

1. Überwachen und Strafen

- Der autoritäre Staat
- Im Netz
- Online-Durchsuchung
- Vorratsdatenspeicherung
- Data Mining
- „Anti-Terror“-Datei
- Wer, warum und wogegen?

2. Der autoritäre Staat

Das Tempo der autoritären Umgestaltung des Staates beschleunigt sich seit den neunziger Jahren immer weiter. Ein paar Stichwörter:

Lauschangriff, neue Polizeigesetze, faktische Abschaffung von Art. 16 GG, Otto-Katalog, ausufernde Telefonüberwachung, DNA-Datenbank samt Massenerfassungen, wahllose Hausdurchsuchungen, Schleierfahndung, Zusammenarbeit der Polizeien, Sicherungsverwahrung, Polizeiverordnungen...

- Egal, ob es eine Gesamtstrategie gibt oder nicht: Der Staat wird immer autoritärer und muss das wohl auch werden – dazu gegen Ende noch mehr.

Bei all dem werden Kontrolltechnologien immer wichtiger.

- Zunächst man sich darüber klar sein, dass die Protagonisten dieser Maßnahmen häufig drastisch verschiedene Interessen haben. Wenn hier von „Ihnen“ die Rede ist, so ist das manchmal das BKA, mal der Bundesinnenminister, mal die Länderminister, mal die einen, mal die anderen Teile der IT-Industrie, mal irgendwer anders – und in jedem Einzelfall ist zu klären, wer da was warum betreibt (im Rahmen dieses Rundumschlags kann ich das natürlich nur ansatzweise, und sobald Technologie ins Spiel kommt, wird das noch komplizierter, weil die „Entscheider“ meist reichlich unzutreffende Vorstellungen vom Gegenstand ihrer Entscheidung haben).

Beispiele für Interessenkonflikte: Kryptografie, Verbindungsdatenspeicherung, „Anti-Terror“-Datei.

Insbesondere *gibt* es noch einen Rechtsstaat, und weite Teile von „Ihnen“ möchten den auch auf jeden Fall behalten (vgl. unten). Das weiß insbesondere das Verfassungsgericht (niedrigere Instanzen zwar tendenziell weniger, aber doch auch), das etliche der erwähnten Projekte und Maßnahmen kassierte oder jedenfalls deutlich einschränkte.

Die Widersprüche innerhalb der der PlanerInnen des autoritären Staates sind unsere Chance, politisch einzugreifen. Demgegenüber sind technische Maßnahmen zwar unter Umständen wirksam, aber keine Dauerlösung, da sie (a) unsere Arbeit schwerer machen, (b) meist erhebliche Sachkenntnis verlangen, wenn sie effektiv sein sollen und (c) häufig auch durch gesetzliche Regularien ausgehebelt werden können (z.B. Krypto-Verbot in Frankreich, Angriffe auf TOR-Server).

Die autoritäre Formierung ist ein politisches Problem und muss in erster Linie politisch bekämpft werden.

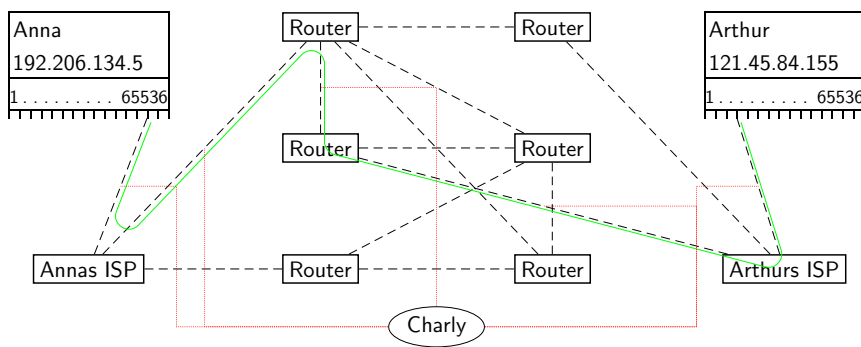


Fig. 1

3. Exkurs: Das Netz

(vgl. Fig. 1)

- Jede Maschine im Netz hat eine Nummer, ihre IP-Adresse. Aus Bequemlichkeitsgründen wird diese Nummer durch vier halbwegs kleine Zahlen dargestellt, aber in Wirklichkeit ist es nur eine Zahl zwischen Null und 4294967296. U.a. weil diese Zahlen allmählich knapp werden, wird das Netz nach und nach so umgebaut, dass diese Nummern zwischen Null und 2^{128} liegen, das Prinzip ändert sich aber nicht: Zu einem bestimmten Zeitpunkt ist eine Nummer an genau einen Rechner vergeben.

Rechner an Unis u.ä. haben in der Regel eine Nummer, die sie auch behalten, und sie sind durch diese Nummer eindeutig global zu identifizieren („statische IP“). Rechner, die über DSL o.ä. angebunden sind, bekommen regelmäßig neue Adressen („dynamische IP“), und nur der ISP kann im Nachhinein sagen, wer wann welche IP hatte – so er es speichert, was für Flatrates an sich gerichtlich untersagt wurde, aber im Zuge der Vorratsdatenspeicherung zur Pflicht werden soll.

- Für die Übertragung von Daten hat jeder Rechner noch jede Menge „Ports“, an die sich Rechner von außen verbinden können und über die sie Daten versenden. Dabei lassen sich Portnummern häufig spezifischen Diensten zuordnen. Auf Port 25 empfangen Rechner normalerweise Mail, auf Port 80 hören sie auf Wünsche nach Webseiten, auf Port 110 warten sie darauf, dass jemand Mail abholt. Diese Zuordnung ist aber nur Konvention und kann jederzeit geändert werden.

4. Der Bundestrojaner

- Der Plan, der in Öffentlichkeit diskutiert wird, ist in etwa: Die Polizei schiebt Verdächtigen Programme unter, die diese installieren und die dann die auf dem Rechner befindlichen Daten durchsucht und „Relevantes“ an die Polizei schickt – und zwar ohne Wissen der Verdächtigen. Außerdem kann es natürlich gleich noch nachsehen, was der/die Betreffende so tut.

Dass die Polizei so etwas schon mal erfolgreich gemacht hätte, ist nicht bekannt. Bei den paar Verfahren, die dabei in Diskussion stehen, hat es jedenfalls offenbar nicht geklappt bzw. war so gar nicht geplant. Tatsächlich ist das auch alles andere als trivial, auch wenn die Unzahl der im Netz befindlichen Zombie-Rechner etwas anderes suggerieren mag. Der vom BGH zurückgewiesene Antrag lässt ahnen, dass die Beamten, die das beantragt haben, sich das einfacher vorgestellt haben als es in wirklich interessanten Fällen sein dürfte.

Um Daten aus einem Rechner abziehen, muss man zunächst eigenen Code auf den Zielrechner bekommen:

- - Einschleusen von Code durch Mails oder geeignet manipulierte Webseiten. Das ist der klassische Trojaner: Man bringt die Zielperson dazu, das Schadprogramm selbst zu starten. Dazu kann man es entweder als tolles, hilfreiches Programm tarnen (so macht das übliche Spyware), dramatischen Hirnschaden von Windows ausnutzen und tarnen, dass überhaupt ein Programm gestartet wird (porn.jpg.exe) oder fehlerhafte Programm auf der lokalen

U Maschine nutzen (z.B. einen Acrobat Reader, der die Ausführung von Programmcode in einem aus dem Netz gezogenen PDF erlaubt oder Defekte in Browsern, die in HTML-Mails enthaltenen Code ausführen). Hier lässt sich mit etwas Vernunft weitgehende Sicherheit erreichen, weshalb dieser Angriff nur taugt, wenn die Polizei entweder nur Idioten im Visier hat oder selbst aus Idioten besteht. Schäubles Vorstellung scheint das zu sein.

U • Ausnutzen von „Hintertüren“. Spekulationen über von Geheimdiensten oder gar von der Polizei in üblichen Betriebssystemen eingebaute Hintertüren sind nicht sehr glaubhaft – für Betriebssysteme, die im Quellcode vorliegen, müsste das unglaublich raffiniert gemacht sein, aber auch für die üblichen proprietären Systeme scheint es nicht wahrscheinlich; würden solche Hintertüren in nennenswertem Umfang genutzt, wäre es jedenfalls schwer zu erklären, dass noch niemand Anzeichen dafür gefunden hat. Dazu kommt, dass Microsoft und Co wahrscheinlich den wirtschaftlichen Schaden, den eine solche Enttarnung mit sich brächte, wie die Pest fürchten. Bleiben unabsichtliche Hintertüren, die durch Programmfehler erzeugt werden. Die für diese Zwecke realistischerweise nötigen „zero-day remotely exploitable bugs“ sind aber zu selten, um „verlässliche“ Ermittlungserfolge zu ermöglichen, auch hängen sie meist von spezifischen Konfigurationen ab, die Privatrechner häufig nicht haben.

U • „Infizieren“ von Programmen, die die Zielperson ohnehin installiert. Das wäre der einzig aussichtsreiche Weg – man wartet, bis die Zielperson gerade ein Sicherheitsupdate macht, den neuen Druckertreiber installiert oder ein Filesharingprogramm zieht. Während der Code durchs Netz wandert, hängt die Staatsgewalt nach dem Vorbild von Viren den gewünschten Code an. Klingt einfach, ist aber im Zweifel auch eher kompliziert, weil man zwecks Erfolgsaussichten alle möglichen Arten von Programmen infizieren können muss (nicht nur „nackte“ Binärdateien, die Viren zur Verfügung stehen, sondern auch z.B. Programme in Archiven, XUL-Kram für Mozilla/Firefox, Java-Bytecode usw.) und dann immer noch mit eventuellen Beschränkungen der Zielumgebung umgehen muss. Dazu kommt, dass mittlerweile Betriebssystemupdates u.ä. mittlerweile digitale Signaturen tragen, die eine Veränderung des Inhalts unmöglich machen, ohne dass es auffällt. Immerhin: Solche Nummern wäre trotz allem möglich, würden aber eine umfangreiche Infrastruktur voraussetzen, die es noch nicht gibt und die für die paar Kröten (die 160 Millionen, die die FAZ zitiert, scheinen extrem unglaubwürdig; in einer Antwort der Regierung auf eine Anfrage der Linksfraktion ist von 200000 Euro Erstinvestition für Online-Durchsuchungen die Rede), die das Ministerium hochhusten möchte, nicht zu bekommen ist.

U Programme zur Überwachung der Rechner existieren hingegen reichlich. Andererseits ist es schwierig, den ausgehenden Verkehr so zu tarnen, dass etwas geschickte HackerInnen nicht sehr einfach merken, dass da etwas vorgeht.

U Fazit: 80% Bocksgesang inkompetenter „Sicherheits“fanatiker. Der wesentliche Effekt ist, dass die Öffentlichkeit weiter desensibilisiert wird und Bedrohungsszenarien samt ihrer brachialen Beherrschungspläne kauft. Die restlichen 20% sind in der Tat aus vielen Gründen bedrohlich – vermutlich würde die „Online-Durchsuchung“ aber ungefähr in dem Umfang angewendet wie der große Lauschangriff und ist von daher eher zu vernachlässigen.

U Viel ernster: Hausdurchsuchung mit Beschlagnahme. Das klappt fast immer, ist für die Betroffenen zusätzlich gleich mal Bestrafung durch die Polizei und ist prima funktionierende Praxis. In dem Sinne sind die ausufernden Hausdurchsuchungen ein weitaus besseres Ziel für Antirepressionskampagnen.

5. Die Vorratsdatenspeicherung

Gemeinsam mit biometrischen Ausweisdokumenten ist das der augenblicklich übelste Angriff auf elementare Freiheitsrechte.

- „Umsetzung einer EU-Richtlinie“ (Frist 15.9.07) – das ist ein Klassiker, wie man über den Umweg über Brüssel unpopuläre Maßnahmen durchsetzt, denn die Schröder-Regierung hat auf EU-Ebene eifrig dafür geworben, während das Berliner Parlament brav dagegen stimmen durfte. Jetzt
- „muss“ man das halt machen, wie traurig. . .

Für sechs Monate bis (mindestens) zwei Jahre müssen die Telekoms speichern, wer wann mit wem von wo wie lange telefoniert oder gemailt hat. Im ursprünglichen Entwurf hätten „alle“ Verbindungen, auch die erfolglosen, gespeichert werden müssen, was speziell im Internetbereich völlig wahnsinnig wäre (DNS-Abfragen, ICMP-Nachrichten. . .). Allein der Plan illustriert, dass die Überwachungsfanatiker nur sehr nebulöse Vorstellungen haben, wovon sie reden. Auf Druck der Telekoms wurde die Richtlinie auf das zusammengestutzt, was sie jetzt ist.

- Wurde am 9.11.2007 im Bundestag abgenickt, wird zum 1.1.2008 in Kraft treten. Die deutsche Umsetzung ist im Bereich dessen, was im IP-Bereich eigentlich gespeichert werden soll, ähnlich nebulös wie die EU-Richtlinie: Mails und Telefonie. Was sowas angesichts von IM, IRC, Voicechats, MMORPGs usf. bedeutet, ist absolut unklar. Es fehlt „Normenklarheit“.

Ansonsten liegen die Daten bei den Telekoms, der Zugriff soll unter Richtervorbehalt stehen. Dabei sollen die Daten nur zur Aufklärung „erheblicher“ oder mittels Telekommunikation begangener Straftaten zur Verfügung stehen. Auch das ist schon fatal z.B. im Hinblick auf die nachträgliche Ausforschung von Strukturen, aber sicher wird es dabei nicht bleiben.

- Richtig toll werden diese Daten nur gemeinsam mit Data Mining. Dafür braucht es aber Zugriff auf die Gesamtdaten, und angesichts des Feature Creep im Bereich „Sicherheit“ wird es den absehbar geben.

6. Data Mining

„Rasterfahndung auf Steroiden“ – der Versuch, Strukturen in großen Datenmengen zu erkennen. Man sammelt alles, was man an Daten bekommen kann: Polizeidaten, Kommunikations- und Bewegungsprofile, Kontodaten, Konsumdaten usf.

- Supervised Data Mining: Man nimmt bekannte Zecken, lässt den Rechner Merkmale identifizieren, mit denen man nach neuen Zecken sucht.
 - Unsupervised Data Mining: Der Rechner guckt aufs Geratewohl, was es an Struktur in den Daten gibt – danach können Menschen überlegen, ob Teile dieser Struktur zeckig aussehen.
- Methoden aus diesem Bereich können auch anderen Zwecken dienen – beispielsweise der Aufdeckung der Verwendung mehrerer Identitäten, das Säubern von Datenbeständen von bewusst oder versehentlich falsch erhobenen Daten usf. Das Ausleuchten von Strukturen ist aber wohl das, was die Staatsgewalt gegenwärtig am aufregendsten findet.

Gegenwärtig auf staatlicher Seite erst in Ansätzen entwickelt (Hartz IV!), vor allem vom Datenschutzrecht behindert – aber alle investieren eifrig.

7. Die Anti-Terror-Datei

Gemeinsame Datei von Geheimdienst und Polizei.

„Erhobene“ Daten der beteiligten Behörden zur (ausländischen) TerroristInnen, UnterstützerInnen, ihren Bekannten („Kontaktpersonen“) und „Sachen“, die damit zu tun haben.

Grunddaten: Daten zur Identifikation, „Fallgruppe“

„Erweiterte Grunddaten“: Kontonummern bis Ausbildungsgang, insbesondere auch Religion, „Volkszugehörigkeit“, Freitextfeld.

- ⊞ Schon das Wort „Erweiterte Grunddaten“ deutet darauf hin, dass hier ein Kompromiss vorliegt: Die Geheimdienste wollten allenfalls eine „Indexdatei“, in der höchstens drinsteht, *dass* sie etwas über wen wissen, aber nicht, *was*. Die Polizei wollte möglichst umfangreichen Zugriff auf das (vermutlich herbeifantasierte) „Wissen“ der Dienste. Das Ergebnis ist die vorliegende Kompromissformel, bei der auf die „Erweiterten Grunddaten“ außer im Eilfall nur mit Einwilligung der einstellenden Behörde zugegriffen werden darf.
- ⊞ Zusätzlich: Verdeckte, beschränkte Speicherung.
Das GDG erlaubt weitere gemeinsame Dateien von Diensten und Polizeien ohne parlamentarische Beratung, d.h. unter Ausschluss der Öffentlichkeit.

8. Politische Philosophie 101

Keine technische Lösung für ein soziales Problem!

- ⊞ Die Auswirkungen des autoritären Staats kann man teilweise technisch mildern – die Vorratsdatenspeicherung lässt sich z.B. mit einigem Sachverstand und der Bereitschaft zum Verzicht auf Bandbreite durch TOR begegnen, Data Mining kann durch Vermeidung von Datenspuren und gezieltes Legen irritierender Spuren ausgehebelt werden –, letztlich kann der Staat durch Gesetze und sanften Terror die „Kosten“ dafür so in die Höhe treiben, dass uns die Konspiration mehr kostet als sie wert ist. Letztlich hilft nur eine politische Auseinandersetzung.
Wie ist das Ganze zu beurteilen? Was passiert hier? Dafür lohnt es sich, ein paar einfache Gesellschaftsmodelle zu untersuchen.
- ⊞ Modell 1: Herrschende und Beherrschte. Die Interessen der Spieler sind leicht zu durchschauen: Herrschende wollen herrschen. Dazu brauchen sie Kontrolle, und dafür brauchen sie so viel Information über die Beherrschten wie möglich – sie wollen transparente Beherrschte. Dass dies dabei hilft, Bedrohungen ihres Status als Herrschende frühzeitig zu identifizieren und dann mit relativ wenig Aufwand zu eliminieren, ist ein angenehmer Nebeneffekt. Auf der anderen Seite ahnen die Herrschenden, dass die Beherrschten ihre Handlungen in der Regel nicht so toll finden – deswegen wollen sie lieber opak sein.
Umgekehrt wollen die Beherrschten nicht, dass ihr Leben in allen Einzelheiten durchleuchtet wird, schon, weil das z.B. erlaubt, UnruhestifterInnen zu identifizieren und mithin ihre Partizipationsmöglichkeiten reduziert – mithin wollen auch sie lieber opak sein, was sich mit dem Wunsch nach ihrer Transparenz von Seiten der Herrschenden schlecht verträgt.. Sie würden aber gerne wissen, was die Herrschenden für sie ausbrüten, wollen also transparente Herrschende.
Dieser fundamentale Interessengegensatz besteht so auch in der realen Gesellschaft. Da im Augenblick die Beherrschten schwach sind, sind die Herrschenden am Drücker und lassen sich eifrig Kontrollmechanismen einfallen. Warum aber beschränken sie sich dann doch wieder selbst?
- ⊞ Modell 2: Add Marktwirtschaft. Marktwirtschaft funktioniert mit einem Rechtsstaat viel besser – die Marktakteure haben Investitionssicherheit, die Geschäfte werden nach Marktregeln (und nicht z.B. nach Gewalt oder staatlicher Willkür) abgewickelt usf. – nicht zuletzt ist in typischen Geschäften ein Mindestmaß an Vertraulichkeit wichtig, nicht nur, da sie praktisch immer in einer Grauzone zur Korruption stattfinden.

Ein Marktteilnehmer will sich also auf das Recht verlassen können – das ist ein Grund, warum wir de facto kein Feindstrafrecht haben. Es gibt dabei noch allerlei weitere Komplikationen, weil es ja z.B. noch weitere Staaten gibt, deren man sich auch bedienen möchte, aber so detailliert muss es jetzt nicht sein. Es bleibt: Marktwirtschaft will einen Rechtsstaat, will opake MarktteilnehmerInnen, will keine Staatswillkür. Daher die Beschränkungen, die sich die Herrschenden auferlegen.

U Dann wäre ja eigentlich alles in Butter, allenfalls müsste man die Marktfraktion unter den Herrschenden stärken. Das ist in etwa das, was Teile der FDP glauben. Leider ist es falsch.

U Modell 3: Gewerkschaften, KommunistInnen, AnarchistInnen. Es gibt Dinge, die die Marktfraktion noch weit mehr fürchtet als eine Willkürherrschaft. Dazu mögen Staaten gehören, die sich der Benutzung verweigern oder gar die Benutzung des eigenen Landes bedrohen, in erster Linie sind das aber Linke. Werden diese stärker, wird auch die Marktfraktion einer Ausweitung der Willkürherrschaft zu stimmen (Beispiele gibt es genug, der Faschismus ist beileibe nicht der einzige – ein Blick in die Geschichte der Gewerkschaften in den USA ist da z.B. sehr aufschlussreich). Daten, die dann bereits vorliegen, werden letztlich beliebig genutzt werden. Und das ist die Hauptgefahr: Uns werden die Daumenschrauben proportional zu unserer eigenen Stärke angezogen werden..

Ganz zu vermeiden ist das natürlich nie. Wenn allerdings der Paranoia der Herrschenden schon ohne wirklich konkrete (fortschrittliche) Umgestaltungsprozesse freier Lauf gelassen wird, wird es später entsprechend schlimmer.

Auch im Normalzustand müssen die Herrschenden sehen, wie sie den sozialen Frieden erhalten – und das bedeutet, dass mit einer ausreichend starken Bewegung all der Kram abgewendet werden kann. Vorbild mag hier die Kampagne zum Volkszählungsboykott sein, die 1982ff viele der Datenschutzrechte, die wir heute noch haben, erkämpft hat.

Was ist zu tun?

- Kampf der Politik der Angst
- U • Sicherheit negativ besetzen – stattdessen lieber konkret benennen, was gemeint ist: Menschenwürde, Unverletzlichkeit (der Person, der Wohnung. . .), Schutz vor Armut usf Insbesondere: Es gibt kein „Grundrecht auf Sicherheit“, und das ist auch gut so.
- Das Übliche

<http://www.datenschmutz.de>