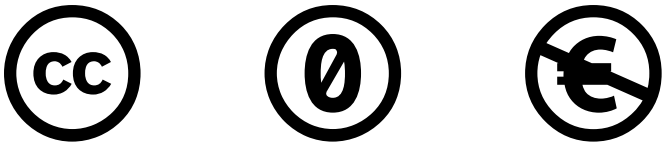
INFORMATIONSSICHERHEIT FÜR AKTIVIST*INNEN



1 Informationssicherheit für Aktivist*innen

Dieses Anleitung zielt darauf ab, einen knappen Überblick zur Informationssicherheit für alle zu bieten, die sich in emanzipatorischen Kämpfen gegen Machtstukturen befinden. Sie umfasst eine Ansammlung von Wissen und Praktiken, die aus persönlichen Erfahrungen, Gesprächen mit Hackern und anderen Aktivist*innen, Hacker-Konferenzen und Universitätskursen zu Computersicherheit und Kryptographie entstanden sind. Der beste Schutz bleibt, Fähigkeiten mit Leuten auszutauschen, denen du vertraust.

Wenn du Korrekturen, Fragen oder Ergänzungen hast, melde dich bei uns (email: activist-security riseup net). Unsere Perspektive ist größenteils aus westlichen Ländern, wir freuen uns besonders über Ergänzungen zu Repression und Taktiken an anderen Orten der Welt.

2 Inhaltsverzeichnis

3 Einleitung

Technologischer Fortschritt hat es nahezu unmöglich gemacht, sich gegen ausreichend starke Angreifer*innen zu schützen (hier [1] ein gruseliges Beispiel). Glücklicherweise haben die meisten von uns nicht die NSA am Hals und die lokalen Behörden haben oft nur begrenzte Möglichkeiten (siehe z.B. dieser Artikel [2] über Polizei-Kooperation). Der Trick ist, ausreichend vorsichtig zu sein, aber die eigene Handlungsfähigkeit zu bewahren.

Dieses Anleitung versucht, die Möglichkeiten als auch die Grenzen aufzuzeigen. Er ist in Folgende Punkte unterteilt:

- **Sicherheitsbewusstsein** zeigt die soziale Seite der Dinge.
- **Physische Sicherheit** beschreibt die physische Absicherung von Informationen.
- **Herkömmliche Kommunikation** behandelt die Pre-Internet-Form der Kommunikation.
- **Digitale Grundsicherheit** diskutiert das Aufbauen einer digitalen Basis von der du kommunizieren kannst.
- **Internetdienste** zeigt Probleme von und Alternativen zu gebräuchlichen Internet-Kommunikationsdiensten auf.

4 Sicherheitsbewusstsein

- **Das so-viel-wissen-wie-nötig-Prinzip**: teile Informationen nur mit denen, die sie brauchen.
- Etabliere einen Raum, in dem Leute merken, wann sie keine neugierigen Fragen stellen sollten und nicht beleidigt sind, wenn Informationen nicht mit ihnen geteilt werden.
- Es ist nicht nötig zu wissen, wer in welcher Gruppe ist und sich an welchen Aktionen beteiligt. Gib nicht mit solchen Dingen an und unterbreche andere, wenn sie es tun. Du kannst nichts aus Versehen ausplappern, was du nicht weißt.
- Bewahre keine unnötigen Informationen (z.B. Plenumsprotokolle) auf und halte deine Wohnung frei von belastendem Material. Mache keine Bilder von Aktionen, auch keine verpixelten, sie können Menschen trotzdem belasten (Quelle [3]).
- Bringe Pseudonyme nicht mit öffentlichen Informationen zusammen (z.B. wenn möglich, speichere keine Emailadressen von Aktivist*innen unter ihren Namen oder Gruppen).
- Lass dich nicht von Paranoia lähmen. Versuche eine realistische Einschätzung der Bedrohung zu bekommen und verdächtige Menschen nicht, Spitzel zu seien, nur weil sie nicht subkulturellen Normen entsprechen.

5 Physische Sicherheit

Während kaum eine unserer Wohnungen erfolgreich eine polizeiliche Durchsuchung abwehren kann, ist es möglich, sich gegen Faschist*innen und staatliche Agent*innen zu Wehr zu setzen.

Unbekanntheit: Es kann praktisch sein, an einem Ort zu wohnen, an dem du nicht gemeldet bist und dessen Fassade sich keine subkulturellen Symbole befinden. Sei trotzdem darauf vorbereitet, dass ausreichend motivierte Mächte der Finsternis dein Zuhause finden und angreifen können.

Passiver Schutz: Um sich vor feindlich gesinnten Kräften von draußen zu schützen, ist es gut, eine geschlossene Gruppe zu bilden. Eine standhafte Haustür und handverlesene Schlüsselvergabe bringen schon eine Menge. Vergitterte Erdgeschoss- oder Kellerfenster und das Verstärken von Fensterscheiben mittels splitterfreier Folie kann weiteren Schutz bieten.

Aktiver Schutz: Eine Sirene und eine Außenlichtanlange helfen größtenteils gegen physische Angriffe, können aber auch bei polizeilichen Durchsuchungen wertvolle Zeit bringen.

Ablaufplan: Habe eine Checkliste („was tun bei einer Polizeidurchsuchung“) und die Telefonnummer deines Anwalts/deiner Anwältin neben der Wohungstür und neben deinem Haustelefon, wenn du noch eines hast.

In manchen Gerichtsbarkeiten kann es helfen, private Zimmer mit Namen zu kennzeichnen, um die Polizei an der Durch-

suchung zu hindern, wenn diese sich nur gegen einzelne Bewohner*innen richtet. Dies gibt aber auch Identitäten aller Bewohner*innen für alle Gäst*innen preis und verweist die Polizei nur auf die ohnehin existierende Gesetzeslage, die von ihr ohnehin häufig ignoriert wird.

Du solltest dir bewusst sein, dass die Bullen und andere Dienste dich möglicherweise außerhalb deiner Wohnung legal durchsuchen dürfen und in einigen Jurisdiktionen kannst du in den Knast kommen, wenn du dich weigerst, Passwörter für deine Geräte rauszurücken (Quelle [4]).

6 Herkömmliche Kommunikation

Mit einer halbwegs sicheren Wohnung, lehn dich erstmal zurück und lass uns mal gucken was unsere Freund*innen so unternommen haben.

6.1 Persönliche Unterhaltungen

Moderne Technik erlaubt heutzutage die Überwachung des gesprochenen Wortes auch aus weiter Entfernung und selbst Mikrofon-unfreundlichen Umgebungen, wie Schwimmbädern oder Konzerthallen, können theoretisch mit moderner Störgeräuschausblendung abgehört werden. Nichtsdestotrotz ist ein kleiner Spaziergang immer noch eine recht sichere Möglichkeit der Kommunikation, solange du davon ausgehst, dass sich keine versteckten Mikrofone in deiner Kleidung oder mitgeführten Gegenständen befinden (das schließt Mobiltelefo-

ne ein!) Wenn du wirklich mehr Sicherheit benötigst, kannst du in einem sichtgeschützem Raum Nachrichten auf ein Blatt Papier schreiben (z.B. unter einer Decke).

Geschlossene Räume sind sogar noch leichter abzuhören. Von heiklen Meetings in etablierten Autonomen Zentren, alternativen Hausprojekten oder linken Kneipen ist deshalb strengstens abzuraten. Wo wir bei persönlichen Unterhaltungen sind, mit moderner Technik können sogar vermummte Demonstrant*innen demaskiert werden (Illustration [5], paper [6]), und die Videoüberwachung gebräuchlicher Treffpunkte ist ein weiterer Grund, sie für vertrauliche Treffen zu meiden.

6.2 Briefe

Dir ist hoffentlich bereits aufgefallen, dass die Vertraulichkeit von Briefpost bestenfalls Glücksspiel ist (hier z.B. ein deutscher Artikel über Postüberwachung). Codewörter sind die letzte Möglichkeit für Eingesperrte und Verzweifelte, aber die Geschichte hat gezeigt, dass geheime Methoden (z.B das Tauschen von Buchstaben) als einzige Sicherheit sehr leicht zu knacken sind.

6.3 (Mobil-)Telefone

Das Wichtigste ist davon auszugehen, dass alle Informationen (Anrufe, SMS, mobiles Internet) , die mittels (Mobil-)Telefon ausgetauscht werden, von Behörden oder potentiell auch anderen Feinden abgefangen werden. Es werden ETSI-Abhör-

schnittstellen benutzt, die für in der EU eingesetzte Mobilfunktechnik verpflichtend und (daher überall verfügbar) sind (Quelle [7]), aber noch dazu können andere motivierte Akteur*innen Daten in einer lokalen Mobilfunkzelle mit Technik für ein paar hundert Euro abgreifen (Quelle [8]).

6.3.1 Die Mobiltelefone an sich sind identifizierbar!

Das Zweitwichtigste, was man über Mobiltelefone wissen muss, ist dass sie eine eindeutige IMEI-Nummer besitzen, die sie im Mobilfunknetz identifiziert. Bei deinem Telefonanbieter ist die IMEI mit der SIM-Karte verknüpft. **Das bedeutet wenn du eine neue SIM-Karte in dein altes Telefon steckst, kann sie ganz einfach der alten SIM-Karte zugeordnet werden.** Für ein safe phone müssen also sowohl Telefon als auch SIM-Karte auf eine Weise beschafft und benutzt werden, die es nicht mit anderen Informationen in Verbindung bringen, z.B. indem Telefone und vorregistrierte SIM-Karten bar bezahlt, oder mit Falschangaben anonym registriert werden (wo das überhaupt möglich ist), zum Beispiel über TOR (siehe unten). Neben den Strafverfolgungsbehördne können auch private Firmen möglicherweise an die Daten kommen, mit denen deine Mobilfunknummer registriert wurde (Quelle [9]).

6.3.2 Bewegungsprofile

Um erreichbar zu sein, melden sich Mobiltelefone regelmäßig bei der *base station*, in die sie eingebucht sind, was das Telefon in der Stadt in einem Minimalradius von 400m um

den Funkturm ortet (Quelle [10]). Diese Information wird üblicherweise von Mobilfunkanbietern gespeichert und ist daher ohne vorherige gezielte Überwachung verfügbar (Quelle [11]). Bei Nutzer*innen zentraler Ortungsdienste (wie Google Maps) kann die Polizei möglicherweise sehr genaue Langzeit-Bewegungsprofile vom Anbieter bekommen (Quelle [12]).

Bei gezielter Überwachung ist es durch Triangulationen und Anfragen möglich, dein Telefon auf 50m genau zu orten (Quelle [13]), bei GPS-fähigem Telefonen sogar auf 5m ((Quelle [14]). Um zeitlich genauere Bewegungsprofile erstellen zu können, benutzen Behörden manchmal *Stille SMS*, damit sich dein Gerät öfter bei dem nächsten Sendemast meldet (Quelle [15]).

Als letzte Möglichkeit kann die Polizei sogenannte *ISMI-Catcher* benutzen, die vorgeben, sie wären der nächste (also signalstärkste) Sendemast und alle Daten der Telefone aufzeichnen, die sich bei ihnen einbuchen, auch Telefongespräche und SMS (Quelle [16], einige reale Beispiele).

Die Polizei ist dafür bekannt, Geodaten für alle möglichen Vorfälle zu nutzen und langfristige Telefonüberwachung von Dutzenden Personen schon bei den lächerlichsten Vorwürfen einzusetzen. IMSI-Catcher wurden sogar schon bei Sitzblockaden gegen Nazi-Aufmärsche eingesetzt. Du solltest also diese Möglichkeit nicht unterschätzen.

6.3.3 Raumüberwachung/ Stille Anrufe

Es wird kontrovers diskutiert, ob es möglich ist, Handymikrophone anzuzapfen auch wenn grade kein Anruf getätigt wird.

Dieser [17] Artikel deutet darauf hin, dass das FBI dazu in der Lage ist; während diese Nachforschungen andeuten, dass es standartmäßig eingebaut sei. Wir *vermuten*, dass es nur bei Zielen mit höchster Priorität eingesetzt wird, denn wenn jeder Bullenladen am Arsch der Welt dazu in der Lage wäre, würde es dazu schon mehr Hinweise darauf geben.

Open Source Smartphone-Betriebsysteme bieten keinen Schutz gegen solche Angriffe, da es üblicherweise eine direkte Verbindung vom Mikrofon zur (immer proprietären, um Regularien zu entsprechen) Baseband-Firmware gibt, die man nicht verlässlich abstellen kann. Um das Ganze noch schlimmer zu machen, können sich selbst Telefone ohne SIM Karte mit dem stärksten Netzwerk verbinden (für Notfalldienste), und es gibt keine Möglichkeit zu überprüfen, ob der Offline- / Flugzeug-Modus hält, was er verspricht. Smartphones können zusätzlich von bösartigen Apps überwacht werden (siehe *Smartphones*).

Um sicher zu gehen, ist es ratsam das Handy zuhause zu lassen, wenn du zu vertraulichen Treffen gehst, oder zumindest die Batterie ein paar Kilometer vor der Treffpunkt zu entfernen, da die Teilnehmenden, Ort, Zeit und Dauer eines Treffens leicht zu erfahren wären, wenn 30 Leute gleichzeitig ihre Telefone ausschalten. Insbesondere wenn du dich mit einer kleinen Gruppe in einer dicht bewohnten Gegend triffst, könntet ihr die angeschalteten Telefone einfach an einem Ort außer Hörweite aufbewahren (z.B. im Kühlschrank zwei Räume weiter).

Des Weiteren sollte erwähnt werden, dass Mobiltelefone ihren Betriebsmodus (Bereitschaft, Beschäftigt) übermitteln, und sich aus dem Netz abmelden, wenn sie ordnungsgemäß runtergefahren werden (sodass das ein anderes Muster ergibt, als wenn einfach der Akku rausgerissen wird).

Wir empfehlen dir, deine tägliche Routine als Aktivist*in so aufzubauen, dass du dich nicht auf Mobiltelefone verlassen musst. Mobiltelefone und SIM-Karten sollten nach der Aktion zerstört werden. Wo sie für langfristigeere aktivistische Infrastruktur notwendig sind, sollten Mobiltelefone und SIM-Karten im internen Netzwerk regelmäßig (z.B. alle 6 Monate) gleichzeitig ausgewechselt werden, um eine Identifikation durch Orts- oder Kommuniktationsmuster zu vermeiden.

7 Digitale Grundsicherheit

Traditionelle Kommunikationswege fühlen sich also gar nicht mehr so sicher an, wie steht also mit dem Internet aus? Als Erstes müssen wir ein sicheres Gerät finden, auf dem wir es benutzen können. Wenn es um Informationen geht, wird der Sicherheitsbegriff in Integrität, Geheimhaltung und Verfügbarkeit unterteilt. Wir schauen gleich, was das bedeutet, aber zunächst lass uns über Verschlüsselung reden.

7.1 Verschlüsselung und Passwörter

Wir werden an dieser Stelle nicht in die Details gehen, aber die grundlegende Idee digitaler Verschlüsselung ist, dass es extrem viele Möglichkeiten gibt, was der Schlüssel zu verschlüsselten Daten ist. Bei genug Möglichkeiten dauert es zu lange, alle Schlüssel auszuprobieren (eine *brute force*-Attacke), wobei alte Verschlüsselungsmethoden geknackt werden, da Computer schneller werden (zum Thema was die NSA scheinbar entschlüsseln kann, siehe hier [18]). Weil sich Menschen riesige Schlüssel auch nicht merken können, benutzen Computer oft eine echt langsame Funktion, um den Schlüssel von einem Passwort abzuleiten. Das ist okay wenn jemand das Passwort ein- oder zweimal eingibt, aber erschwert es, alle möglichen Passwörter durchzuprobieren. Aber wenn dein Passwort *1312* oder *Revolution* oder so ist, kann es mit einer *Wörterbuchattacke* geknackt werden. Eine Möglichkeit ist es, ein komplett zufälliges Passwort zu erzeugen (howto [19]), auf Papier zu notieren, es sich zu merken und den Zettel nach einigen Tagen zu zerstören.

Falls das zu kompliziert klingt oder du Angst hast, das Passwort nach einem Urlaub zu vergessen oder so, ist es am Besten, eines der folgenden Konzepte zu verwenden, und es mit *zufälligen Mustern* zu kombinieren.

Schema 1: die ersten Buchstaben eines zufälligen Satzes zu verwenden (**D**ieser **S**icherheitsratgeber **i**st **1 s**uper *%3* **P**asswort**!**)

Schema 2: einfach viele zufällige Worte aneinander zu hängen (AnanasFernseherVerwirrung$2Salat).

Aber auch ein gutes Passwort ist für'n Arsch, wenn die Bullen einen Virus auf deinen Computer gepackt haben, und das Passwort sehen, während du es tippst, was uns zum nächsten Punkt bringt.

7.2 Aussuchen deines Gerätes (Integrität)

Heutzutage ist kein Gerät völlig unter deiner Kontrolle. Laptops und Computer werden mit undurchsichtiger Low-Level Software („*firmware*"), die von den Hersteller*innen kontrolliert wird[A].

7.2.1 Smartphones

Das Gleiche gilt für Tablets; und bei Smartphones oder Tablets mit SIM-Karten-Slot ist es noch schlimmer, weil sie zusätzlich aus dem Netz kontrolliert werden (Quelle [29]) und diese kontrolle dazu missbraucht werden könnte, auf persönliche Daten auf dem Gerät zuzugreifen (source [30]). Dazu kommt, dass Smartphones komplexe Rechner sind, die oft von den Hersteller*innen keinen Sicherheitsupdates bekommen, und

[A] Technischer Hintergrund: auf den meisten Intel-basierten Computern läuft eine Software, die das System parallel zum Betriebssystem kontrolliert (AMT [20]), die in der Herstellerfirmware "deaktiviert" werden kann, aber die diese Firmware ist proprietäre Software und moderne Intel-Prozessoren starten üblicherweise nur signierte Firmware (Intel Boot Guard [21]), sodass du nie in der Lage sein wirst, alternative Firmware wie Libreboot [22] zu verwenden, und selbst wenn du könntest, gäbe es immer noch Dinge in deinem Computer, zu dem du den Quellcode nicht hast (noch [23] mehr [24] technischer [25] Hintergrund [26] hier [27]). Es gab bereits Fälle, in denen Schadsoftware AMT benutzt hat (Quelle [28]).

so leichte Ziele für Angriffe sind (Quelle [31]). Neben hinterhältigem Attacken aus dem Netz, werden auch bösartige Apps für die Überwachung eingesetzt (Quelle [32]) und die Menge an Umgebungssensoren macht Smartphones zu prima Spionagegeräten, selbst wenn du das Mikrophone rausreißen würdest (z.B. 1 [33],2 [34]). Außerdem sind Smartphones von Grund auf dafür gemacht, massenhaft Daten über Leute zusammenzutragen (Gruselbeispiel: Artikel [35], paper [36]) - Daten, die öfter für Behörden (mit oder ohne Anfragen) einsehbar sind, als nicht.

Daher wird vom Benutzen von Smartphones für vertrauliche politische Arbeit strengstens abgeraten, da auch die Sicherheit alternativer Internetdienste wie Jabber/XMPP auf der Mehrzahl der Geräte stark beeinträchtigt ist[B]. Ja - uns ist schon klar dass die meisten Menschen, die das hier lesen, ein Smartphone als ihr Hauptkommunikationsmittel verwenden. Bei der Suche nach einem halbwegs sicheren privatem Gerät gibt es nur so richtig die Wahl zwischen Android und iOS, weil Randgruppen-Alternativen wie Sailfish OS [37] bislang noch nichtmal persönliche Daten verschlüsseln können. Google entwickelt Android, um eine Plattform für Werbung und Datensammlung zu kontrollieren. Apples iOS hat viele eingebaute Sicherheitsfunktionen, aber so praktische Dinge wie remote wipe werden selbst mit einem hohen Eingriff in die Privatsphäre bezahlt, und von Ausnahmen [38] abgesehen, kooperiert die Firma im Allgemeinen mit staatlichen Einrich-

[B] Diese Sicherheitsanalyse zeigt recht gut dass auch ohne böse Absichten Mobilgeräte einfach nicht besonders sicher sind.

tungen.

Open Source - Varianten von Android (wie *Replicant* [39], *Copperhead OS* [40] oder, gebräuchlicher, *Lineage OS* [41]) bieten ein Google-freies Android, mit dem Nachteil, viele praktische Apps zu verlieren, während die generellen Nachteile von Smartphones weiterhin bestehen. Sie erfordern üblicherweise das Entsperren des *boot loaders* des Gerätes, damit es überhaupt möglich ist, ein alternatives Android darauf zu installieren, was dann z.B. die Polizei auch tun könnte, wenn sie für ein paar Stunden Zugriff auf dein Gerät hat (Diskussion [42]). Wo die alternativen Android-Varianten manchmal Sicherheitsupdates für alte Geräte anbieten, wo der Hersteller das nicht tut, sind alternative Android *ROMs* noch dazu in Wirklichkeit oft schlecht mit Updates versorgt (Diskussion 1 [43], 2 [44]; Übersicht für LinageOS [45]).

Falls nötig, ist unser Rat, am besten ein Tablet **ohne SIM-Karten-Slot** zu benutzen (weil es nicht aus dem Mobilfunknetz kontrolliert werden kann), oder falls nötig ein Smartphone, welches von Copperhead OS, oder von Lineage OS gut unterstützt wird.

7.2.2 Laptops and Computer

So viel wie möglich freie Open Source - Software auf einem Laptop oder Computer laufen zu lassen, gibt dir eine Menge Kontrolle zurück. Bei geschlossene Software wie Microsoft Windows oder Apples Mac OS besteht die Gefahr, dass die Firmen den Stafverfolgunsbehörden dabei helfen, gegen das Verbrechen zu kämpfen, und in deinen Computer einzubre-

chen. Bei *Linux* oder anderen Open Source - Alternative ist der Quellcode für alle offen einsehbar und somit ist es wesentlich schwieriger, ihn zu manipulieren. Übrigens, der beste Schutz gegen Viren ist, einfach keine Software von irgendwelchen belieben Websites herunterzuladen und keine potenziell gefährlichen Email-Anhänge von Personen zu öffnen, denen du nicht vertraust. Das schließt Microsoft Office Dokumente ein, da sie für diverse Angriffe benutzt werden können (Quelle [46]). Antiviren-Software bietet nur überaus lückenhaften Schutz, aber ist selbst angreifbar (Quelle [47].

Es gibt viele verschiedene Bündel des Linux Kerns mit diverser Open Source Software, die Distributionen genannt werden. Wenn der Computer für vertrauliche aktivistische Arbeit genutzt wird, kann Tails [48], eine Distribution, die einen Fokus auf Sicherheit und Anonymität legt, neben einem anderen Betriebssystem, z.B. einer anderen Linux-Variante, installiert werden.

Für hauptsächlich persönliche Nutzung sind die folgenden beiden Distributionen weniger auf Sicherheit angepasst, aber relativ einfach zu installieren, zu nutzen und zu aktualisieren:

- *Ubuntu Linux* [49] ist die Basis für Linux Mint und hat eine Firma hinter sich, die versucht, eine möglichst benutzer*innenfreundliche Linux-Variante zu schaffen. Es basiert selbst auf *Debian* [50], einer der ältesten Community-Distributionen. Die Firma gibt die Entwicklungsrichtung vor, aber es gibt dennoch eine starke Community.

- *Linux Mint* [51] bietet eine der schmerzfreisten Wege, ein Open Source System mit vielen, wahrscheinlich bekannten, Anwendungen wie Firefox, VLC Player, LibreOffice etc. zu bekommen. Allerdings gab es ein paar Diskussionen über ihre Sicherheitsrichtlinien, und du solltest im Update-Manager "Stabilität und Sicherheit optimieren" auswählen und regelmäßig *alle* Updates (auch Level 4) im Update-Manager auswählen, um auf der sicheren Seite zu sein. Es gibt verschiedene Oberflächen, von denen *XFCE* schlicht und schnell ist, und auch auf älteren Geräten noch gut läuft, und *Cinnamon* ein wenig gehobener.

- *Installation*: Stell sicher, das alle deine wichtigen Daten auf einem *externen* Medium gespeichert ist (externe Festplatte oder USB-Stick) und versuche Unterstützung von einem Computergeek zu bekommen, falls möglich. Es ist möglich Linux und Windows auf dem Rechner zu installieren (Dualboot), aber gehe davon aus, **dass alles überschrieben werden kann**. Für den Anfang, gibt es hier eine Anleitung, Ubuntu von einem USB-Stick zu installieren, die auch mit Linux Mint funktionieren sollte, indem du einfach deren Dateien runterlädst, und hier gibt es ein Video, wie man Linux Mint installiert. Aber lies erstmal den nächten Absatz…

7.3 Festplattenverschlüsselung (Geheimhaltung)

Verschlüssele deinen Computer! Alle weiteren Ratschläge für Software und Kommunikation bringen gar nichts, wenn dein Computer nicht sicher ist. **Die Verschlüsselung bringt nur was bei Angriffen gegen ausgeschaltete Computer, wenn die Polizei deinen Computer entsperrt mitnimmt, werden sie einfach deine Daten kopieren.** Ein gesperrter oder schlafender Rechner mit vernünftigem Passwort ist besser als nichts, aber das Gerät sollte so oft wie möglich runtergefahren werden. **Wenn die Polizei an deiner Tür klopft, renne als erstes zu deinem Coputer und drücke den Power-Knopf, bis er ausgeht.**

Es gibt hauptsächlich drei Arten, wie du deine Daten verschlüsseln kannst:

7.3.1 Verschlüssele deine Eigenen Dateien

Wenn du nicht sicher bist, nimm das hier: ausschließlich deine „Eigene Dateien" werden verschlüsselt (das schließt Firefox Bookmarks etc. ein), den Rest aber nicht.

- ▲ Vorteile:
  - △ Der Computer funktioniert ziemlich normal und deine persönlichen Daten sind trotzdem ziemlich sicher.

- ▼ Nachteile:
  - ▽ Du solltest ein langes Benutzer*innenpasswort benutzen, welches du jedesmal eintippen musst, wenn du den Bildschirm sperrst.
  - ▽ Es ist möglich, deine Programme (z.B. Firefox, GPG) so zu manipulieren, sodass sie deine Passwörter freigeben etc.

Anleitung :
Während der Linux Installation, „Eigene Dateien verschlüsseln"beim Erstellen eines Nutzers/Nutzerin auswählen.

7.3.2 Das ganze System verschlüsseln

Das bedeutet, dass nur ein sehr kleiner Teil auf deiner Festplatte unverschlüsselt bleibt und alles andere - deine Programme etc. - verschlüsselt ist

- ▲ Vorteile:
  - △ Das macht es schwerer z.B. eine falsche Version des Firefox oder GPG auf deinem Computer zu packen.
  - △ Du brauchst bloß ein sehr starkes Passwort einmal beim Hochfahren und dann reicht ein Kürzeres für deine Bildschirmsperre.
- ▼ Nachteile:
  - ▽ Du musst deinen Computer starten, das Passwort eingeben und erst dann fährt der Rechner weiter hoch.

- ▽ Du musst dir zwei Passwörter merken.

Anleitung :
Während der Linuxinstallation bei Installationstyp „Verschlüssele die neue (Linux Mint/Ubuntu)-Installation für mehr Sicherheit".

7.3.3 Einen verschlüsselten Container benutzen

Eine externe Festplatte oder eine sehr große Datei (ein "Container") werden verschlüsselt und du musst sie separat entsperren / Dateien rein und raus schreiben / wieder sperren.

- ▲ Vorteile:
  - △ Kann benutzt werden, um Daten zwischen verschlüsselten Computern auszutauschen.
  - △ Kannst auf externen Festplatten benutzt werden.
  - △ Kann auf Windows und Mac OS benutzt werden.
  - △ Kann als ein zusätzlicher sicherer Ort auf einem schon verschlüsselten Linux benutzt werden, der normalerweise gesperrt ist.
  - △ Hat eine spezielle Funktion, die falsche Daten anzeigt, wenn du gezwungen werden solltest, ein Passwort rauszurücken.
- ▼ Nachteile:
  - ▽ Alle möglichen temporären Daten wie z.B. von LibreOffice, Thunderbird Email, Firefox-Profile etc., sind nicht verschlüsselt.

▽ Muss separat geöffnet und geschlossen werden.

Anleitung :
Veracrypt [52] installieren und der Anleitung [53] folgen.

7.3.4 Android and iOS

▷ **Android:** zu *Einstellungen -> Sicherheit* gehen und auf *Gerät verschlüsseln* drücken ausführlichere Anleitung

7.3.5 Einschränkungen

Dein Passwortfeld muss ja von irgendwo kommen und so gibt es immer Daten auf deinem Gerät, die nicht verschlüsselt sind und die manipuliert werden können (z.B. Ersetzen deines Linux-Passwortfelds mit einem, dass dein Passwort an die Polizei schickt). Das kann mit einigen Tricks erschwert werden[C], aber das realistischste Szenario ist eine einfache Hausdurchsuchung.

7.4 Datensicherung (Verfügbarkeit)

Wenn es zu einer Hausdurchsuchung (oder einem einfachen Einbruch) kommt, wird auch das best-verschlüsselte Gerät einfach von der Polizei mitgenommen. Um dir ein wenig Stress

[C] Man kann diesen Angriff nur vereiteln, in dem man die unverschlüsselten Daten signiert und die Signatur von einem Teil des Computers überprüfen lässt, dem man vertraut. Das kann entweder mittels eines TPMs, oder leichter verfügbar per SecureBoot und Vertrauen in die Herstellerfirmware erreicht werden (das machen moderne Linux-Distributionen). Ein paar Hinweise: 1 [54], 2 [55]

zu ersparen, bringe **regelmäßig** verschlüsselte Kopien deiner Daten zu jemanden außerhalb deiner Wohnung, idealerweise zu Leuten, die weder Verwandschaft, noch in der selbe Gruppe aktiv sind.

Wenn wir schonmal dabei sind: selbst öffentliche Daten sollten nicht bei IT Firmen gelagert werden, da sie diese einfach löschen [56] oder aus Versehen verlieren könnten.

8 Internetdienste

Mittlerweile können wir hinter verschlossenen Türen unseren gut gesicherten Laptop nutzen, um lange Sicherheitsratgeber zu schreiben, aber wie können wir jetzt eigentlich sicher mit Leuten sprechen?

Abgesehen von den unten genannten technischen Aspekten, bieten alternative Provider die einen weiteren Grad an Sicherheit, da sie Daten verschlüsselt lagern und nicht mit Behörden zusammenarbeiten. Eine Liste alternativer Tech-Kollektive gibt es hier [57], noch mehr hier [58] und hier [59] eine Liste alternative Email-Anbieter. Wir empfehlen, sich Alternativen zu Riseup.net zu suchen, weil ihre exponierte Postition und die rechtliche Lage in den USA eine Menge Druck auf ein einzelnes Tech-Kollektiv erzeugt, und sie Anfang 2017 in zwei unemanzipatorischen Kriminalfällen mit den Behörden kooperiert haben (Quelle [60]). Wir glauben nicht, dass existierende Infrastruktur dringend von Riseup abgezogen werden muss.

8.1 Ein paar Worte zu Web-Browsern

Web-Browser wie Mozilla Firefox oder Google Chrome sind komplexe Monster, und viele Websites verfolgen ihre Benutzer*innen. Das Riseup-Kollektiv hat eine kompakte Anleitung [61], wie du deinen Browser sicherer nutzen kannst.

8.2 Anonymität

Der ganze Punkt des Internets ist die Verbindung von zwei Computern, wie deinen und sagen wir… *Youtube*. Damit die Katzen-Videos ihren Weg zurück zu dir finden, müssen die Computer auf dem Weg (*Router*) deine Internetadresse kennen. Das Problem an der Geschichte ist, dass wenn irgendwelche Computer auf dem Weg von der Polizei überwacht werden, oder du eine böse Website besuchst, wie die der Polizei, sie deine Internetadresse zu deinem Aufenthaltsort zurückverfolgen können, oder sie mit deiner restlichen Online-Aktivität verknüpfen (wie z.B. deine Mails abrufen). Um dies zu vermeiden, gibt es zwei Methoden, die für zusätzliche Sicherheit idealerweise miteinander beide kombiniert werden sollten.

Die erste Methode besteht darin, eine Software zu benutzen, die *TOR* [62], oder *The Onion Router* (Der Zwiebel Router) heißt. Runtergebrochen funktioniert das wie folgt: du sendest Daten die auf 3 verschiedenen Ebenen verschlüsselt sind (daher die Zwiebel) über drei Computer(*TOR-Knoten*), wobei der erste Knoten deine Internetadresse kennt und den zweiten Knoten, der kontaktiert werden soll (aber nicht das Ziel); der

zweite Knoten weiß gar nichts (außer den Kontakt zum dritten Knoten), und der dritte Knoten kennt das Ziel, aber nicht den Ursprung. Für ein Maximum an Sicherheit solltest du Tails [63] auf einem USB-Stick installieren und statt deinem normalen Linux / Windows oder sonstigen Betriebssystem deinen Computer mit Tail starten. Auf diese Weise hast du die größten Chancen, dass es keine Verknüpfung zwischen deinen anonymen Aktivitäten und deiner normalen Internetnutzung gibt. Die nächst-sicherste Möglichkeit ist, den Anleitungen zu folgen (Linux [64], Windows [65], Mac OS X [66]) und benutze auf jeden Fall den TOR-Browser, wenn du vertrauliche Dinge tust.

Wenn du unbedingt ein Mobilgerät nutzen musst, gibt es eine Software namens Orbot [67] für Android-Geräte. Auf Apple-Geräten bietet der Onion browser [68] zumindest einen minimalen Browser mit TOR.

Die zweite Methode ist einfach das Nutzen öffentlicher Wlans an Orten, an denen es keine Kameraüberwachung gibt. Unglücklicherweise hat das Wlan deines Computer eine einzigartige *MAC* Adresse. Diese kann durch Software geändert werden, falls das Wlan sie speichern sollte (wie es einige Firmenportale machen, um sicherzustellen, das du die AGB schon zur Kenntniss genommen hast oder um zu gucken, ob du deine Stunde freies Internet schon aufgebraucht hast), aber am Besten benutzt du diese Methode nur, um für zusätzliche Sicherheit bei der Nutzung von TOR (idealerweise mit Tails, welches eine zufällige MAC-Adresse übertragen wird).

8.3 Email

Emails sind wie Postkarten, nimm also an, sie werden von Emailanbietern und Behörden gelesen. PGP ist eine Art deine Emails-Inhalte zu verschüsseln (die Postkarte einzupacken), aber sei dir bewusst, dass der Betreff und der Fakt wer wann mit wem, und von welchem Computer kommuniziert, nicht verborgen wird.

Immerda.ch hat eine gute deutschsprachige Einleitung [69]., wie PGP funktioniert. PGP-Verschlüsselung benötigt *Schlüssel* (spezielle Dateien, von denen der private Schlüssel mit einem Passwort geschützt ist), die wie Schloss und Schlüssel, den Zugang zu Informationen einschränken soll. Daher hängt die PGP-Sicherheit stark von der sicheren Übergabe der Schlüssel ab, also stell sicher, das du den richtigen Schlüssel bekommst, z.B. indem du ihn persönlich von der Zielperson erhältst.

Der "Surveillance Self-Defence"-Ratgeber der Electronic Frontier Foundations hat eine ziemlich gute PGP-Anleitung (Linux [70], Windows [71], Mac OS X [72]).

Du solltest deine Aktivist*innen-Mailadresse am besten gar nicht auf Mobilgeräten nutzen, aber wenn unbedingt nötig, **stell sicher dass deine Kommunikationspartner*innen dem zustimmen** und verwende K9-Mail [73] mit OpenKeychain [74] auf Android.

8.4 Mailinglisten

Wenn PGP Nachrichten zwischen zwei Leuten verschlüsselt, was ist dann mit Mailinglisten? Wenn es nur eine kleine Guppe ist, dann könnt ihr *öffentliche* PGP-Schlüssel austauschen, sodass jede*r Nachrichten so verschlüsseln kann, dass jede*r Empfänger*in sie lesen kann. Leider wird das schnell unübersichtlich, besonders wenn neue Leute hinzukommen. Daher sind Leute auf eine andere Lösung gekommen, die zwar nicht ganz so sicher ist, aber besser als nichts.

Schleuder [75] ist eine Mailinglisten-Software, die ihr eigenes PGP Schlüssel-Paar bekommt. Jede*r verschlüsselt dann die Emails mit Schleuders Mailinglisten-Schlüssel, schickt diese an die Schleuder, welche sie entschlüsselt, und für jede*n Empfänger*in einzeln verschlüsselt und verschickt. Der Nachteil ist natürlich, dass wer auch immer Schleuder betreibt, auch den Privaten Key der Schleuder besitzt, und alle Nachrichten entschlüsseln könnte. Schleuder ist ein komplexes Biest und es ist empfehlenswert, es von einem Tech-Kollektiv zu benutzen, dem du vertraust, beispielsweise von Immerda.ch [76].

8.5 Messengers / Chat

TL;DR: benutze den Rest nicht und lies unten bei **Jabber** weiter, und benutze **Signal** für außenstehende Personen (z.B. Journalist*innen) die du nicht dazu bringen kannst, Jabber zu benutzen.

Skype hat den Ruf, verschlüsselt zu sein, allerdings haben sie selbst gesagt, dass sie willens und fähig sind, Informa-

tionen an Strafverfolungsbehörden weiterzugeben, und tun dies auch. Alle deine geschriebenen Texte werden auf Skype-Servern gespeichert und können dort von der Polizei eingesehen werden (Quelle [77]).

Seit einiger Zeit werden mobile Messenger-Apps, die auf Telefonnummern basieren, immer beliebter. Wenn du in Erwägung ziehst, irgendwelche "sicheren" Messenger auf einem Mobilgerät zu nutzen, sei daran erinnert [78] erinnert, dass Kommunikation durch das Mobilfunknetz anfällig für Abhören und Manipulationen ist.

Um rauszufinden, welche deiner Kontakte dieselbe App nutzen, müssen die Apps generell Informationen über **alle** Kontakte auf ihre Server hochladen (Quelle [79]), aber sie tun das in verschiedenem Ausmaß von einer verschleierten Form der Telefonnummer bis hin zum ganzen Adressbuch. **Die Auswirkungen für Aktivist*innen sind enorm, denn wenn auch nur eine Person eine anonyme Nummer mit dem Klarnamen der Person hochläd, ist der ganze Aufwand umsonst.**

Whatsapp ist bei weitem die erfolgreichste Messenger App heutzutage, und seit kurzem behaupten sie auch, Ende-zu-Ende-Verschlüsselung (alles ist verschlüsselt zwischen dir und der Person mit der du sprichst) zu unterstützen. Allerdings ist der Quellcode ihrer Programme nicht frei verfügbar. Es gibt Probleme mit ihrer Ende-zu-Ende-Verschlüsselung, die allerdings keine Absicht zu sein scheinen (Quelle 1 [80], 2 [81], 3 [82]). In der Vergangenheit war es möglich, jede(r/m) möglich, Profildetails für jede Telefonnummer einzusehen (Quelle [83]) und es ist immer noch jede[r/m] möglich, den Online-Status

beliebiger Whatsapp-Nutzer*innen einzusehen (Quelle [84]).

Dasselbe gilt im Wesentlichen für **Threema**, da dies auch keine Open Source Software ist.

Telegram hat viele durch ihren angeberischen Altruismus überzeugt. Sie stellen tatsächlich den offenen Quellcode der clients bereit„ aber die Verschlüsselung besteht aus veralteten Techniken der 70er (Quelle [85]), muss manuell eingeschaltet werden und funktioniert für Gruppen Chats gar nicht. Auf der anderen Seite nehmen sie, wenn sie dein Adressbuch kopieren, im Gegensatz zu anderen Messengern nicht nur die Nummer sondern auch gleich die Namen mit (Quelle [86]). Passenderweise ist es dem deutschen BKA gelungen, sich in Gruppenchats zu hacken (Quelle [87]).

Nun, **Signal** [88]. Die Leute hinter Signal legen *viel* mehr Wert auf Privatsphäre als die restliche Bande der telefonnummernbasierten Messenger und waren die Ersten, die verschlüsselte Gruppechats möglich gemacht haben. Unserer Meinung nach sind Behauptungen [89], Signals Ende-zu-Ende-Verschlüsselung sei gebrochen worden, unrichtig, und tatsächlich wurden die Endgeräte gehackt, nicht die Kommunikation von Signal selbst. Auch wenn sie technisch gesehen alle Kommunikationsmuster einsehen können (nicht aber den Inhalt) (Quelle [90]), hat der Gründer Sinals zumindest einen vertrauenswürdigeren Hintergrund (Quelle [91]; und ziemlich witzige Geschichten [92] hat er auch). Dennoch ist das System zentralistisch und auch wenn die Software Open Source ist, behalten sie die volle Kontrolle über ihr Netzwerk. Signal ist für Android und iOS verfügbar. Sobald man sich mittels einer dieser Apps registriert hat,

kann eine Desktopanwendung mit der App verknüpft werden, von wo an Signal auf einem Laptop oder Computer auch ohne ein Mobilgerät benutzt werden kann. Auf Android gibt es Signal auch ohne Google Play via `https://signal.org/android/apk/`, aber Signals Erfinder hat alternative Clients explizit aufgefordert, das Netzwerk zu verlassen (Quelle [93]). Leute finden ausgefuchste Wege, um die Notwendigkeit einer Telefonnummer zu umgehen (Anleitung [94]). Alles in Allem ist Signal eine gute Wahl für Menschen, die ohnehin Android- oder Apple-Smartphones benutzen, aber **wir würden eine auf Mobiltelefonen und -Nummern basierte Plattform nicht als interne Gruppeninfrastruktur empfehlen.**

8.6 Jabber/XMPP

Willkommen bei **Jabber** / XMPP. *Endlich hast du es geschafft!* ***Das empfehlen wir momentan für vertrauliche Echtzeitkommunikation.***

Ähnlich wie bei Email, können Leute von vielen verschiedenen Anbietern (siehe Tech-Kollektive oben) miteinander reden. Auch ähnlich wie bei Email bietet Jabber standardmäßig nur eine sehr schwache Verschlüsselung. Für richtige Nachrichten, bietet *OTR* eine ziemlich brauchbare Verschlüsselungsmethode für synchrone Kommunikation (beide Leute sind gleichzeitig online). Allerdings gibt es einige Einschränkungen:

- Der Fakt, dass zwei Leute miteinander kommunizieren, wird nicht verschleiert. benutze also Psuedonyme, die nicht mit anderen Aktivitäten verbunden sind.

- OTR benutzt üblicherweise ein Authentifizierungssystem, dass auf Wissen basiert, das nur dein Gegenüber wissen kann. Es ist wichtig davon Gebrauch zu machen, um sicherzugehen, dass dein gegenüber auch wirklich die Person ist, von der du ausgehst. Ansonsten, falls es der Dunklen Seite gelingt, deinen Jabber-Anbieter zu bedrängen, kann sie sich als dein*e /Freund*in ausgeben.
- Dateien die du über Jabber versendest werden nicht durch OTR verschlüsselt.
- Audio- und Videochats in Jabber clients werden nicht standardmäßig verschlüsselt.

Einige Jabber-Clients unterstützen *OMEMO* als neuere Alternative zu OTR, welche auch Gruppenchats verschlüsseln kann und asynchrone Kommunikation unterstützt, ähnlich wie die Mobil-Messenger. Mit Conversations [95] for Android und ChatSecure [96] für iOS kann Jabber eine Alternative zu diesen Messengern sein, die sich zentraler Kontrolle entzieht. Bedauerlicherweise unterstützen nicht alle Jabber-Server die Speicherung von Nachrichten an dich, wenn du offline bist (eine Übersicht gibt es hier [97]). Auch ist die Chatsoftware für Laptops und Computer ein bisschen langsam damit, OMEMO zu unterstützen, weswegen wir bis auf Weiteres empfehlen, bei OTR zu bleiben. Als eine Alternative zu Pidgin (welches üblicherweise in den Jabber-Anleitungen vorkommt) empfehlen wir die Installation von Gajim [98].

einfachJabber.de [99] eine ausführliche deutschsprachige Einführung und Anleitungen für alle möglichen Geräte und

Systeme. Englische Toturials findest du im EFF Surveillance Self-Defence guide (Linux [100], Mac OS [101], Windows [102]).

8.7 Sprach- / Videochat

Es gibt Lösungen die Open Source sind, für eine Vielzahl von Plattformen verfügbar sind und Ende-zu-Ende-Verschlüsselung für Audio und Video anbieten (Überblick [103]). Wenn mensch mit den Nachteilen leben kann, ist Signal (siehe oben) die praktikabelste Lösung für Mobilplattformen.

Auf Laptops und Computern ist **Tox** [104], solange du es zum Laufen bringen kannst, eine ziemlich faszinierende, sehr sichere und anspruchslose Alternative. Eher traditionell bietet **Jitsi** [105] verschlüsselte Anrufe mittels entweder *SIP* oder noch besser auch Jabber/XMPP (siehe oben) - Account. **Ring** [106] ist eine weitere vielversprechende Alternative, die wir aber noch nicht getestet haben. **Mumble** [107] ist eine gute Lösung für Leute, die einen eigenen Server betreiben können und auch über das Systemli Tech-Kollektiv verfügbar.

Ein mehr Ad-hoc orientiete Methode involviert eine Technik namens *WebRTC* und benötigt nur einen modernen Web-Browser, wie Firefox oder Chrome, mit dem Nachteil, dass man einer zentralen Website vertraut, nicht bösartig zu sein (und die Verbindung zu diesem Netzwerk nicht manipuliert). **pavala.tv** [108] und **meet.jit.si** [109] sind zwei Open Source - basierte Lösungen dafür.

8.8 Blogs, Websites und Social Media

Wenn du nicht gerade eine Person mit Computersicherheits-Fachwissen in deiner Gruppe hast, solltest du wahrscheinlich keine eigene Website betreiben, da die Mächte des Bösen häufig Websites zensieren oder - möglicherweise schlimmer - Daten darüber sammeln, wer sie betreibt (Quelle [110]). Andererseits geben Social Media - Konzerne gern Daten weiter oder manipulieren emanzipatorische Inhalte auf verschiedene Weise (Quelle [111]). Die beste Alternative ist es, ein Blog bei einem der Tech-Kollektive zu eröffnen, oder ein Kollektiv, dem du vertraust, deine Website betreiben zu lassen, wenn du wirklich eine eigene Website benötigst.

9 Kurz zusammengefasst

Wenn das hier alles deinen Kopf zum Qualmen gebracht hat, ist hier unser Fazit.

9.1 TL;DR:

- Mmache Aktionen mit Leuten, denen du traust, sei ehrlich zu ihnen, aber tratsche und prahle nicht rum und behalte nicht mehr Informationen als nötig.
- Trenne deine Aktivist*innen- und bürgerliche Identität so sehr wie möglich.
- Halte Treffen an unverdächtigen Orten ohne Mobiltelefone ab.

- Installiere Linux auf deinen Rechner und verschlüssele deine Daten, lerne wie du PGP für Gruppen-Emails benutzt und bau dir ein Jabbernetzwerk mit authentifizierter OTR- oder OMEMO-Verschlüsselung für spontane Kommunikation auf.
- Lerne wie du TOR sicher benutzt.
- Teile deine Fähigkeiten mit anderen, bringt euch gegenseitig Sachen bei und bekomm keine Panik.

9.2 Beispiel-Setups

- **Laptop / Desktopcomputer:** Tails für ernsthafte Anonymität, ein verschlüsseltes Linux Mint mit TOR Browser, Thunderbird+Enigmail für verschlüsselte Email, Veracrypt um externe Medien zu verschlüsseln, Gajim für Jabber mit OMEMO-Verschlüsselung, Signal Desktop falls nötig.
- **Wenn's sein muss, Smartphone für persönliche Nutzung:** ein gut von Copperhead OS oder Lineage OS unterstütztes Android-Smartphone mit verschlüsselten Daten, Orbot für TOR, Conversations für Jabber mit OMEMO falls nötig und Signal als Messenger app.

Quellen und Links

[1] https://www.cs.tau.ac.il/~tromer/mobilesc/

[2] https://electrospaces.blogspot.de/2017/06/dutch-russian-cyber-crime-case-reveals.html

[3] https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/

[4] https://theintercept.com/2017/09/23/police-schedule-7-uk-rabbani-gchq-passwords/

[5] https://twitter.com/zeynep/status/904683388354867201

[6] https://arxiv.org/abs/1708.09317

[7] https://en.wikipedia.org/wiki/Lawful_interception

[8] https://ferrancasanovas.wordpress.com/cracking-and-sniffing-gsm-with-rtl-sdr-concept/

[9] https://medium.com/@philipn/want-to-see-something-crazy-open-this-link-on-your-phone-with-wifi-turned-off-9e0adb00d024

[10] https://en.wikipedia.org/wiki/Cell_site#Range

[11] http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

[12] https://www.cnet.com/how-to/how-to-delete-and-disable-your-google-location-history/

[13] https://en.wikipedia.org/wiki/U-TDOA

[14] https://de.wikipedia.org/wiki/GSM-Ortung#cite_note-3GPP43059-3

[15] https://en.wikipedia.org/wiki/Short_Message_Service#Silent_SMS

[16] https://en.wikipedia.org/wiki/IMSI-catcher

[17] http://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/

[18] https://theintercept.com/2017/05/11/nyu-accidentally-exposed-military-code-breaking-computer-project-to-entire-internet/

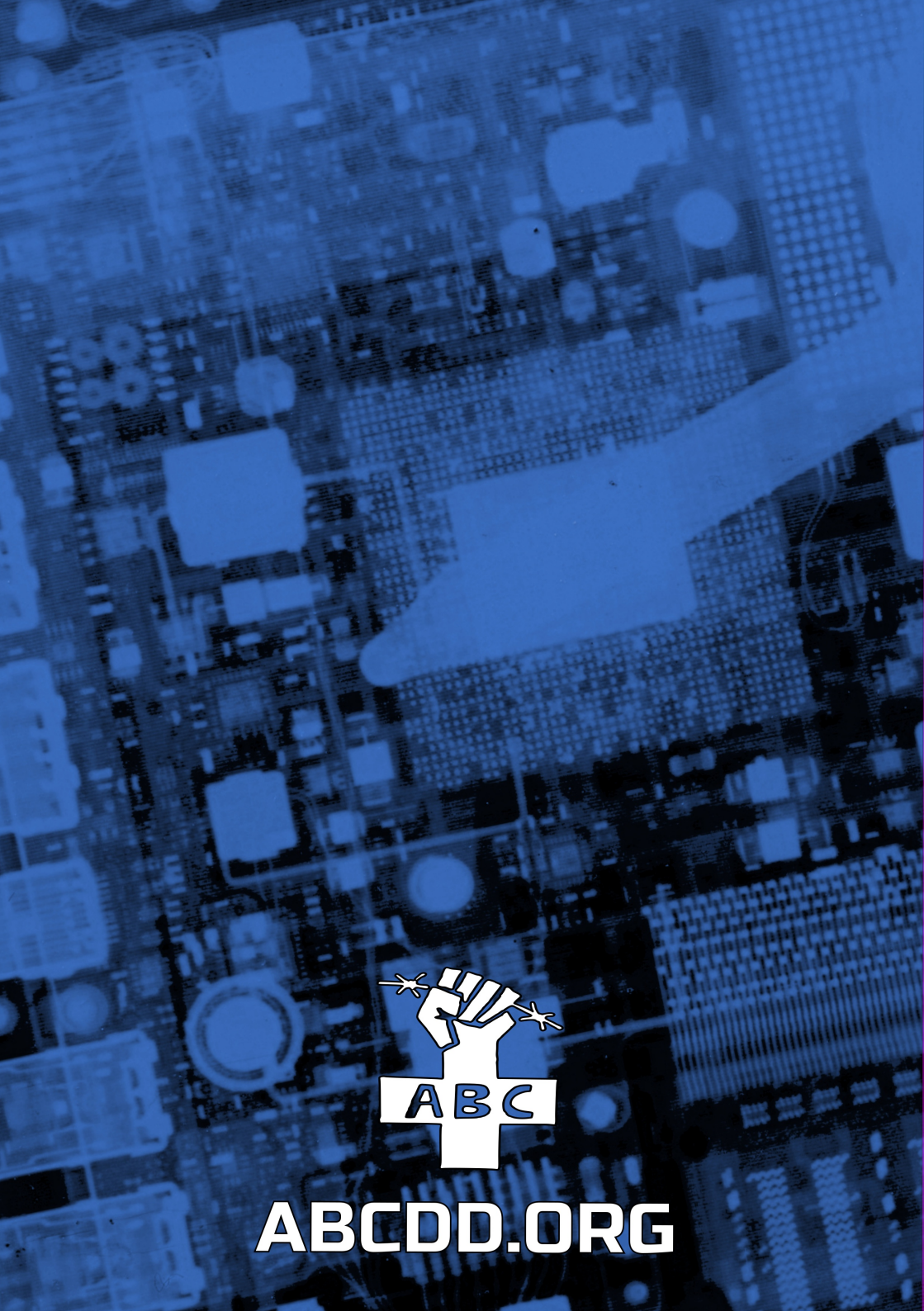
[19] https://ssd.eff.org/en/node/23/#0

[20] https://en.wikipedia.org/wiki/Intel_Active_Management_Technology
[21] https://mjg59.dreamwidth.org/33981.html
[22] https://libreboot.org/
[23] https://github.com/ptresearch/me-disablement/blob/master/How%20to%20become%20the%20sole%20owner%20of%20your%20PC.pdf
[24] https://embedi.com/blog/bypassing-intel-boot-guard
[25] https://github.com/flothrone/bootguard
[26] https://schd.ws/hosted_files/osseu17/84/Replace%20UEFI%20with%20Linux.pdf
[27] http://blog.ptsecurity.com/2017/08/disabling-intel-me.html
[28] https://www.bleepingcomputer.com/news/security/malware-uses-obscure-intel-cpu-feature-to-steal-data-and-avoid-firewalls/
[29] http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone
[30] https://www.tomsguide.com/us/backdoor-samsung-galaxy-devices,news-18470.html
[31] http://www.pcworld.com/article/2953052/security/most-android-phones-can-be-hacked-with-a-simple-mms-message-or-multimedia-file.html
[32] http://www.wthr.com/article/tapping-your-cell-phone
[33] https://mjg59.dreamwidth.org/46952.html
[34] https://crypto.stanford.edu/gyrophone/files/gyromic.pdf
[35] https://www.bleepingcomputer.com/news/security/234-android-applications-are-currently-using-ultrasonic-beacons-to-track-users/
[36] http://christian.wressnegger.info/content/projects/sidechannels/2017-eurosp.pdf
[37] https://sailfishos.org/
[38] https://www.engadget.com/2016/03/28/apple-s-encryption-battle-with-the-fbi-is-over-for-now/
[39] http://www.replicant.us/
[40] https://github.com/copperheados/

[41] https://lineageos.org/
[42] https://www.reddit.com/r/LineageOS/comments/66o5iv/questions_about_security/
[43] https://www.reddit.com/r/Android/comments/6g9imm/the_issue_of_security_in_lineageos/
[44] https://security.stackexchange.com/questions/162798/is-lineageos-more-secure-than-android-vanilla
[45] https://cve.lineageos.org/devices
[46] https://www.thedailybeast.com/this-is-how-cops-trick-dark-web-drug-dealers-into-unmasking-themselves
[47] https://theintercept.com/2015/06/22/nsa-gchq-targeted-kaspersky/
[48] https://tails.boum.org/
[49] http://www.ubuntu.com/desktop
[50] http://www.debian.org
[51] http://www.linuxmint.com/
[52] https://veracrypt.codeplex.com/releases
[53] https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial
[54] http://blog.hansenpartnership.com/owning-your-windows-8-uefi-platform/
[55] http://kroah.com/log/blog/2013/09/02/booting-a-self-signed-linux-kernel/
[56] http://fusion.net/story/325231/google-deletes-dennis-cooper-blog/
[57] https://www.systemli.org/en/friends.html
[58] https://help.riseup.net/en/security/resources/radical-servers
[59] https://prxbx.com/email/
[60] https://riseup.net/en/about-us/press/canary-statement
[61] https://riseup.net/en/better-web-browsing
[62] https://www.torproject.org/
[63] https://tails.boum.org/
[64] https://ssd.eff.org/en/module/how-use-tor-linux

[65] https://ssd.eff.org/en/module/how-use-tor-windows
[66] https://ssd.eff.org/en/module/how-use-tor-mac-os-x
[67] https://guardianproject.info/apps/orbot/
[68] https://mike.tig.as/onionbrowser/
[69] https://wiki.immerda.ch/index.php/immerda:GnuPGIntroduction
[70] https://ssd.eff.org/en/module/how-use-pgp-linux
[71] https://ssd.eff.org/en/module/how-use-pgp-windows
[72] https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
[73] https://k9mail.github.io/
[74] https://www.openkeychain.org/
[75] http://schleuder2.nadir.org/
[76] https://wiki.immerda.ch/index.php/immerda:NewSchleuderList
[77] https://en.wikipedia.org/wiki/Skype_security#Eavesdropping_by_design
[78] http://news.softpedia.com/news/ss7-attack-leaves-whatsapp-and-telegram-encryption-useless-503894.shtml
[79] https://whispersystems.org/blog/contact-discovery/
[80] https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages
[81] https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/
[82] http://technosociology.org/?page_id=1687
[83] https://www.lorankloeze.nl/2017/05/07/collecting-huge-amounts-of-data-with-whatsapp/
[84] https://robertheaton.com/2017/10/09/tracking-friends-and-strangers-using-whatsapp/
[85] https://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/
[86] https://news.ycombinator.com/item?id=6915194
[87] https://motherboard.vice.com/de/article/pgk7gv/exklusiv-wie-das-bka-telegram-accounts-von-terrorverdaechtigen-knackt
[88] https://signal.org/

[89] https://www.theregister.co.uk/2017/07/14/uk_spookhas_gchq_can_crack_endtoend_encryption_says_australian_ag/?mt=1500021512347
[90] https://en.wikipedia.org/wiki/Signal_(software)#Metadata
[91] https://moxie.org/blog/we-should-all-have-something-to-hide/
[92] https://moxie.org/stories.html
[93] https://github.com/LibreSignal/LibreSignal/issues/37#issuecomment-217211165
[94] https://yawnbox.com/index.php/2015/03/14/create-an-anonymous-textsecure-and-redphone-phone-number/
[95] https://conversations.im
[96] https://chatsecure.org/
[97] https://gultsch.de/compliance_ranked.html
[98] https://gajim.org/
[99] http://www.einfachjabber.de/
[100] https://ssd.eff.org/en/module/how-use-otr-linux
[101] https://ssd.eff.org/en/module/how-use-tor-mac-os-x
[102] https://ssd.eff.org/en/module/how-use-tor-windows
[103] https://en.wikipedia.org/wiki/Comparison_of_VoIP_software
[104] https://tox.chat
[105] https://jitsi.org/
[106] https://ring.cx/en
[107] https://mumble.info
[108] https://palava.tv/
[109] https://meet.jit.si/
[110] https://www.washingtonpost.com/local/public-safety/judge-lets-internet-firm-redact-user-identifying-data-in-information-provided-to-prosecutors-in-rioting-case/2017/10/10/dacf710a-adf2-11e7-9e58-e6288544af98_story.html
[111] https://netzpolitik.org/2017/ziemlich-schnell-entfreundet-tuerkei-kritiker-verlieren-raetselhaft-viele-follower-auf-facebook/


ABC
ABCDD.ORG