```
t);

ingerprint_generator *generator,
 signal_buffer *local_identity_buffer,
t signal_buffer *remote_identity_buffer,



ingerprint_generator *generator, signal_buffer **fing
l_buffer *identity_buffer);

ring(fingerprint_generator *generator,
erprint_buffer);

ator **generator,



> 1) {

enerator));



_generator));
```

Staatstrojaner und die Problematik von Gruppenchats

Einleitung

Dieser Text entstand im Juli ‘20 in der Schweiz im Rahmen einer Auseinandersetzung mit dem Thema Staatstrojaner und Signal-Gruppenchats. Diese Notwendigkeit ergab sich, da vermehrt politisch aktive Gruppen solche Gruppenchats, zum Teil unreflektiert, zu benutzen begannen.

Diese Zusammenstellung soll Gedankenanstösse bieten und eine Grundlage für Diskussionen in verschiedenen politischen Zusammenhängen sein. Sie ist weder vollständig noch abgeschlossen.

Am Ende befindet sich eine Liste mit Links zum Thema, den Lesenden wird zugetraut, diese selbst mit einem kritischen Blick zu betrachten, einiges davon kann nicht für alles uneingeschränkt empfohlen werden.

Der Text wurde im April ‘21 nochmals überarbeitet und aktualisiert.

Was sind Staatstrojaner

Staatstrojaner sind heimlich, durch staatliche Behörden, installierte Programme auf Computern oder Smartphones. Danach können die Behörden mit dem Programm die Kommunikation der Person mitverfolgen, auch wenn diese verschlüsselt über das Internet übertragen wird, wie dies mit Chatprogrammen wie z.B. WhatsApp oder Signal der Fall ist. Ausserdem können Daten manipuliert werden.

Staatstrojaner funktionieren im Grundsatz wie ein Schadprogramm von Hacker*innen, das im Hintergrund unbemerkt Daten von einem Rechner überträgt. Die Installation kann manuell (dafür dürfen Ermittler*innen

---

1 NZZ 9.1.2019

2 z.B. über durch Anordnung der Behörden fingierte Oberflächen von durch die Zielperson häufig benutzten Internetseiten (v.a. Mailanbieter): vpn-anbieter-vergleich-test.de/wie-wird-der-bundestrojaner-auf-dem-geraet-installiert/

3 IMSI-Catcher sind Geräte, mit denen die auf der SIM-Karte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann.
https://de.wikipedia.org/wiki/IMSI-Catcher

auch in private Räume eindringen)[1] oder digital[2] erfolgen. Staatstrojaner sowie IMSI-Catcher[3] werden oft auch GovWare für »Government Software« genannt[4] .

Wer setzt Staatstrojaner ein?

Nachrichtendienst

Beim Nachrichtendienst des Bundes (NDB) steht die präventive Überwachung in verschiedenen Formen und ohne konkreten Verdacht auf eine Straftat im Zentrum. Das neue Nachrichtendienstgesetz (NDG) als rechtliche Grundlage von 2017 baut die Überwachungsmöglichkeiten des Geheimdienstes massiv aus. Die private Kommunikation von Personen, die sich in der Schweiz aufhalten, kann weitgehendst überwacht werden, ohne dass ein Verdacht auf eine strafbare Handlung vorliegen muss. Neben Abhören von Telefongesprächen, Verwanzen von Privaträumen, Abgreifen von Daten über Kabelverbindungen meint dies ebenfalls Eindringen in Computer und das Manipulieren von diesen (Artikel 26 NDG). Bedingung ist eine Gefährdung der inneren oder äusseren Sicherheit oder die Bedrohung von wesentlichen Landesinteressen. Die Datenbeschaffungsmassnahmen müssen durch eine*n Einzelrichter*in des Bundesverwaltungsgericht und Verteidigungsminister*in /Sicherheitsausschuss des Bundesrates genehmigt werden. Aufsichtsinstanz ist die Geschäftsprüfungsdelegation (GPdel) des Parlamentes. Der NDB gibt keine Auskunft darüber, in welchen Fällen und wie häufig seit 2017 Staatstrojaner eingesetzt wurden[5]. Im »Ersten Bericht zur Bedrohungslage gemäss neuem Nachrichtendienstgesetz (Mai 2019)« werden als »Bedrohungen im Einzelnen« und »sicherheitspolitisch bedeutsame Vorgänge im Ausland« unter »Terrorismus« genannt: »ethno-nationalistischer Terrorismus und Gewaltextremismus«, u.a. «PKK» und «Rojava», sowie mögliche

---

4 Klaus & Mathys (2016), ‚The Best of BUEPF'- Was ändert sich mit der Revision? in: Jusletter IT https://www.swlegal.ch/media/filer_public/dc/47/dc47baeb-f1da-4611-9202-852a28c72eb7/160916_roland-mathys-samuel-klaus_the-best-of-buepf-was-andert-sich-mit-der-revision.pdf .

5 Humanrights.ch, 25.09.2017; NZZ 11.01.2020

gewalttätige Demonstrationen in der Schweiz. Unter »Gewalttätigem Extremismus« aufgeführt ist »Gewalttätiger Linksextremismus«, welcher über längere Zeit gewalttätige Kampagnen führe, international vernetzt sei, gewalttätig gegen Blaulichtorganisationen v.a. anlässlich Demonstrationen vorgehe, wobei »Schäden an Leib und Leben der Einsatzkräfte« in Kauf genommen oder bezweckt würden.

Strafverfolgungsbehörden

Mit dem Inkrafttreten des »Bundesgesetzes betreffend der Überwachung des Post- und Fernmeldeverkehrs« (BUEPF) von 2018 wurden neben weiteren Verschärfungen die gesetzlichen Grundlagen für den Einsatz von IMSI-Catchern[6] sowie für Staatstrojaner[7] geschaffen[8]. Es ist geheim, wo der Bund die GovWare einkauft, die Beschaffung habe 6 Millionen Franken gekostet, weit mehr als budgetiert. Mit einer Lizenz kann nur ein Gerät überwacht werden[9].

Der Einsatz muss von der Staatsanwaltschaft angeordnet und von einem Zwangsmassnahmengericht bewilligt werden. Gemäss einem Artikel der NZZ vom 11.01.2020 nutzen die Strafverfolger*innen die Lizenzen des Bundes zur Überwachung verschlüsselter Kommunikation rege. Als Beispiel wird die Staatsanwaltschaft des Kantons Waadt zitiert, die 2019 in zwei Strafuntersuchungen Staatstrojaner verwendet hat, einmal bei Verdacht auf Menschenhandel und einmal wegen Betäubungsmitteldelikten. Andere Kantone äussern sich »aus ermittlungstaktischen Gründen« nicht dazu. Das Bundesamt für Polizei (Fed Pol) sieht den Einsatzbereich von Staatstrojaner in ihrem Zuständigkeitsbereich etwa darin, um Unterstützer*innen terroristischer Organisationen zu überführen.

Am 13. Juni 2021 wird über das «Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (kurz PMT) abgestimmt[10]. Tritt dieses in Kraft, ist es den Behörden möglich, Personen präventiv zu

---

6 Art. 269bis StPO ‚Einsatz von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs"

7 Art. 269 ter StPO ‚Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs"

8 Trotz fehlender Rechtslage hatte Mario Fehr für den Kanton Zürich schon 2014 Govware eingekauft (NZZ 9.1.2019). Auch wurden Staatstrojaner im ‚Fall Stauffacher" bereits 2008 verwendet (NZZ 15.10.2011).

9 NZZ 11.01.2020, »Staatstrojaner werden intensiv eingesetzt«

überwachen und einzuschränken, ohne dass sie einer Straftat verdächtigt werden. Das Bundesgesetz PMT verbindet extrem vage Definitionen mit weitreichenden Kompetenzen für die Polizei, die einschneidende Massnahmen gegen potenziell gefährliche Personen verfügen könnte - ohne richterliche Prüfung und ohne ausreichenden Rechtsschutz. Dieses Gesetz weitet die Möglichkeiten der Behörden aus und wird auch die digitale Überwachung politisch aktiver Personen vereinfachen. Digitale Überwachung und der Einsatz von Trojanern wurde schon vor der Einführung des BUEPF 2018 heimlich durchgeführt, z.B im Verfahren gegen Andrea Stauffacher 2008[11].

Die Tendenz ist klar. Die digitale Überwachung ist eines der wichtigsten Mittel der Strafverfolgung und wird in Zukunft an Bedeutung gewinnen.

Wie die »Digitale Gesellschaft« kritisiert, ist höchst intransparent, wie häufig und in welchen Fällen Staatstrojaner eingesetzt werden[12]. So können sie auch bei Ermittlungen gegen Bagatelldelikte verwendet werden . Nachfolgend werden die Straftaten aufgelistet, bei deren Untersuchung ein Einsatz von Staatstrojaner möglich ist.

---

10 https://www.ejpd.admin.ch/ejpd/de/home/themen/abstimmungen/terrorismusbekaempfung.html und https://www.humanrights.ch/de/ipf/initiativen-parlament/bundesgesetze-zur-terrorbekaempfung/polizeiliche-massnahmen-chronologie/

11 https://www.nzz.ch/trojaner_im_fall_stauffacher_eingesetzt-1.12994241?reduced=true , https://www.computerworld.ch/business/malware/staatstrojaner-bund-vier-mal-eingesetzt-1322294.html und https://linksunten.mirrors.autistici.org/node/48779/index.html

12 NZZ 11.01.2020 und Digitale Gesellschaft, „Mit Staatstrojaner auch gegen Bagatelldelikte“ 18.03.2020

Im Folgenden die Katalog-Straftatbestände gemäss Art. 269ter StPO:

- → Vorsätzliche Tötung (Art. 111 StGB)
- → Mord (Art. 112 StGB)
- → Totschlag (Art. 113 StGB)
- → Schwere Körperverletzung (Art. 122 StGB)
- → Verstümmelung weiblicher Genitalien (Art. 124 StGB)
- → Gefährdung des Lebens (Art. 129 StGB)
- → Gewaltdarstellungen (Art. 135 StGB)
- → Veruntreuung (Art. 138 StGB)
- → Diebstahl (Art. 139 StGB)
- → Raub (Art. 140 StGB)
- → Unbefugte Datenbeschaffung (Art. 143 StGB Abs. 1)
- → Sachbeschädigung (Art. 144 Abs. 3 StGB)
- → Datenbeschädigung (Art. 144 bis Ziff. 1 Abs. 2 u. Ziff. 2 Abs. 2 StGB)
- → Betrug (Art. 146 Abs. 1 u. 2 StGB)
- → Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 Abs. 1 u. 2 StGB)
- → Check- und Kreditkartenmissbrauch (Art. 148 StGB)
- → Erpressung (Art. 156 StGB)
- → Hehlerei (Art. 160 StGB)
- → Menschenhandel (Art. 182 StGB)
- → Freiheitsberaubung und Entführung (Art. 183 u. 184 StGB)
- → Geiselnahme (Art. 185 StGB)
- → Sexuelle Handlungen mit Kindern (Art. 187 StGB)
- → Sexuelle Handlungen mit Abhängigen (Art. 188 Ziff. 1 StGB)
- → Sexuelle Nötigung (Art. 189 Ziff. 1 u. 3 StGB)
- → Vergewaltigung (Art. 190 StGB)
- → Schändung (Art. 191 StGB)
- → Sexuelle Handlungen mit Anstaltspfleglingen, Gefangenen, Beschuldigten (Art. 192 Abs. StGB)
- → Förderung der Prostitution (Art. 195 u. Art. 196 StGB)
- → Pornografie (Art. 197 Abs. 3, 4 u. 5 StGB)
- → Brandstiftung (Art. 221 Abs. 1 u. 2 StGB)
- → Verursachung einer Explosion (Art. 223 Ziff. 1 StGB)
- → Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht (Art. 224 Abs. 1 StGB)
- → Verursachen einer Überschwemmung oder eines Einsturzes (Art. 227 Ziff. 1 Abs. 1 StGB)
- → Beschädigung von elektrischen Anlagen, Wasserbauten und Schutzvorrichtungen (Art. 228 Ziff. 1 Abs. 1 StGB)
- → Gefährdung durch gentechnisch veränderte oder pathogene Organismen (Art. 230 bis StGB)
- → Verbreiten menschlicher Krankheiten (Art. 231 Ziff. 1 StGB)
- → Verbreiten von Tierseuchen (Art. 232 Ziff. 1 StGB)
- → Verbreiten von Schädlingen (Art. 233 Ziff. 1 StGB)
- → Verunreinigung von Trinkwasser (Art. 234 Abs. 1 StGB)
- → Störung des öffentlichen Verkehrs (Art. 237 Ziff. 1 StGB)
- → Störung des Eisenbahnverkehrs (Art. 238 Abs. 1 StGB)
- → Geldfälschung (Art. 240 Abs. 1 StGB)
- → In Umlaufsetzen falschen Geldes (Art. 242 StGB)
- → Einführen, Erwerben, Lagern falschen Geldes (Art. 244 Abs. 2 StGB)
- → Urkundenfälschung (Art. 251 Ziff. 1 StGB)
- → Strafbare Vorbereitungshandlungen zu Art. 111 f., 122, 124, 140, 183, 185, 221, 264 f. u. 264c ff. StGB (Art. 260 bis StGB)

- → Kriminelle Organisation (Art. 260ter StGB)
- → Gefährdung der öffentlichen Sicherheit mit Waffen (Art. 260 quarter StGB)
- → Finanzierung des Terrorismus (Art. 260 quinquies StGB)
- → Völkermord (Art. 264 StGB)
- → Hochverrat (Art. 265 StGB)
- → Angriffe auf die Unabhängigkeit der Eidgenossenschaft (Art. 266 StGB)
- → Diplomatischer Landesverrat (Art. 267 StGB)
- → Verbotene Handlungen für einen fremden Staat (Art. 271 StGB)
- → Politischer Nachrichtendienst (Art. 272 Ziff. 2 StGB)
- → Wirtschaftlicher Nachrichtendienst (Art. 273 StGB)
- → Militärischer Nachrichtendienst (Art. 274 Ziff. 1 Abs. 2 StGB)
- → Nachrichtendienst gegen fremde Staaten (Art. 301 StGB)
- → Geldwäscherei (Art. 305bis Ziff. 2 StGB)
- → Befreiung von Gefangenen (Art. 310 StGB)
- → Bestechung schweizerischer Amtsträger / Bestechen (Art. 322ter StGB)
- → Bestechung schweizerischer Amtsträger / Sich bestechen lassen (Art.322quater StGB)
- → Bestechung fremder Amtsträger (Art. 322septies StGB)

Ausländergesetz (AuG):

- → Förderung der rechtswidrigen Ein- und Ausreise sowie des rechtswidrigen Aufenthalts (Art. 116 Abs. 3 AuG)
- → Täuschung der Behörden (Art. 118 Abs. 3 AuG)

Kriegsmaterialgesetz (KMG):

- → Widerhandlungen gegen die Bewilligungs- und Meldepflichten (Art. 33 Abs. 2 KMG)
- → Widerhandlungen gegen das Verbot von Kernwaffen, biologischen und chemischen Waffen (Art. 34 KMG)
- → Widerhandlungen gegen das Verbot der Antipersonenminen (Art. 35 KMG)
- → Widerhandlungen gegen das Verbot der Streumunition (Art. 35a KMG)
- → Widerhandlungen gegen das Finanzierungsverbot (Art. 35b KMG)

Kernenergiegesetz (KEG)

- → Missachtung von Sicherheits- und Sicherungsmassnahmen (Art. 88 Abs. 1 u. 2)
- → Widerhandlungen bei nuklearen Gütern und radioaktiven Abfällen (Art. 89 Abs. 1 u. 2)
- → Missachtung der Bewilligungspflichten bei Kernanlagen (Art. 90 Abs. 1)

Weitere Straftatbestände

- → Betäubungsmittel (Art. 19 Abs. 2 u. 20 Abs. 2 BetmG) mit jeweils einem umfangreichen Katalog von
- → Güterkontrolle (Art. 14 Abs. 2 GKG)
- → Doping (Art. 22 Abs. 2 SpoFöG)

Signal-Messenger-App

Den Signal Chat Service gibt es seit ca. 2010 und gehört der Signal-Stiftung. Die Applikation verwendet Telefonnummern als Identifikation und ermöglicht Ende-zu-Ende-Verschlüsselung aller Unterhaltungen sowie eine verstärkte Verschleierung von Metadaten[13]. Der Messenger ist kostenlos und Open Source, enthält aber auch gewisse Abhängigkeiten zu Googlediensten[14]. Die Kommunikation per Signal läuft zur Zeit über verschiedene Dienste von externen Anbieter*innen, so etwa Amazon AWS, Microsoft, Google und andere[15]. Dank den komplett öffentlich einsehbaren Sourcecodes lässt sich das Programm von unabhängigen Quellen überprüfen, zuletzt etwa ein Audit durch eine Gruppe von Forsche*innen um Christoph Hagen anfangs 2021 (zu Kontaktdatenoffenlegung)[16]. Seit kurzem experimentiert Signal in einer Betaversion in Britannien mit einem Payment-Dienst[17], dieser wird von vielen Expert*innen teilweise heftig kritisiert[18,19].

Technische Ausgangslage

Signal braucht zwingend eine Telefonnummer zur Identifizierung, viele Personen verwenden dabei ihre persönliche Telefonnummer und sind so schlussendlich eindeutig identifizierbar.

Der Download findet über Google- und Apple-Stores statt, die beiden Anbieter registrieren bei Downloads auch die Gerätenummer[20] (IMEI). Eine andere Möglichkeit wäre die APK-Datei direkt von der Homepage herunterzuladen und so eine Verknüpfung von Gerätenummer und App-Download zu umgehen, dies setzt jedoch etwas mehr technisches Wissen voraus, ansonsten ist die Installation von APK-Dateien ausserhalb von Stores ein Sicherheitsrisiko.

---

13 https://signal.org/blog/sealed-sender/

14 https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9

15 https://www.kuketz-blog.de/signal-jegliche-kommunikation-erfolgt-ueber-tech-giganten-wie-amazon-microsoft-google-und-cloudflare/

16 https://community.signalusers.org/t/wiki-overview-of-third-party-security-audits/13243

17 https://signal.org/blog/help-us-test-payments-in-signal/

18 https://www.schneier.com/blog/archives/2021/04/wtf-signal-adds-cryptocurrency-support.html

19 https://www.stephendiehl.com/blog/signal.html

2016 prüfte eine Studie[21], ob Signal sogenannte Man-in-the-middle-Attacken[22] erkennen kann. 21 von 28 User*innen haben ihren Verifikationscode nicht mit ihrem Gegenüber abgeglichen, was einen solchen Angriff ermöglichte.

Finanzierung

Die Initiatoren des Signal-Vorgängers TextSecure Moxie Marlinspike (arbeitete unter anderem für Google, Facebook und WhatsApp) sowie Stuart Andersson (Robotik - Spezialist) haben 2011 ihr damaliges Start-Up Whisper Systems an Twitter verkauft. Marlinspike, von Twitter für eine kurze Zeit als Sicherheitschef beschäftigt, trennte sich Ende 2012 wieder vom Techgiganten und entwickelte TextSecure sowie RedPhone als Open-Source-Projekte unter dem Firmennamen «Open Whisper System» weiter.

Anfangs 2018 verkündeten Marlinspike und Brian Acton, Co-Gründer und Ex-Besitzer von Whatsapp die Gründung der Signal-Stiftung, für die Acton 50 Millionen Dollar zur Verfügung stellte.

Das Projekt finanzierte sich aber bereits vor der Stiftungsgründung und auch weiterhin zumindest teilweise mit Beratungsverträgen, Spenden und Finanzierungsvorschüssen. Unter anderem durch den US-staatlichen «Open Technology Fund», welcher in Vergangenheit direkt mit der NSA zusammen gearbeitet hat sowie verschiedenen Stiftungen, etwa die «Freedom of Press Foundation».

Gruppenchats

Erst seit einem Update im Oktober 2020 ist es auch in Signal-Gruppenchats möglich, an alle teilnehmenden Personen Administrationsrechte zu geben. Die zusätzlichen Rechte ermöglichen unter anderem das Entfernen von

---

20 https://www.kuketz-blog.de/take-back-control-googles-datensammelwut-unter-android-einschraenken/

21 https://www.ndss-symposium.org/wp-content/uploads/2017/09/09-when-signal-hits-the-fan-on-the-usability-and-security-of-state-of-the-art-secure-mobile-messaging.pdf

22 Man-in-the-middle-Attack:die angreifende Person hängt sich zwischen beide Kommunikationspartner*innen und gibt vor, die jeweilige andere Person zu sein

Nutzer*innen und das Löschen der Gruppenchats (sofern vorher alle Nutzer*innen den Chat verlassen haben oder entfernt wurden). Zudem lassen sich die Gruppenchats so konfigurieren, dass neue Mitglieder nicht einfach hinzugefügt werden können, sondern diese zuerst von einer Administrations-Person bestätigt werden müssen.

Trotz diesen Erweiterungen in den Berechtigungen – welche wohl die Sicherheit von Gruppenchats verbessert – bleiben mehrere Schwachstellen:

Ungelöschte Gruppenchats auf Endgeräten
Tritt eine Person aus Gruppenchats aus oder wird sie entfernt, so verbleiben trotzdem gewisse Informationen auf dem Gerät der Person bestehen. So lässt sich auch weiterhin der bisherige Chatverlauf lesen, insbesondere Ein- und Austritte sowie vergebene Administrationsrechte (diese Hinweise sind sogar von den «verschwindenden Nachrichten» ausgenommen). All diese Informationen verschwinden erst vom Gerät der Person, wenn sie aktiv aus Signal gelöscht werden. Falls die Person wieder in den Chat hinzugefügt wird und die Chat-Chronik zuvor nicht auf ihrem Gerät gelöscht hat, erhält sie alle Benachrichtigungen zu Ein-/Austritten und Administrationsrechtsvergabe nachträglich.

Attraktivität für GovWare
Durch die grosse Informationsfülle, die in Gruppenchats entstehen kann, sind die Geräte der Benutzer*innen logischerweise auch attraktivere Ziele für Strafverfolgung und Informationsbeschaffung durch Geheimdienste – ein Zugang zu den Nachrichten mittels eines Staatstrojaners bei nur wenigen Personen ermöglicht die Einsicht in grosse Mengen von Nachrichten, allenfalls von sehr vielen Personen – und erlauben das genauere Evaluieren von weiteren Zielen. Aber auch ganz ohne Staatstrojaner und erschnüffelter Inhalte vermögen bereits anfallende Metadaten[23] von

23 https://www.kuketz-blog.de/signal-welche-metadaten-hinterlaesst-der-messenger-bei-amazon-und-co/

Gruppenchats erhebliche Informationen über unsere Netzwerke und Affinitäten zu verraten. Dabei stellt sich gerade für unsere Verfolger*innen nicht die Frage, ob die «Gruppenchatbeziehungen» sich auch im realen Leben wiederfinden. Aber wollen wir der künstlichen Konstruktion von Affinitäten in Zeiten von immer schärfer werdenden Terrorgesetzen noch Futter liefern? Wir sollten uns diese Möglichkeit zumindest stärker ins Bewusstsein rufen und dementsprechend umsichtig agieren.

Entfremdung und verschwindende Gesprächskultur

Nebst den Gefahren durch Überwachung und Verfolgung anhand unserer digitalen Vernetzung gibt es ein weiteres Problem, das es anzugehen gilt: die oftmals mit viel Mühe, Reflexion und Auseinandersetzung verbundene Entwicklung einer einschliessenden Gesprächskultur – zum Beispiel ein kritischer Umgang mit Lautstärke, Redezeit und Privilegien, aber auch Rücksichtnahme auf Geäussertes, das "Sich-ins-Wort-Fallen" oder eine fokussierte Diskussion zu einem Thema, all das wird in Gruppenchats schnell ein Ding der Vergangenheit. In der Geschwindigkeit getippter Nachrichten gehen nicht selten Themen unter oder Stimmen vergessen, mit den automatisch verschwindenden Nachrichten ist gestern Diskutiertes heute schon wieder vom Tisch. Der*die schnellste Schreiber*in gibt regelmässig Takt und Thema vor. Und im Rythmus eintreffender Nachrichten reduzieren sich unsere Beziehungen auf eindimensionale Botschaften ohne Zwischentöne und Gefühlsausdruck, denen auch der grosszügige Einsatz von Emojis kein würdiger Ersatz sein kann.

So erschüttern und greifen nicht nur die Repressionsbehörden mit ihrer Verfolgung unsere Beziehungen an, sondern auch wir selbst werden zu einem aktiven Teil in der Zerstörung unserer selbstaufgebauten Gegenentwürfe von Gemeinschaften.

Was bedeutet das z.B. im Falle einer Beschlagnahmung des Mobiltelefons?

Mit Hilfe eines Trojaners kann jeder noch so gut verschlüsselte Chat gelesen und ausgewertet werden, da der Trojaner alles mitliest, was die benutzende Person auch sieht. Ist das Telefon nur unzureichend geschützt (fehlende Verschlüsselung, Fingerabdrucksperre, kurzer Sperrcode, Signal nicht zusätzlich mit PIN geschützt), ist bei einem physischen Zugriff auf das Gerät durch die Strafverfolgung das Installieren von Malware und somit das Mitlesen der Chats trivial, nicht-gelöschte Chatverläufe können so u.U. etliche Personen kompromitieren.

Weitere Aspekte

Die Benutzung eines Gruppenchats ist nur vordergründig eine persönliche und individuelle Entscheidung. Nicht nur alle beteiligten Personen eines Gruppenchats, sondern auch deren Umfeld tragen die Konsequenzen, wenn es zu Überwachung oder Strafverfolgung kommen sollte. Bei einer Hausdurchsuchung oder den Recherchen zum weiteren Umfeld einer Person betrifft es schnell auch Personen, die nicht an einem Gruppenchat beteiligt sind.

Es ist praktisch unmöglich, dass wir selber entscheiden, welche Inhalte harmlos und welche eventuell belastend sind. Wir wissen nicht, wie sich die Dinge entwickeln, welche Personen eventuell ins Visier der Behörden kommen, welche banalen Nachrichten ihnen eine wichtige Information liefern oder was in Zukunft passieren wird.

Fall-Beispiel: In Basel wurden Leute vor Gericht gezerrt für die angebliche Teilnahme an einer Demo, bei der es zu Glasbruch und Graffiti kam, weil sie am Tag der Demo mit anderen Beschuldigten SMS ausgetauscht haben (Basel 18)[24] .

---

24 https://www.labournet.de/internationales/schweiz/politik-schweiz/der-schauprozess-von-basel-gegen-die-basel-18/ und https://wwwwoz.ch/-9544

Konsequenzen

Der vermeintliche Vorteil eines Gruppenchats ist die schnelle Kommunikation. Es stellt sich die Frage, ob dieses Tool uns mehr nützt als schadet und wir die negativen Aspekte dafür in Kauf nehmen können.

Oftmals ist es so, dass sich vieles bei einer kurzen Sitzung oder einem Treffen, welches ja meistens auch bei Verwendung eines Gruppenchats stattfindet, vieles besser klären lässt und damit auch keine Personen ausgeschlossen werden, die kein Smartphone haben oder Chats nicht benutzen möchten. Viele Dinge müssen nicht sofort geklärt werden, sondern können an einem nächsten Treffen diskutiert werden.

Ausschlüsse passieren auch innerhalb eines Gruppenchats, weil z.B. jemensch die Sprache nicht versteht, sich in dieser nicht ausdrücken/schreiben kann oder weil eine Person während der Diskussion nicht auf ihr Smartphone schauen kann oder möchte.

Der Staat hat immer ein Interesse, Widerstand zu überwachen, egal wie gross dessen tatsächliche Relevanz ist. Wir können hächstens vermuten, welche Aktivitäten für sie interessant sind und welche nicht. Eine harmlos scheinende Aktion kann schnell auch Grund für eine Strafverfolgung sein.

Deshalb kann es für uns auch ein Vorteil sein, wenn wir uns von Anfang an nicht blind auf Technologien verlassen. Am Gedanke, verschlüsselt zu kommunizieren, ist grundsätzlich nichts falsch, jedoch sollte mensch sich mit den verwendeten Technologien auseinandersetzen und kritisch hinterfragen.

Ebenfalls sollten wir uns überlegen, was kommunizieren wir, wem, wann, wie und wo. Welche Information wollen wir vor wem verheimlichen?

AntiRep Winterthur, antirepwinterthur@riseup.net
PGP-Fingerprint: 586F C997 399E AD38 7772
5858 E0F7 72BD BB30 3FE5

Zum weiterlesen:

«Metadaten verraten Ihnen absolut alles über das Leben einer Person. Wenn Sie genug Metadaten haben, brauchen Sie den Inhalt nicht wirklich.»

Stewart Baker, früherer NSA General Counsel

«(Die USA) töten Unschuldige basierend auf Metadaten.»

Ehemaliger Direktor von NSA und CIA, Michael Hayden

➔ **https://youtu.be/kV2HDM86XgI?t=1079**

Wanze im Hosensack - Die Schweiz hat die Überwachung der Bevölkerung systematisch ausgebaut. Das Kernstück ist dabei unser treuer Begleiter: das Mobiltelefon. Dank ihm können Behörden immer wissen, wo wir sind.

➔ **https://barrikade.info/article/1762**

Schalte dein Telefon nie aus - In den 1980er Jahren entwarf eine Anarchistin, die zum Beispiel ein Verwaltungsgebäude in Brand setzen wollte, ihren Plan und prüfte gleichzeitig, ob es in ihrem Haus keine Abhörgeräte gab. Ende der 90er Jahre schaltete dieselbe Anarchistin das Telefon aus und benutzte verschlüsselte Nachrichten im Internet. Da wir uns den 2020er Jahren nähern, müssen wir unsere Strategie überdenken: Die Informationsbeschaffung hat sich verbessert, und wir müssen dies auch berücksichtigen.

➔ **https://barrikade.info/article/1738**

Android ohne Google

➔ **https://www.kuketz-blog.de/android-ohne-google-take-back-control-teil1/**

LineageOS
➔ **https://www.kuketz-blog.de/lineageos-take-back-control-teil2/**

Daten sammeln - Wann haben Sie heute zum ersten Mal ihr Smartphone benutzt? Wie und wo haben Sie es mit dem Internet verbunden? Welche Apps verwendet? Wohin gesurft? Etwas online bestellt? Mit wem kommuniziert? Wie lange, bzw. Textlänge? Wohin sind Sie mit Ihrem Handy gegangen (wie schnell fortbewegt)?
➔ **https://www.aufschrittundklick.de/daten-sammeln/**

Privacy Handbuch
➔ **https://www.privacy-handbuch.de/handbuch_70.htm**

Da geht was! - Smartphones mit PinMe auch ohne Standortfreigabe tracken
GPS aus, WLAN aus – schon lässt sich ein Smartphone nicht mehr verfolgen. Falsch! Forscher zeigten, dass man auch anders herausfinden kann, wo Smartphone-Nutzer waren.
➔ **https://www.heise.de/select/ct/2018/7/1522378170373856**

Was die angeblich harmlosen Metadaten alles über uns verraten - Auf Vorrat gespeichert
Die Geheimdienste (und nicht nur die) möchten so viel wie möglich über alles und jeden wissen. An alle Daten kommen sie nicht so einfach ran, darum beschränken sie sich oft auf die die eigentlichen Daten beschreibenden Metadaten. Das lässt sich der Öffentlichkeit auch viel besser verkaufen, denn die Metadaten sind ja »völlig harmlos«.
➔ **https://entwickler.de/online/security/vorratsdatenspeicherung-metadaten- 174414.html**

Android Smartphone (google-frei) einrichten
Was ist grundsätzlich von Smartphones zu halten? Sollte man sie überhaupt benutzen? Wir finden: Smartphones sind praktische Helferlein, die Alltag und politische Organisierung erleichtern können. Richtig ist aber auch, dass Smartphones die universelle Wanze in der Hosentasche und ein großes Helferlein für staatliche Überwachung und globale Werbekonzerne sein können. Der Fokus des Artikels liegt darauf, das Smartphone von den Massenüberwachungs – Tools der grossen Internet- Konzerne, vor allem Google, zu bereinigen und damit ein Mindestmass an Privatsphäre wiederherzustellen. Schutz gegen gezielte Angriffe auf einzelne Smartphones, etwas durch Ermittlungsbehörden, ist nur am Rande Thema.
➔ **https://wiki.systemli.org/howto/android/setup#warum_das_alles**

Use you Smartphone as securely as possible
All mobile phones support voice and text communication. These days, most of them do a great deal more. Mobile phones are an integral part of our daily lives, in part because of their small size, versatility and relatively low cost. These same qualities make them invaluable to human rights defenders, who often rely on them to exchange and store sensitive data in ways that previously required access to a trusted computer. This guide is primarily about smartphones: Much of the advice in this guide is relevant to other mobile devices, as well. Some of it applies to feature phones (basic, old-fashioned mobile phones).
➔ **https://securityinabox.org/en/guide/smartphones/**

PRISM BREAK – Alternativen zu proprietärer Software
➔ **https://prism-break.org/de/**

Broschüre: Surveillance Self Defence - A Collective Matter
Gedanken zu Kommunikationssicherheit, FOSS, Verschlüsselung, Smartphones und praktischen Tipps im Alltag
➔ **https://barrikade.info/article/4071**

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world

➔ **https://www.eff.org/issues/privacy**

CAPULCU – Technologiekritische Gruppe aus DE die regelmässig Artikel/Bücher veröffentlicht

➔ **https://capulcu.blackblogs.org/**

Chaos Computer Club

➔ **ccc.de/de/tags/staatstrojaner**

TAILS Broschüre: Tails – The amnesic incognito live system
Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente. Diese Anleitung erhebt den Anspruch, auch für Computer-Nicht-Expert*innen verständlich und nützlich zu sein.

➔ **https://capulcu.blackblogs.org/neue-texte/bandi/**

Kanadische Uni-Forschungsstelle zu Spy-Ware

➔ **https://citizenlab.ca/**

```
47  static int fingerprint_gene
48          const ec_public_key_list *unsorted_key_lis
49
50  static int fingerprint_generator_create_for_impl(f
51          const char *local_stable_identifier, const
52          const char *remote_stable_identifier, cons
53          fingerprint **fingerprint_val);
54
55  static int fingerprint_generator_get_fingerprint(f
56          const char *stable_identifier, const signa
57
58  static int fingerprint_generator_create_display_st
59          char **display_string, signal_buffer *fing
60
61  int fingerprint_generator_create(fingerprint_gener
62          int iterations, int scannable_version,
63          signal_context *global_context)
64  {
65      fingerprint_generator *result_generator;
66
67      assert(global_context);
68
69      if(scannable_version < 0 || scannable_version
70          return SG_ERR_INVAL;
71      }
72
73      result_generator = malloc(sizeof(fingerprint_g
74      if(!result_generator) {
75          return SG_ERR_NOMEM;
76      }
77      memset(result_generator, 0, sizeof(fingerprint
78
```