMS und Telefaxen sowie Funkzellenabfragen. Seit 2017 gibt es auch die Quellentelekommunikationsüberwachung um verschlüsselte Kommunikationsüberwachung zu können. Geregelt in Paragraf 100a StPO[1] ist über eine Kette verschiedene Listen von Straftatbeständen ersichtlich, das Telekommunikationsüberwachung bei "schweren" Fällen von Hausfriedensbruch (Besetzungen, Blockaden von Kohleinfrastruktur, ...), Landfriedensbruch (Blockaden etc.) sowie bei der Bildung einer kriminellen Vereinigung zulässig ist.

Das alles sind Delikte, die Aktivist*innen recht schnell vorgeworfen werden können. Die Möglichkeit, dass man selbst oder Genoss*innen im Umfeld abgehört werden, sollte nicht unterschätzt werden. Vor allem in Zeiten ausufernder Repression gegen Antifaschist*innen, wie der Fall Lina zeigt und dem aktuell laufenden Budapest-Verfahren, sind neben Hausdurchsuchungen sicherlich auch einige Telefonanschlüsse angezapft. Dieser Realität müssen wir in die Augen schauen und die Informationsgewinnung der Repressionsbehörden durch diese Maßnahmen auf ein Minimum reduzieren.

[1] https://www.gesetze-im-internet.de/stpo/__100a.html

5.2 Telefonate, SMS Abhören

Bei der TKÜ zapfen die Cops den Telefonanschluss einer Person an, hören dann Gespräche mit und lesen jede SMS, die das Telefon sendet oder empfängt. Heutzutage gibt es kein Knistern oder Knacken mehr in der Leitung, wenn man abgehört wird, es ist schlichtweg als betroffene Person nicht möglich auf einfachen Wegen davon mitzubekommen.

5.2.1 Beispiele

Im Rahmen eines Ermittlungsverfahrens gegen die Fanszene von BSG Chemie Leipzig wurden 2015 921 Telefonanschlüsse abgehört[2]. Diese Zahl ist unglaublich hoch und ein Zeichen dafür, dass diese Ermittlungsmethode dafür vorbestimmt ist komplett auszuufern. Sobald eine verdächtige Person X einen Anruf von einer anderen Person bekommt, stellt sich bei den Cops die Frage, ob diese andere Person nicht auch überwacht werden sollte - schließlich stehen die beiden ja wohl in engerem Kontakt. So konnten in kürzester Zeit aus ein, zwei abgehörten Anschlüssen ganze 921 werden. Darunter waren nicht nur komplett unbeteiligte Personen wie die Großeltern der Fans, sondern auch Geheimnisträger:innen wie Journalist:innen und Rechtsanwälte.

5.2.2 Verteidigung

Klassischen Abhörmaßnahmen von Telefon und SMS sind wirkungslos gegen verschlüsselte Messenger wie Element, Signal und Co. Sobald ihr eure Telefonate und Nachrichten darüber austauscht seid ihr geschützt. Wichtig ist dabei konstant zu sein und mit allen Genoss:innen in eurem Umfeld klar festzulegen, dass auch wirklich nur noch darüber kommuniziert (also auch telefoniert wird). Oft kommt es vor, dass mal jemand nicht pünktlich beim Plenum auftaucht und dann notdürftig doch mal über den normalen Weg angerufen wird - solche kleinen Ausreißer gilt es zu vermeiden.

Des Weiteren ist es möglich Auskunftsersuchen bei Behörden wie der Landes-, Bundespolizei oder dem Verfassungsschutz zu stellen[3]. Darüber erfahrt ihr zwar nicht konkret, ob ihr abgehört werdet, wenn jedoch in den Antwortschreiben steht, das sie weitere Informationen über euch besitzen, diese aber geheimgehalten werden, um die Ermittlungsarbeit nicht zu gefährden, ist das ein recht guter

[2] https://netzpolitik.org/2018/abhoerskandal-um-fussballfans-in-leipzig-921-belauschte-telefone/

[3] Auskunftsgenerator: http://datenschmutz.de/cgi-bin/auskunft

Hinweis darauf das gerade Abhör- oder andere Überwachungsmaßnahmen laufen.

5.3 Mails Abhören

E-Mail-Anbieter:innen mit mehr als 10.000 Usern müssen in Deutschland "überwachungsbereit" sein. Das bedeutet sie sind verpflichtet Vorkehrungen zu treffen, die es Cops erlauben eine Überwachungsmaßnahme unverzüglich einzuleiten. Das kann einerseits bedeuten, dass sie das "Archiv" eines kompletten Postfaches bekommen - also alle E-Mails, die bis zu diesem Zeitpunkt von einer bestimmten E-Mail Adresse gesendet oder empfangen wurden. Andererseits können sie auch E-Mail-Adressen live überwachen, d.h. wenn bei dir eine neue E-Mail reinkommt passiert das genauso auf dem Präsidium deiner Lieblingsinstitution und eventuell liest der Bulle die Nachricht sogar noch vor dir.

5.3.1 Beispiele

2022 hat die Polizei in Bayern neben Telefonanschlüssen auch eine E-Mail-Adresse der Letzten Generation abgehört[4]. Viel gebracht hat dieser massive Eingriff in Privatsphäre und Pressefreiheit offenbar nicht. Die SZ zitiert einen Vermerk des Landeskriminalamts zu der Anschlussüberwachung: „Erkenntnisse über bevorstehende Aktionen, welche nicht bereits durch Pressemitteilungen oder -Konferenzen veröffentlicht wurden, konnten im Rahmen der Überwachung nicht festgestellt werden.“

5.3.2 Verteidigung

Ähnlich wie beim Abhören von Telefonaten oder SMS hilft auch hier Verschlüsselung. Verschlüsselte Mails können die Cops nicht lesen, sie sind aufgeschmissen und kratzen sich ratlos am Kopf. Dennoch können sie sehen, wann und mit wem Mails ausgetauscht wurden. Teilweise reichen den Cops diese "Metadaten" schon aus, um ihre Schlüsse zu ziehen.

5.4 Funkzellenabfrage

Mit der Funkzellenabfrage können Verkehrsdaten von Mobilfunkteilnehmer:innen ermittelt werden. Dazu werden Informationen von Mobiltelefonen und anderen Mobilfunk-Endgeräten erhoben, die sich, in einem bestimmten

[4] https://netzpolitik.org/2023/telekommunikationsueberwachung-polizei-soll-monatelang-die-letzte-generation-abgehoert-haben/

Zeitraum und in einem bestimmten Bereich – von hundert Metern bis hin zu einigen Kilometern – über eine Funkzelle im Mobilfunknetz angemeldet haben. Das Ziel von Funkzellenabfragen ist die Identifizierung von potenziellen Tatverdächtigen. Wenn bekannt ist, welche Personen sich zu einem bestimmen Zeitpunkt wo aufgehalten haben, kann unter Umständen der Kreis der Tatverdächtigen eingeengt werden.

5.4.1 Beispiele

Bei der Gegenkundgebung zum Naziaufmarsch zum Gedenken an den 13. Februar 1945 im Februar 2011 in Dresden wurden mittels mehrerer Funkzellenabfragen über eine Million Verkehrsdatensätze und über 40.000 Bestandsdatensätze von Versammlungsteilnehmern und Unbeteiligten gespeichert und ausgewertet[5]. Im Rahmen des G20-Gipfels in Hamburg wurden laut einer Antwort des Hamburger Senats 38 Anträge zur Erhebung von Funkzellendaten gestellt[6]. Mindestens 612 Funkzellenabfragen wurden in Berlin laut dem Jahresbericht 2019 angeordnet[7].

5.4.2 Verteidigung

Sobald man ein Telefon mit SIM-Karte betreibt, kann man von Funkzellenabfragen betroffen sein. Eine Möglichkeit ist das Telefon zu Hause zu lassen, oder ohne SIM über WLAN zu nutzen. Man kann auch Auskunft verlangen, ob man von Funkzellenabfragen betroffen war[8].

[5] https://www.addn.me/uploads/Pr%C3%BCfbericht1902.pdf

[6] https://www.buergerschaft-hh.de/parldok/dokument/58940/g20_technische_ueberwachungsmassnahmen_iii.pdf

[7] Netzpolitik 12.06.2020 "12 Funkzellenabfragen pro Woche": https://netzpolitik.org/2020/berlin-12-funkzellenabfragen-pro-woche/

[8] https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.Benachrichtigungsersuchen-Funkzellenueberwachung

III Abschluss

6. Abschluss

6.1 Weiterführende Informationen

6.1.1 EFF Surveillance Self Defence

Die Sicherheits-Guides der Electronic Frontier Foundation sind sehr zu empfehlen. Dort gibt es Tipps und Tools für sichere online Kommunikation und vieles mehr.

https://ssd.eff.org/

6.1.2 Notrace.How

No trace, no case. A collection of tools to help anarchists and other rebels understand the capabilities of their enemies, undermine surveillance efforts, and ultimately act without getting caught.

https://www.notrace.how/

6.1.3 Sicherheitsratgeber für Aktivist*innen

Der Sicherheitsratgeber vom Anarchist Black Cross Dresden zielt darauf ab, einen knappen Überblick zur Informationssicherheit für alle zu bieten, die sich in emanzipatorischen Kämpfen gegen Machtstrukturen befinden.

https://abcdd.org/security-guide/

6.1.4 Vorträge vom CCC

Im Umfeld des Chaos Computer Club gibt es jedes Jahr viele Events mit sehr informativen Veranstaltungen und Vorträgen. Einige davon werden aufgezeichnet und können nachträglich geguckt werden. Es lohnt sich auf jeden Fall mal rein zu schauen!

https://media.ccc.de

6.1.5 Cryptoparty Handbook

Das Cryptoparty Handbuch bietet Informationen zu fast allen Dingen, die mit digitalen Daten in den weiten des Internets zu tun haben.

https://cryptoparty.is/handbook/

6.1.6 Tails

Tails (The Amnesic Incognito Live System) ist eine auf Debian basierende Linux-Distribution. Ihr Ziel ist es, die Privatsphäre und Anonymität des Nutzer*in zu schützen. Um dies zu erreichen, setzt Tails insbesondere auf die Nutzung des Tor-Netzwerks. Das System kann direkt von einer Live-DVD oder einem USB-Stick gebootet werden und hinterlässt dann keine Spuren auf dem genutzten Computer.

https://tails.net

"EIN PACKENDES UND ERSCHRECKENDES HEFT. 'AKTUELLE METHODEN STAATLICHER :UBERWACHUNG' ZEIGT SCHONUNGSLOS, WIE ALLGEGENW:ARTIG DIE :UBERWACHUNG IN UNSEREM ALLTAG IST. TROTZ DER D:USTEREN BOTSCHAFT KONNTE ICH ES NICHT AUS DER HAND LEGEN." - ANNA

"ICH HATTE MIR MEHR ERHOFFT, ABER 'AKTUELLE METHODEN STAATLICHER :UBERWACHUNG' WAR EINE EINZIGE KATASTROPHE. D:USTER, DEPRIMIEREND UND V:OLLIG HOFFNUNGSLOS. AM ENDE F:UHLTE ICH MICH, ALS G:ABE ES KEINE RETTUNG AUS DIESEM SCHEISS SYSTEM." - ARTHUR

"'AKTUELLE METHODEN STAATLICHER :UBERWACHUNG' IST EIN AUGEN:OFFNER. ES ZEIGT EINDRINGLICH, WIE TIEFGREIFEND DIE :UBERWACHUNG IN UNSER LEBEN EINGREIFT. DIE D:USTERE REALIT:AT, DIE HIER DARGESTELLT WIRD, HAT MICH NACHHALTIG BEEINDRUCKT." - CELINE

"TROTZ ALLER VERSUCHE, DEINE PRIVATSPH:ARE ZU SCH:UTZEN, BLEIBT DIE :UBERWACHUNG ALLGEGENW:URTIG UND ERDR:UCKEND. DIE FREIHEIT IST EINE ILLUSION – STELL DICH DER D:USTEREN REALIT:AT." - CHAT-GPT

A-DRESDEN.ORG

ANARCHISTISCHES NETZWERK DRESDEN