Bitte twittern sie jetzt nichts!

„Soziale Netzwerke“, Überwachung und Repression

Redaktionskollektiv der RHZ

Flugblätter nerven. Da plant die Gruppe eine Veranstaltung oder eine Demo und hat wirklich genug zu tun. Und dann muss auch noch mobilisiert werden. Der Text für das Flugblatt darf nicht zu kurz sein und nicht zu lang, ein einigermaßen ansprechendes Layout muss auch her. Das dauert und kostet vielleicht sogar Geld. Dann muss das Zeug gedruckt werden, das kostet auch Zeit und Geld. Und dann müssen die Zettel verteilt werden, in Kneipen und Projekten, Läden und Zentren, von denen die Gruppe annimmt, dass dort die Leute verkehren, die wahrscheinlich an der Veranstaltung interessiert sind. Ein echter Kraftakt. Die Hälfte der Blätter wird sowieso nicht verteilt und landet im Müll. Und wie viele der Leute, die dann wirklich kommen, durch diese arbeitsintensiven Flugis aufmerksam geworden sind, ist am Ende eine Glaubensfrage.

Das geht auch einfacher. Und schneller. Und billiger. Zum Beispiel mit Facebook. Oder mit Twitter. Abgesehen von letzterem gibt es kaum Vorgaben zu Länge und Aussehen. Text geschrieben, von der Gruppe inhaltlich angenommen, getwittert, gepostet oder eingestellt, fertig. Im Idealfall geht die Nachricht zielgerichtet an ausgewählte Personen oder Gruppen. Und die können es ruckzuck an Andere weiterleiten. Ein schönes Beispiel für die schnelle, gezielte und erfolgreiche Mobilisierung großteils über solche Kanäle sind die Proteste gegen die Gefahrengebiete in Hamburg im Januar 2014. Immer wieder konnten innerhalb kürzester Zeit Aktivist_innen aus der näheren und weiteren Umgebung (und auch die bald auf Twitter eingeklinkte Polizei) zu wirkungsvollen Aktionen zusammengerufen werden.

Für die Mobilisierung zu Aktionen, zur Verbreitung von Nachrichten, zum Austausch von Material und auch einfach, um in Kontakt zu bleiben, sind sie enorm praktisch, diese so genannten sozialen Medien und einiges mehr, was im weiteren Rahmen damit zu tun hat. Die bekanntesten und sicher am meisten genutzten sind Facebook, Twitter und Youtube. Auch in den Beiträgen dieses Schwerpunkts der *RHZ* werden diese drei Kanäle am häufigsten genannt. Doch bei all unseren Betrachtungen geht

es genauso auch um Flickr, Tumblr, Skype, Instagram, Google+, LinkedIn, Xing, Finya und viele andere, mehr oder weniger bekannte Plattformen, auf denen sich (auch linke) Menschen tummeln. Bei vielen dieser Werkzeuge, die uns das tägliche Leben, auch das politische, zweifellos einfacher machen, kämen viele unserer Genossinnen und Genossen gar nicht auf die Idee, dass es da ein Problem geben könnte.

Klar, Facebook und Google sind Datenkraken, haben wir alles hundertmal gehört. Wenn sie trotzdem verwendet werden, ist vielleicht ein kleines bisschen schlechtes Gewissen dabei. Aber wenn lustig Kontobewegungen, Reiseplanungen und sportliche Leistungen vom Smartphone aus verwaltet werden, ist das Problembewusstsein schon ein ganz schönes Stück kleiner. Warum eigentlich? Nur weil all diese Angebote, die uns Konzerne und teils auch Behörden völlig selbstlos machen, so praktisch sind?

Alles schon immer geahnt, aber ignoriert?

Als Edward Snowden ab Mitte 2013 nach und nach das ganze monströse Ausmaß der Bespitzelung und Ausforschung nicht nur, aber auch im Internet öffentlich machte, hatten sich viele Linke eine größere öffentliche Reaktion erwartet. Massen erschütterter Bürger_innen hätten schreiend durch die Städte ziehen und staatliche Gebäude angreifen müssen. Nichts dergleichen geschah. Auch in der Linken gab es kaum Reaktionen. Wenn überhaupt wurde mit den Schultern gezuckt: Im Prinzip haben wir das doch alles eh schon vermutet, nur nicht jedes Detail gekannt. Und damit zurück zum kleinen Tagesgeschäft.

Unabhängig von der Frage, wie dieser alle Menschen betreffende Komplex hätte genutzt werden können (und vielleicht immer noch genutzt werden kann), um staats- und kapitalismuskritische Positionen in einer breiteren Öffentlichkeit auszubauen, hätte auch eine innerlinke Auseinandersetzung mit den Enthüllungen und unseren Kommunikationswegen stattfinden müssen. Vielleicht kann ja der Schwerpunkt dieser *RHZ*-Ausgabe zumindest ein paar Gespräche anstoßen. Denn was uns Edward Snowden und seine Unterstützer_innen über die Aktivitäten des US-amerikanischen Schnüffeldienstes NSA (National Security Agency), des britischen Pendants GCHQ (Government Communications Headquarters) und der befreundeten Dienste wie BND (Bundesnachrichtendienst) und VS (Verfassungsschutz) mitteilten, ist wahrlich nicht zum Schulterzucken geeignet.

So kann die NSA nach den geltenden gesetzlichen Konstruktionen der USA ohne richterliche Anordnung Telekommunikations- und auch Internetunternehmen zwingen, ihr Zugang zur persönlichen Kommunikation jedes und jeder Nichtamerikaner_in weltweit zu geben. Damit kann sie alle seine oder ihre Telefonate, Facebook-Chats, Google-Suchen, Yahoo-E-Mails und so weiter abrufen. Auch das massenhafte

flickr/YuriVuSamoilov (CC BY 2.0)

Sammeln von Metadaten ist dank des Patriot Acts und seiner weitreichenden Auslegung keinerlei richterlichen oder sonstigen Kontrolle unterworfen.

IT-Unternehmen und Geheimdienste Hand in Hand

Die Snowden-Dokumente machen deutlich, wie eng die Privatunternehmen mit der NSA zusammenarbeiten. Am besten zeigt dies das Beispiel Microsoft, ähnlich läuft es bei den meisten anderen Unternehmen. Microsoft wirbt für seine Produkte mit Slogans wie „Ihre Privatsphäre hat bei uns Priorität" oder „Wir halten es für wichtig, dass Sie die Kontrolle darüber haben, wer Zugang zu Ihren persönlichen Daten in der Cloud haben darf." Doch hinter den Werbebotschaften ist das Unternehmen geradezu übereifrig, der NSA Zugang zu mehreren seiner populärsten Dienste zu verschaffen – etwa zu Skype, Outlook und OneDrive (vormals SkyDrive). Mit letzterem speichern und bearbeiten rund 250 Millionen Menschen online Daten. In einem der von Snowden veröffentlichten NSA-Papiere heißt es: „Seit 7. März 2013 sammelt nun PRISM im Rahmen des Programms PRISM Standard Stored Communications Daten von Microsoft Skydrive für einen abgefragten Sektor. (...) Dieser Erfolg ist das Ergebnis monatelanger Zusammenarbeit des FBI mit Microsoft, um diese Lösung für die Abfrage und die Sammlung zu installieren."

Über Skype, 2011 von Microsoft aufgekauft, jubelte die NSA in einem Memo vom 3. April 2013: „PRISM ist nun in der Lage, Skype-Kommunikationen zu sammeln. (...) Die SSO geht davon aus, auf Kontaktlisten, Kreditkarten-Infos, Anrufprotokolle, Benutzerkonten-Infos und weiteres Material zugreifen zu können. (...) Die PRISM-Skype-Sammlung hat sich in weniger als zwei Jahren zu einem unerlässlichen Bestandteil der NSA-Berichterstattung entwickelt."

Mitte 2012 rüstete Microsoft sein E-Mail-Portal Outlook nach, um alle seine Kommunikationsdienste – darunter auch das viel genutzte Hotmail – in einem zentralen Programm zusammenzufassen. Die NSA hatte Sorge, dass ihr die Verschlüsselung, die Microsoft den Outlook-Kund_innen anbot, den Zugang zum Datenverkehr blockieren könnte. Aber bereits am 26. Dezember 2012 konnte die NSA in einem Memo feststellen: „Am 31. Juli begann Microsoft (MS), den webbasierten Chat mit der Einführung des neuen Outlook.com-Dienstes zu verschlüsseln. Diese neue Verschlüsselung – Secure Socket Layer (SSL) – hat die Gewinnung von Daten aus dem neuen Dienst (...) (bis zu einem gewissen Grad) für die Geheimdienste praktisch unmöglich gemacht. MS hat in Zusammenarbeit mit dem FBI eine Überwachungsmöglichkeit für das neue SSL entwickelt. Diese Lösungen wurden erfolgreich getestet und am 12. Dez. 2012 in den Echtbetrieb aufgenommen."

Auf soziale Online-Netzwerke wie Facebook und Twitter dagegen greift die NSA mit dem Programm XKeyscore zu. Das funktioniert so einfach wie die E-Mail-Durchsuchung: Ein_e Analyst_in gibt beispielsweise auf Facebook den gewünschten Namen ein, dazu den Datumsbereich der zu untersuchenden Aktivitäten, und schon liefert XKeyscore sämtliche Informationen, die das Profil enthält: Nachrichten, Chats, Kontakte, Fotos, private Beiträge. Allein im Dezember 2012 sammelte die Abteilung SSO der NSA auf diese Weise 41 Milliarden (!) Datensätze. Das Programm speichert den vollständigen Inhalt einer Seite drei bis fünf Tage lang, so dass Analyst_innen zeitlich zurückgehen und vollständige Sessions wiederherstellen können. „Interessanter" Inhalt kann dann extrahiert und in Datenbanken dauerhaft gespeichert werden.

In einem entsprechenden Memo vom 11. März 2011 feiert die NSA das Programm BLARNEY: „BLARNEY hat erste wesentlich bessere und vollständigere Facebook-Inhalte geliefert. Das ist ein wichtiger Schritt nach vorn und steigert die Möglichkeiten der NSA, (...) Facebook abzuschöpfen. Die Aktion wurde vor sechs Monaten in Partnerschaft mit dem FBI begonnen, um

das Problem eines unzuverlässigen und unvollständigen Facebook-Sammelsystems anzugehen. Damit hat die NSA nun Zugang zu einem breiten Spektrum von Facebook-Daten mittels Kontroll- und Suchvorgängen. OPIs sind begeistert, weil sie nun kontinuierlich viele Content-Felder erhalten, etwa Chats, die bisher nur gelegentlich zur Verfügung standen. Manche Contents werden völlig neu sein, zum Beispiel Teilnehmer-Videos. Insgesamt wird das neue Facebook-Sammelsystem eine gute Chance zum Ausspähen unserer Ziele bieten – von der Ortung auf der Grundlage ihrer IP-Adressen und des User Agent bis hin zum Sammeln sämtlicher privaten Kommunikation und zur Profilinformation."

Alles nicht so schlimm?

Ob nun gerade der eigene Account für Geheimdienste so wichtig ist, dass gerade er nicht nur routinemäßig abgegriffen, sondern auch konkret von einem Menschen ausgewertet wird, ist irrelevant. Zu wissen, dass es technisch möglich ist und permanent und massenhaft passiert, aber darauf zu hoffen, dass es gerade eine_n selbst nicht betrifft – was im Übrigen niemals überprüfbar ist – ist schon absurd. Immerhin haben in Spanien solche Ausforschungen schon zu konkreten Verhaftungen geführt.

Ähnliches wie für die oben ausführlicher dargestellten gilt in unterschiedlichem Maße auch für alle anderen Online-Angebote, egal wie viel uns die Anbieter über Sicherheit, Privatsphäre und eigene Möglichkeiten der Verschlüsselung erzählen. Und all diese Daten gibt die NSA an verschiedenste Dienste der USA und befreundeter Nationen weiter – auch an die deutschen Dienste.

Alles nicht so schlimm? Doch, alles sehr schlimm. Denn (auch vermeintlich private) Aktivitäten linker Menschen in den Online-Netzwerken müssen zwar nicht immer konkrete Ermittlungen unterstützen. Und sie müssen auch nicht zwingend politische Strukturen abbilden und damit offenlegen. Aber auch aus selektiven und privaten Aktivitäten, aus Urlaubsbildern oder schon den feststellbaren Online-Zeiten lassen sich Muster erstellen und damit (oder bei Abweichungen von ihnen) Bewegungen, Handlungen oder Verhalten erkennen oder vorhersagen. Auch das erhöht das Repressionsrisiko. Mal ganz unabhängig davon, dass Überwachung an sich auch zu Einschüchterung und damit Anpassung führt. Und wieder ganz konkret: Die britische Polizei experimentiert gerade recht erfolgreich damit, nicht zuzuordnende Bilder von Überwachungskameras mit Bildern auf Facebook abzugleichen, um so Menschen identifizieren zu können. Da genügt, in Verbindung mit den durch Metadaten feststellbaren Beziehungen, manchmal schon ein Gruppenbild von einer Party.

Selbstverständlich wird jede_r Leser_in Überwachung, Ausspähung, Manipulation ablehnen. Dafür (beziehungsweise dagegen) schreiben wir Flugblätter und Artikel, demonstrieren wir. Aber warum machen wir es den staatlichen und privatwirtschaftlichen Stellen dann in unserer täglichen Praxis so leicht, so viel über uns zu erfahren? Was aber soll oder kann unsere Konsequenz aus all dem so gern verdrängten Wissen um unsere Ausspähung und unsere eigene Komplizenschaft sein? Paranoia schieben? Den Stecker ziehen und raus aus diesem Internet (das wird sowieso bald wieder vergehen)?

Zumindest sollten wir als Menschen mit einem emanzipatorischen Anspruch die Angriffe auf uns nicht noch erleichtern. Dazu müssen wir nicht raus aus dem Internet und zurück zur Wandzeitung. Auch das Internet ist eine Plattform, auf und um die politisch gekämpft werden muss. Aber eine richtige Parole ist sicher die von Nadir verkündete: Raus aus Facebook! Denn einen „korrekten" Umgang mit Facebook gibt es nicht. Filter einschalten und Pseudonyme verwenden kann nicht Entstehung, Erkennung und Verknüpfung von Metadaten verhindern.

Druck ausüben, Alternativen nutzen, Eigenverantwortung zeigen

Wer es ablehnt, die – wie bequemen auch immer – Dienste der IT-Unternehmen in Anspruch zu nehmen, die mit der NSA und ihren Partnern zusammenarbeiten oder aber sich und die Daten ihrer Nutzer_innen nicht sichern wollen oder können, übt Druck aus. Andere Unternehmen oder Projekte, die tatsächlich einen Schutz der Privatsphäre anbieten wollen und können, werden so gestärkt – RiseUp beispielsweise, systemausfall.org, SO36.net, free.de, systemli, aktivix.org, immerda.ch, autistici, sindominio und viele andere. Die Liste der Alternativen zu GMX, Yahoo, Google und Microsoft ist lang. Außerhalb der sozialen Netzwerke, im klassischen E-Mail-Verkehr etwa, sollten auf jeden Fall Verschlüsselungsmethoden wie PGP und Browser-Anonymisierer wie Tor genutzt werden.

Wir stehen zwischen den beiden Polen Bequemlichkeit und große Reichweite einerseits und Offenlegung der eigenen Aktivitäten, Einstellungen und Strukturen andererseits. Und wir müssen uns positionieren, ob wir wollen oder nicht. In der Praxis läuft es auf einen Mix aus Eigenverantwortung, vertrauenswürdiger Infrastruktur (zumindest in Teilen), Verschlüsselung und Datensparsamkeit hinaus. Das durchzuhalten ist keine leichte Aufgabe. Aber Daten, die nicht online gestellt, abgegriffen und gespeichert werden, können auch nicht gegen uns verwendet werden. Offline wie online gilt: Anna und Arthur halten's Maul! ❖

■ Die NSA-Dokumente wurden zitiert nach Glenn Greenwald, Die globale Überwachung – Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, München 2014.

Wegbereiter eines smarten Totalitarismus?

Googles gesellschaftliche Gestaltungsmacht

Lars, Bochum

Google, Facebook, Twitter und Co. sind die idealen Dienstleister eines neuen digitalen „Panoptikums“. Sie sammeln und liefern individuelle Lebensmuster und schaffen damit ein umfassendes Instrumentarium, um Verhalten zu kategorisieren, vorherzusagen und zu beeinflussen. Die Monetarisierung und Monopolisierung von Informationen verleiht diesen Diensten eine historisch noch nie dagewesene gesellschaftliche Gestaltungsmacht. Unsere „freiwillige“ Teilhabe am digitalen „Dauersenden“ trägt maßgeblich zu dieser Machtkonzentration bei.

Warum begeben wir uns digital-exhibitionistisch in den Zustand völliger Durchleuchtung unserer Privatsphäre? Warum liefern wir freiwillig die Datenbasis, die jegliche Überwachung zur Selektion zwischen normalem und abweichendem Verhalten benötigt? Ein trendig, handlich-mobiles Lifestyle-Smartphone ermöglicht „soziale“ Teilhabe an einer nahezu allumfassenden digitalen Informationswelt. Alles in dem angenehmen Glauben, das eigene Leben und Arbeiten „smarter“ kontrollieren und effizienter dirigieren zu können. Die Animation zu Selbstoptimierung und -entblößung ersetzt überkommene Kategorien eines Orwell’schen Überwachungsstaates – niemand wird zum Schweigen gebracht, sondern vielmehr zum geschwätzigen „always on“ gedrängt. Dabei geben wir Kontrolle über sensible Details unserer Persönlichkeit an Dritte ab und büßen Selbstbestimmung durch eine völlig fremdbestimmte digitale Verwertung unserer permanenten Netzaktivität ein.

Erfassung und Vermessung aller Lebensabläufe

Meine über das Handy übermittelten Standorte markieren für mich „gewöhnliche“ Orte. Mein über Kredit-, EC- oder Payback-Karte protokollierter Geldverbrauch hinterlässt ebenfalls eine individuelle Alltagssignatur in Höhe, Ort und Verwendungszweck meiner Ausgaben. Telefon, Email, Twitter und Facebook liefern ein nahezu vollständiges Soziogramm meiner Kontakte: Eine einfache Software stellt die Frage „Wer ist mit wem wie intensiv verknüpf?“ grafisch dar. Stichwort- und semantische Analyse unverschlüsselter Kommunikation legen

den Charakter der sozialen Beziehungen offen und liefern ganz nebenbei meinen typischen „Sprachabdruck“. Schon eine Analyse weniger Monate bildet mein individuelles „Durchschnittsverhalten“ hinreichend präzise ab und macht das für mich „normale“ Verhalten vorhersagbar. Abweichungen von diesem Verhalten sind leicht detektierbar und lösen gleichsam bei Schnüffelbehörden und ökonomischen Datenverwerter*innen erhöhte Aufmerksamkeit aus.

Keine der genannten Auswertungsmethoden erfordert unmittelbaren Personalaufwand für die abhörende Behörde oder ihren privatwirtschaftlichen Partnerdienst. Niemand muss sich explizit für mich interessieren! Selbstlernende Algorithmen erledigen die Analysen über die Rechenzentren der Festplattenfarmen in der „Cloud“ automatisch und parallel für Millionen von „freiwilligen“ Datenlieferant*innen.

Wer sich ein Android-Smartphone der neuesten Generation zulegt nimmt in Kauf, dass es niemals ganz abgeschaltet ist. Denn es lässt sich komfortablerweise auf „Zuruf“ wecken und ansprechen. Neben dem Mikrofon ist auch die Kamera immer an, damit wir das Handy per Augenbewegung steuern können. Vollgestopft mit insgesamt 20 Sensoren nimmt es permanent unsere Umgebung wahr. Bei den Schnittstellen zum Datenaustausch hingegen spart der Hersteller bewusst, denn unsere Daten sollen alle in der „Cloud“, also auf Googles Festplattenfarmen, landen – unverschlüsselt, damit Google den Inhalt analysieren kann.

Fitnessarmband und Health Kit – Werkzeuge der Selbstoptimierung

Die Sensorik unserer ständigen Begleiter nähert sich dabei unserem Körper immer weiter an. Über 30.000 Apps (Anwendungsprogramme für Smartphones und Tablets), gibt es bereits zum Thema „Gesundheit und Fitness“, nochmal so viele zum Thema „Sport“ und etwa 25.000 aus dem Bereich „Medizin“. In kabelloser Verbindung zu einem der zahlreichen Fitnessarmbänder oder smarten Uhren zählen die Apps Schritte, messen Kalorienverbrauch, Puls und Blutzuckerspiegel und sagen uns, wie gut wir schlafen. Wer sie nutzt, soll genau kontrollieren, ob er die selbstgesteckten Ziele erreicht – ob es nun ums Abnehmen geht, um neue sportliche Bestleistungen oder darum, „gesünder“ zu leben. Ganz nebenbei wird auf spielerisch, smarte Weise die gesellschaftliche Doktrin der Selbstdisziplinierung und -optimierung verinnerlicht. Für moderne Leistungsträger*innen gehören die hippen Fitnessarmbänder als funktionales Lifestyle-Accessoire bereits zum Standard.

Während sich Patient*innen und Ärzt*innen bislang noch erfolgreich gegen den staatlich verordneten Funktionsausbau der elektronischen Gesundheitskarte zur digitalen Patientenakte wehren, lassen Google und Apple diesen konfliktreichen Aushandlungsprozess links liegen, indem sie das Smartphone von der Fitness- zur vollständigen Gesundheitszentrale ausbauen. Google Fit und Apples Health Kit fordern zur optimalen Gesundheitsbetreuung auf dem Smartphone die digitale Verwaltung von Arzt- und Laboruntersuchungen inklusive Medikation sowie die Eingabe der Ernährungsgewohnheiten.

Bei der Erfassung und Entschlüsselung des menschlichen Erbguts versucht Google, die Datenvorherrschaft zu erlangen. Mit der im Juni 2014 vorgestellten Zugangssoftware für Genomdateien stellte Google die wichtigste Plattform seines Projektes „Google Genomics“ vor – die „Google Cloud“ ist fortan für Analyse und Austausch von Daten der beiden weltgrößten Genomdatenbanken zuständig.

Alle Daten sind Kreditdaten – Googles „Life Operating System“

„Wir sind nicht die Kunden, wir sind die Produkte“ von Google, Facebook, Twitter und Konsorten. Begünstigt durch die Snowden-Enthüllungen und die Debatte um umfassende Ausspähung durch Geheimdienste und ihre privatwirtschaftlichen Partner*innen dringt diese Erkenntnis ganz langsam durch. Viele hatten lange geglaubt, Google sei im Wesentlichen eine Suchmaschine und die Erstellung der Datenbank aller Suchbegriffe samt „sinnvoller“ Ergebnisse diene in erster Linie der Angebots- und Wissensvermittlung.

Mittlerweile jedoch klingt es nicht mehr verschwörerisch, dass die Analyse der personalisierten Verknüpfung aller individuellen Suchanfragen das eigentliche Geschäft mit der Suchmaschine darstellt und die Suchmaschine lediglich das Herzstück für die Monopolstellung bei der Erfassung sämtlicher Lebensregungen ist. Denn hierauf gründet sich Googles Marktführerschaft bei Internet-Browsern (Google Chrome), bei Betriebssystemen für mobile Endgeräte (Android), Online-Videos (Youtube) und auf dem Bereich der Mail-Anbieter (GoogleMail). Google macht mittlerweile kein Geheimnis mehr aus dem Zugriff auf sämtliche unverschlüsselten Inhalte, die der Konzern in diesen Geschäftsbereichen sammelt. Eine von Google unerwünschte Von-Anfang-bis-Ende verschlüsselte Kommunikation ist die einzige Chance, dem zu begegnen.

Googles Finanzdienstleister „Zest“ benutzt nach eigenen Angaben sage und schreibe 80.000 verschiedene Indikatoren zur Überprüfung der Kreditwürdigkeit von Personen für seine Kund*innen und schreibt folgerichtig zum Geschäft mit der Inwertsetzung sämtlicher Lebensspuren: „Alle Daten sind Kreditdaten.“ Die Breite der erfassten Parameter lässt eine viel umfassendere „Bonitäts“-prüfung zu: Wer ist versicherungs-, bildungs- oder gesundheitsvorsorgewürdig?

In Zukunft sollen alle uns umgebenden und steuerbaren Dinge ein Betriebssystem haben und mit ihresgleichen und uns vernetzt sein. Google arbeitet aufgrund seiner Marktstellung und Finanzkraft mit Nachdruck daran, dass es sich hierbei um das Google-Betriebssystem Android handelt. So dienen die letzten Unternehmenszukäufe auf dem Bereich Thermostate, Rauchmelder, Haushaltsroboter, Überwachungskameras, selbstfahrende Autos, Satelliten, Drohnen, Internetseekabel und Internet-Ballons dazu, die eigene Systemsoftware zu platzieren und den Datenzugriff auf möglichst große Teile der Daten-Infrastruktur zu gewährleisten.

Die Beschreibung von Googles Aktivitäten wäre jedoch hoffnungslos gestrig, wenn wir den Eindruck vermittelten, die Erfassung samt Analyse personenbezogener Informationen wäre das eigentliche Ziel von Google. Es geht um mehr als Monetarisierung und Monopolisierung von Information. Es geht um nicht weniger als die Erschaffung neuer Realitäten.

Wer genauer auf das ehemalige Kernstück von Google schaut stellt fest, dass auch die Suchmaschine hochgradig manipulativ programmiert ist. Nicht nur im überkommenen Sinn möglichst zielgerichteter Werbung, sondern bezogen auf die Erreichbarkeit von Information an sich. Über den komplexen Algorithmus zur Gewichtung von Einträgen erhalten verschiedene Nutzer*innen unterschiedliche Informationen auf die gleiche Frage. Mit der Detailgenauigkeit der persönlichen Profile ist schon auf dieser Ebene eine subtile und hoch wirksame Beeinflussung von Nutzer*innen möglich. Ein anonymisierter Internetzugriff ist daher die absolute

Grundvoraussetzung, um dieser Manipulationsmöglichkeit zu begegnen.

Googles offen deklariertes Ziel ist es, diese Vorrangstellung als smart manipulativer Lebensbegleiter auszubauen. Schon bald werden wir Google nicht mehr nach Begriffen suchen lassen, sondern fragen, was als nächstes zu tun sei, so Google-Vorstand Eric Schmidt. Denn Google, so seine selbstbewusste Vorstellung, organisiert unsere gesamte Umgebung. Google widmet seit Neuem der Frage der Willensbildung und der Nachbildung menschlicher Gehirne mit dem Projekt „Google Brain“ einen eigenen Unternehmenszweig.

Im Unterschied zu Orwells Überwachungsstaat geht es nicht mehr um die Beschneidung des Gedankenspielraums, also das Unterdrücken von „Delikten“ im Stadium ihrer gedanklichen Entstehung, zum Beispiel durch das Eliminieren des Vokabulars zur Formulierung solcher Gedanken. Im Gegenteil, das „digitale Panoptikum“, das Google, Facebook und Co. derzeit stärker bestimmen als ihre staatlichen Partnerdienste, bringt niemanden zum Schweigen, sondern ermutigt alle zum „always on“ – dem digitalen Dauersenden. Statt Schweigen anzuordnen, animiert die neue Macht auf smarte Weise zur exhibitionistischen Organisierung und Optimierung des Selbst. Offenkundig wird niemand gefügig, sondern vielmehr abhängig gemacht. Keine bedrohliche, repressive Fratze, sondern die bunte, freundliche Welt der Apps wird dazu benötigt. Kreativität- und effizienzsteigernde Hilfsprogramme auf unseren Smartphones stimulieren zur „freiheitlichen“ Selbstentblößung.

Ansätze von Widerstand

Wer sich gegen die Verletzung von Persönlichkeitsrechten durch das Ausspionieren jeglicher Netzdaten, gegen DNA-Datenbank und (Drohnen-)Kameraüberwachung politisch aktiv zur Wehr setzen will, sollte auch mit der Preisgabe der eigenen Alltagsdaten nicht nur sparsamer, sondern vor allem strategisch umgehen. Gerade das Zusammenführen meiner verschiedenen Aktivitäten, Interessen, Neigungen, Einkäufe, Kommunikation zu einer integralen digitalen „Identität“ ist die Grundlage für die Mächtigkeit von schnüffelnden Analysewerkzeugen. Methoden des Identitäts-Splittings können mit annehmbarem Aufwand das reale Ich auf unterschiedliche digitale Identitäten „verteilen“.

Wir rufen dazu auf, den richtigerweise einzufordernden Grundsätzen eines freien und anonymen Netzes angesichts der Überwachungsrealität nicht ohnmächtig und tatenlos „hinterher zu diskutieren“, sondern a) die Möglichkeiten einer alltäglichen Verweigerung gegenüber digitaler Erfassung zu nutzen und b) den alltäglichen Übergriff aktiv anzugreifen.

Versuchen wir, Googles gesellschaftlicher Gestaltungsmacht ein deutliches und symbolträchtiges Zeichen entgegenzusetzen – Googles Datenbrille bietet dazu eine gute Gelegenheit, denn sie ist in breiten Teilen der Bevölkerung höchst umstritten. Google ist im Bereich des sozialen Widerstands übrigens extrem empfindlich. So war die Verunsicherung im Konzern groß, als im letzten Jahr mehrfach Googles Shuttle-Busse in San Francisco gestoppt und angegriffen wurden. Aktivist_innen hatten mit diesen Aktionen mobil gemacht gegen enorme Mietpreissteigerungen im Einzugsbereich der klimatisierten Luxus-Busse, die die solventen Google-Mitarbeiter_innen zur Konzernzentrale fahren.

Wenn wir unserem Gegenüber in der Bahn oder auf der Straße die Google-Brille absetzen, zündet die Diskussion um unfreiwillige Datenweitergabe vermutlich von selbst. Wer will schon per Bild-, Video- oder Tonaufzeichnung inklusive GPS-genauer Ortsinformation aufgenommen und auf Googles Festplattenfarmen verewigt werden? Wer will unmittelbar zum Zeitpunkt des Angeblicktwerdens per Ableich mit Googles Bilderdatenbank im Internet von jeder daher gelaufenen Datenbrillenträger_in identifiziert und gegoogelt werden?

Wir schlagen vor, die smarten Herren und Damen mit der „Google Glass“ im Gesicht von der Seite anzumachen und aufzufordern, ihre Daten-Brille umgehend wegzupacken – sonst machen wir das! Ziel ist es, mit alltäglicher und schwungvoller Konfrontation den rücksichtslosen Techno-Trendsetter_innen ihr 24-Stunden-Dasein als Googles unbezahlte Datensammler_innen unattraktiv zu machen und die öffentliche Debatte um die Erfassung und Auswertung persönlicher Daten zu befeuern. In den USA kam es bereits zu handfesten Auseinandersetzungen wegen der berechtigten Sorge, heimlich aufgezeichnet oder unmittelbar „gescannt“ zu werden. Viele Kneipen und Clubs beteiligen sich an der Kampagne gegen Googles „glassholes“ und schmeißen Datenbrillenträger_innen zum Schutz ihrer Kundschaft raus. Nicht ohne Grund wurde die Einführung der Datenbrille in Europa auf das vierte Quartal 2014 verschoben – im Überwachungskameras gewohnten Großbritannien ist die Brille hingegen schon seit Ende Juni 2014 erhältlich. ❖

Terroristensuche auf Facebook

Deutsche Geheimdienste weiten Online-Schnüffelei massiv aus

Redaktionskollektiv der RHZ

Die deutschen Geheimdienste wollen Online-Netzwerke deutlich stärker durchkämmen als bisher. Damit wollen sie auf Facebook, Instagram, Youtube und anderswo so bezeichnete Extremist_innen und Terrorist_innen entdecken und ausforschen – selbstverständlich auch linke. Allein der Auslandsgeheimdienst BND will dafür bis 2020 insgesamt 300 Millionen Euro zusätzlich. Und das vor allem für die Inlandsüberwachung zuständige Bundesamt für Verfassungsschutz (BfV) baut gerade eine neue Referatsgruppe auf, die „Erweiterte Fachunterstützung Internet" (EFI).

Das ist nicht weniger als „eine strategische und organisatorische Neuaufstellung", wie BfV-Präsident Hans-Georg Maaßen mitteilte. Die EFI soll mit ihren 75 Vollzeitstellen in sechs Referaten, angesiedelt in Berlin und in Köln, „Verbesserung und Ausbau der Telekommunikationsüberwachung von internetgestützter Individualkommunikation" gewährleisten. Der so direkt benannte Ausbau der Überwachung sei aber trotzdem „keine Ausweitung", es werde „auch in Zukunft (...) keine anlasslosen, verdachtsunabhängigen und damit ungezielten Maßnahmen" geben. Die neuen Mitarbeiter_innen – Stellenanzeigen wurden bereits im Frühjahr geschaltet – sollten lediglich ein computergestütztes System zur Auswertung großer Datenmengen schaffen. Eine manuelle Auswertung sei wegen des großen Datenvolumens nicht mehr möglich.

Sprich: Der Geheimdienst saugt schon seit langem massenhaft Daten „anlasslos, verdachtsunabhängig und damit ungezielt" aus dem Internet und den so genannten sozialen Netzwerken, kann sie in dieser Menge aber nicht wie gewünscht verarbeiten und auswerten. „Im Bereich der digitalen Kommunikation handelt es sich dabei um Daten, die das BfV gemäß seinen Befugnissen nach dem G-10-Gesetz bereits erhoben hat", heißt es in der Mitteilung ganz unmissverständlich[1]. Für die exzessive Extremist_innensuche im Netz berechnet das BfV allein im abgelaufenen Haushaltsjahr 2,75 Millionen Euro extra, weitere Mittel wurden beantragt.

Massive Ausweitung der Online-Überwachung

Natürlich arbeitet diese große Referatsgruppe nicht nur an der öffentlich angekündigten „Auswertung von großen Datenmengen". Laut *Süddeutscher Zeitung*, *WDR* und *NDR* geht es nach einem internen Papier des Geheimdienstes um ein System eben doch zur „Gewinnung, Verarbeitung und Auswertung von großen Datenmengen aus dem Internet". Kein Wunder, dass das BfV im Frühsommer Expert_innen „zum Auffinden und zur Darstellung bestimmter Informationen aus den Individualüberwachungsmaßnahmen (zum Beispiel eines Facebook-Chats)" suchte. Auch wenn der Geheimdienst also bislang schon alles abgreift und es daher eine quantitative Ausweitung gar nicht geben muss (oder kann): Die Erschließung all dieses Rohmaterials ist eine massive qualitative Ausweitung der Online-Überwachung.

Und die betrifft selbstverständlich nicht nur Leute, die beispielsweise IS-Logos und Syrien-Reisepläne offen auf ihr Profil stellen. Denn ob eine beliebige online aktive Person zu „Extremismus" oder Terrorismus neigt oder nicht, lässt sich eben oft erst feststellen, nachdem die Kommunikation geknackt und ausgewertet wurde. Und zum weiteren Ausbau soll die EFI nicht nur neue strategische und technische, sondern auch rechtliche Methoden der Informationsauswertung und -analyse entwickeln. Die Möglichkeiten des Geheimdienstes sollen also durchaus erweitert werden.

Dabei setzt das BfV auch auf die Kompetenz des „Strategie- und Forschungszentrums Telekommunikation", das bereits 2011 im Bereich des Bundesinnenministeriums gebildet wurde. Zum anderen will der Dienst aber ganz nebenbei die Möglichkeiten der Telekommunikationsüberwachung (TKÜ) mit dem System „Perseus" ausbauen. Das betrifft einerseits Internetkommunikation (E-Mail, Chatprotokolle, Websessions und Datentransfere). Andererseits steckt in diesem Paket aber auch die Aufbereitung der klassischen Telefonie (Sprache, Telefax, SMS), die damit noch besser gelingen soll – durch automatisierte Bearbeitung, aber alternativ auch durch andere Entschlüsselungswerkzeuge.

Neben der herkömmlichen anschlussbasierten Überwachung sollen dazu „darüber hinausgehende TKÜ-Varianten" zum Zuge kommen. Dazu zwinge den Geheimdienst die „Nomadisierung" des Nutzer_innenverhaltens, die Internationalisierung der angebotenen Dienste, die Verschlüsselung der Kommunikation sowie die mangelnde Verpflichtbarkeit ausländischer Provider. Das riecht nach dem massenhaften Einsatz von Trojanern. Und auch Formulierungen wie „konspirative informationstechnische Überwachungsmaßnahmen" von Online-Diensten (Server-TKÜ, Foren-Überwachung und E-Mail-TKÜ) deuten auf einen Ausbau der technischen Fähigkeiten hin.

Außerdem soll die EFI mit anderen Sicherheitsbehörden zusammenarbeiten und Daten und Erkenntnisse austauschen – eine nationale oder inhaltliche Begrenzung gibt es im EFI-Konzept nicht. Das BfV verweist zwar auf die durch den Grundgesetzartikel 10 gegebene rechtliche Begrenzung. Doch wie in einem Dokument der NSA vom Januar 2013 zu lesen ist, sind deutsche Dienste gern bereit, bei der Umsetzung des so genannten G-10-Gesetzes „Risiken" einzugehen. Und sie suchen laut NSA selbstständig nach „neuen Möglichkeiten" der Zusammenarbeit. Eine Ausweitung der Schnüffelei auf Facebook, Youtube & Co. will der deutsche Inlandsgeheimdienst in all dem aber nicht erkennen. ❖

1 Der verbreitete, aber sinnentstellende Name „G-10-Gesetz" steht für das „Gesetz zu Artikel 10 des Grundgesetzes" von 1968. Es regelt die Befugnisse der deutschen Nachrichtendienste zu Eingriffen in das durch Artikel 10 des Grundgesetzes garantierte Brief-, Post- und Fernmeldegeheimnis.

flickr/nikkilemieux (CC BY-ND 2.0)

Offline Aussagen verweigern, online alles offenlegen?

Beispiele aus der Praxis

Redaktionskollektiv der RHZ

Dass Polizei und Staatsanwaltschaft (und auch die diversen Geheimdienste) mit Interesse Homepages von linken Strukturen auswerten und gegebenenfalls gegen sie verwenden, ist nichts Neues. Erinnert sei hier nur an die unzähligen Verfahren gegen Menschen, die sich auf der Homepage von „Castor? Schottern!" öffentlich zum aktiven Protest gegen einen Castor-Transport bekannt hatten.

Aber in der Unterstützungspraxis der Roten Hilfe e. V. gibt es auch immer wieder Fälle, in denen Facebook, Twitter & Co. die Ermittlungsarbeit der Polizei erleichtert oder überhaupt erst ermöglicht haben. So bei einem Fall aus Göttingen: An Silvester 2013 sollen hier Burschenschaftler mit Böllern beworfen worden sein. Diese hielten den vermeintlichen Täter fest, letztlich konnte er ihnen aber entkommen. Allerdings hatte in dieser Situation einer seiner Freunde den Namen des Genossen gerufen. Mit dieser Information suchten die Burschis den Genossen dann bei Facebook – mit Erfolg. So kamen sie an seinen Familiennamen und weitere Daten und konnten ihn dann namentlich bei der Polizei anzeigen. Die polizeilichen Ermittlungen, die sonst erst einmal gegen Unbekannt geführt worden wären und vielleicht ergebnislos geblieben wären, wurden so ganz massiv erleichtert.

In einem anderen der Roten Hilfe e. V. bekannt gewordenen Fall durchsuchte die Polizei selbst die von einem Genossen und seinem sozialen und politischen Umfeld errichtete Online-Struktur: Gegen Unbekannt war wegen Körperverletzung Anzeige erstattet worden. Immerhin konnten Zeug_innen aber die Freundin des angeblichen Täters identifizieren. Die Polizei durchsuchte daraufhin den Facebook-Account der Freundin nach ihren Kontakten und fand so den Genossen, der dann identifiziert werden konnte. In der Folge wurde gegen ihn ermittelt und Anklage erhoben. Letztlich gab es einen Freispruch wegen Notwehr.

Auch in vielen weiteren Fällen dürften die eigenen Auftritte in den so genannten sozialen Netzen polizeiliche und staatsanwaltschaftliche Ermittlungen oder geheimdienstliche Analysen erleichtern oder überhaupt erst ermöglichen – unabhängig davon, ob es unseren Genoss_innen bekannt ist oder nicht und unabhängig davon, ob sie es beim Stellen eines Unterstützungsantrags erwähnen oder nicht. Die so wichtige Aussageverweigerung im direkten Kontakt mit Polizei und Staatsanwaltschaft wird so zumindest in Teilen entwertet oder ganz ad absurdum geführt. Und bei dieser Form der Offenlegung der eigenen Strukturen und Aktivitäten erweisen sich eben auch auf den ersten Blick völlig unproblematische Angaben und Beziehungen als möglicherweise entscheidend für den Erfolg der Repression gegen uns. ❖

Twittern für die Anti-Antifa?

Auch Nazis werten linke Online-Aktivitäten aus

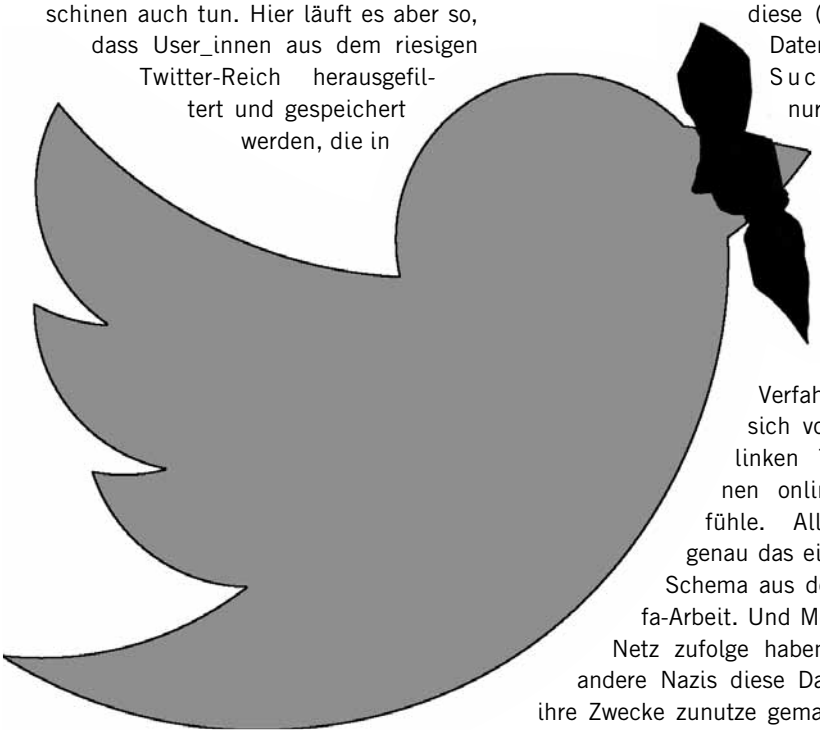
Redaktionskollektiv der RHZ

Nicht nur staatliche Repressionsorgane interessieren sich brennend für linke Äußerungen und Strukturen im Netz. Auch für faschistische Gruppen und Personen können linke Online-Präsenzen eine wahre Goldgrube sein, auch und besonders für Anti-Antifa-Aktivist_innen.

Ein nur auf den ersten Blick nicht allzu bedrohlich wirkendes Beispiel ist das eines rechten Berliners, der die Twitter-Accounts vor allem linker Aktivist_innen, Journalist_innen und Organisationen filzt. Darauf aufbauend hat er eine umfangreiche Datenbank politischer Gegner_innen angelegt, die ständig weiter ausgebaut wird. Auf seiner Homepage läuft eine Software, die automatisch Tweets crawlt, also auf bestimmte Begriffe rastert – ähnlich wie es Google und andere Suchmaschinen auch tun. Hier läuft es aber so, dass User_innen aus dem riesigen Twitter-Reich herausgefiltert und gespeichert werden, die in ihren Tweets bestimmte, Linken zugeordnete Begriffe verwenden – beispielsweise „Nazi“ oder „typische“ Begriffe aus der Antirassismus- oder Feminismusarbeit. Und dann landen sie mitsamt Screenshots auf der öffentlich einsehbaren und durchsuchbaren Liste der politischen Gegner_innen. Über 4.000 Twitter-Nutzer_innen und ihre Aussagen finden sich dort bereits.

Diese Liste führt nun beispielsweise viele sich als links verstehende Mitglieder der Piratenpartei (deren Mitglied auch der Initiator dieser Datenbank ist), Journalist_innen der *jungle World* (ebenso wie deren Hauptaccount) und anderer Medien, den zur Gentrifizierung forschenden Wissenschaftler Andrej Holm, den Berliner Abgeordneten Hakan Tas von der Partei Die Linke, die Initiative „Fußball gegen Nazis“ und die Gruppen „Antifa Heidekreis“ und „Antifa Union Dortmund“. Dazu kommen hunderte Einzelpersonen, die in dieser Datenbank landeteten, weil sie sich auf Twitter positiv zu antifaschistischen Themen äußerten.

Zwar behauptet der Betreiber, er führe diese (öffentliche!) Datenbank mit Suchfunktion nur zu privaten Zwecken – zur Dokumentation und Recherche als Vorbereitung auf juristische Verfahren, weil er sich von einzelnen linken Twitterer_innen online gemobbt fühle. Allerdings ist genau das ein bekanntes Schema aus der Anti-Antifa-Arbeit. Und Meldungen im Netz zufolge haben sich auch andere Nazis diese Datenbank für ihre Zwecke zunutze gemacht und die dort gesammelten Namen in eigene Listen kopiert.



„Wer Nachrichten im Netz verbreitet muss sich im Klaren sein, dass sie erfasst und verwertet werden.“

Allerdings hat sich der rechte Sammler, der in seinen eigenen Tweets auch schon mal davon phantasiert, seine „nach Anarchie“ schreienden Gegner_innen zu „kreuzigen und ihre Köpfe auf Speeren“ vor sich herzutragen, wenn sie sich außerhalb des Rechtsstaats mit ihm messen müssten, eine Verteidigung zurechtgelegt, die Linken durchaus zu denken geben sollte. So schreibt er: „Jeder der öffentlich Nachrichten im Netz verbreitet, muss sich im Klaren sein, dass diese Nachrichten erfasst, indexiert, kategorisiert und verwertet werden. Daher sollte man nur Dinge von sich publizieren, für die man auch morgen noch in den Spiegel schauen kann.“ Wenn auch das Hauptproblem dabei nicht die Betrachtung im eigenen Spiegel ist.

Aber es muss jedem und jeder Linken klar sein, dass eben nicht nur der für viele nur diffus wahrnehmbare staatliche Repressionsapparat in all seinen Ausformungen interessiert die linke Präsenz auf Twitter und Facebook, Flickr und Linkedin erforscht, speichert und nutzt. Auch Nazis und ihre Strukturen bedienen sich hier dankbar. Sicher auf einem technisch weniger hohen Niveau als beispielsweise der Verfassungsschutz, aber immer noch mit für uns ausreichend problematischen Ergebnissen. Mit der Benutzung von Facebook beispielsweise machen Linke nicht nur ihre eigene Kommunikation, Meinung, „Likes“ transparent. Sondern, viel folgenreicher, sie decken Strukturen und sogar Einzelpersonen aus ihrem Umfeld auf, die selbst mit Facebook oder anderen Kanälen wenig oder gar nichts zu tun haben. Sie geben zumindest Teile ihres privaten und beruflichen Umfelds preis und machen sich und dieses Umfeld damit angreifbar. ❖

„Das Netz ist ein politischer Raum, um den gekämpft werden muss“

Zur Facebook-Nutzung linker Gruppen und Menschen

Nadir

Facebook (fb) ist eine der größten privatwirtschaftlichen Datenkraken unter der Sonne – eine Einschätzung, die viele teilen werden. Nutzer*innen hinterlassen auf fb mehr Daten, als das bloße Auge sehen kann. Die Datenberge werden von fb im Hintergrund systematisch durchkämmt, um Profile zu ergänzen und Querverbindungen abzuleiten.

Daten werden nie gelöscht, selbst auf Klick hin nicht. Sie werden den Augen der User*in nur verborgen. Spätestens seit den Veröffentlichungen von Edward Snowden ist klar, dass diese Daten nicht bei fb bleiben, sondern ihren Weg in die Repressionsorgane finden. Die Kritik am Gebaren von fb lässt sich noch lange fortsetzen. Wir gehen davon aus, dass das Wesentliche bekannt ist. Trotz dieser Kritik wird fb von linken Gruppen zur Mobilisierung benutzt. Begründet wird dies mit der „Reichweite“, die eine Kampagne auf fb entwickeln kann oder auch mangelnder Zeit und fehlendem technischem Know How, um Alternativen zu nutzen.

Wer glaubt, fb mit fake accounts, der Nutzung von Tor und anderen technischen Finessen „gegen den Strich“, das heißt für die eigenen Zwecke und entgegen der Intention des Unternehmens nutzen zu können, gibt sich jedoch einer Illusion hin. Zwar lässt sich fb tatsächlich halbwegs anonymisiert als webspace-provider benutzen, aber diese Nutzungspraxis lässt sich nicht auf die Adressat*innen der Mobilisierung übertragen. Die oft gepriesene Reichweite auf fb entsteht dadurch, dass Nutzer*innen „Freundschaften“ schließen, Dinge „liken“, in Gruppen aktiv sind und sich eine Reputation erarbeitet haben – nur aufgrund dieses sozialen Netzes verbreiten sich Kampagnenmobilisierungen so gut.

Wenn die Adressat*innen sich aber um ihrer eigenen Sicherheit willen ähnlich „gegen den Strich“ verhalten wie die Mobilisierer*innen – keine Freundschaften schließen, nichts liken etc. – also ebenfalls mit minimalstem Datenschatten unterwegs sind, dann bricht die Reichweite auf das Niveau einer ordinären Webseite bei einem x-beliebigen Anbieter zusammen. Mit anderen Worten: Die Mobilisierer*innen sind darauf angewiesen, dass ihre Adressat*innen fb eben nicht gegen den Strich verwenden, sondern im Sinne von fb ordentlich Daten produzieren.

Spätestens hier stellt sich die Frage, ob ein nach Verwertungsinteressen modelliertes Soziales Netz mit einer nach Emanzipation strebenden sozialen Bewegung kompatibel ist oder ob nicht vielmehr ein emanzipatorisches Soziales Netz nur aus und mit der Bewegung entstehen kann. Beispiele hierfür könnten Indymedia und das spanische Soziale Netz „Lorea“ sein.

Das Netz ist ein politischer Raum, um den gekämpft werden muss – die andere Seite ist jedenfalls schon jetzt mit Kräften dabei! ❖

„Unproblematisch, um linke Analysen mitzuteilen“

Zum Nutzen von Facebook und Twitter für linke Gruppen

Antifa Pinneberg

Wir sind Antifaschist_innen aus Schleswig-Holstein und dort in der Antifa Pinneberg organisiert. Wir wurden von der Ortsgruppe Hamburg der Roten Hilfe e.V. für eine Diskussionsveranstaltung zum Umgang mit Facebook & Co. angefragt. Vor allem deshalb, weil wir mal mehr, mal weniger Twitter nutzen, um zu mobilisieren und Nachrichten zu verschiedenen Themen zu verbreiten.

Wir sind beim Thema Facebook & Co. ganz sicher keine Expert_innen, niemand von uns nutzt Facebook oder Twitter, um privat zu kommunizieren. Auch als Gruppe nutzen wir Facebook nicht. Facebook und Twitter sind sicher gut, um schnell zu verschiedenen Themen viele Informationen zu bekommen, ungeachtet ihrer Qualität.

Wir halten beide Netzwerke nicht nur für problematisch, um über Themen zu diskutieren, sondern lehnen es als Möglichkeit ab. Für problematisch halten wir nicht, dass sich Gruppen/Initiativen wie zum Beispiel NSU-Watch auch auf Facebook und Twitter bewegen und so anderen Menschen ihre Analyse mitteilen.

Problematisch sehen wir, dass Einzelpersonen durch Kommentare/Diskussionen/Likes in diesen Netzwerken unbedacht politische Zusammenhänge offenlegen und so sich und andere gefährden.

Letztlich kann es nur heißen, seinen Facebook- und/oder Twitter-Account zu schließen. ❖

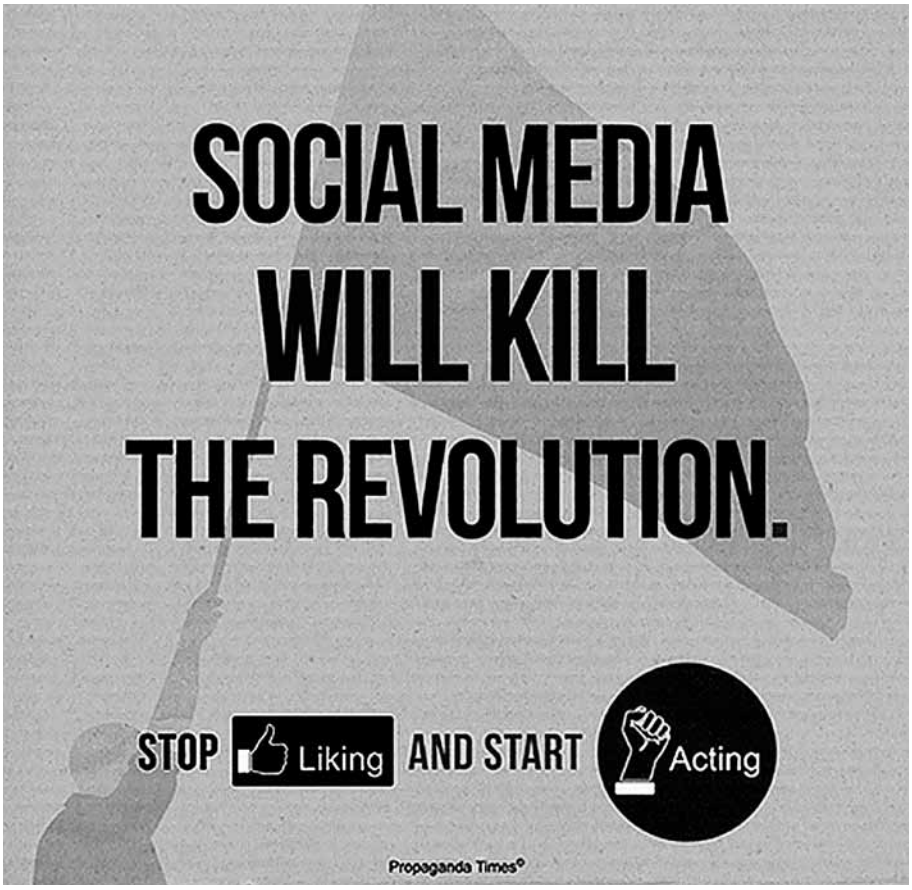
► http://antifapinneberg.blogsport.de

World Wide War

Software zur Aufstandsbekämpfung

Münchner Soligruppe für die kriminalisierten Antimilitarist_innen vom GÜZ-Camp

Im Mai 2014 berichteten die *Süddeutsche Zeitung* und andere Medien über ein technisches Aufrüstungsprogramm, das sich der BND 300 Millionen Euro kosten lassen will. Ziel ist, die Internetkommunikation in sozialen Netzwerken wie Facebook und Twitter in Echtzeit zu überwachen und aus den Daten Analysen über mögliche Bedrohungen für die Bundesrepublik zu erstellen. Entwickelt und weltweit vermarktet wird die benötigte Überwachungstechnik von Software- und Rüstungsfirmen. Abnehmer_innen sind vor allem Polizeibehörden und Militär, die diese Technik nicht zur „Auslandsaufklärung", sondern vor allem zur Überwachung und Aufstandsbekämpfung im Inland einsetzen.



PropagandaTimes (CC BY-NC-ND 2.0)

Soziale Netzwerke töten die Revolution! Drum raus aus dem Netz und rein ins wahre Leben …

Durch die Enthüllungen des ehemaligen Geheimdienst-Mitarbeiters Edward Snowden ist bisher zumindest ansatzweise die Ausforschungspraxis von Einzelpersonen und Institutionen weltweit durch den amerikanischen Militärgeheimdienst NSA und den britischen Nachrichtendienst GCHQ öffentlich geworden. Dabei ist die Überwachung wohl vor allem auf quantitativer Ebene eine neue Dimension. Die Praxis selbst, Datenströme zu protokollieren, im Bedarfsfall zu entschlüsseln und auszuwerten und digitale Kommunikation in Echtzeit zu überwachen, ist schon länger Bestandteil der Geheimdienstarbeit vieler Länder dieser Erde.

Die Technik, die dafür notwendig ist, wird seit Jahren von zahlreichen IT-Spezialfirmen in unterschiedlichen Formaten entwickelt, angeboten und verkauft. Auch die verschiedenen Polizeibehörden der BRD kaufen diese Technologie und setzen sie ein. Zuletzt geriet der von der hessischen Firma DigiTask für das BKA entwickelte „Bundestrojaner" in die Schlagzeilen, weil er so programmiert wurde, dass seine Anwendungsmöglichkeiten gesetzliche Einschränkungen missachteten.

Weltweit gibt es mehrere hundert Anbieter_innen im IT-Sektor und Militärbereich, die sich auf diesem Markt bewegen. Sie tummeln sich auf internationalen Sicherheitsmessen, werben für ihre Produkte gerne mit Kriegsszenarien und verkaufen an jeden, der genug bezahlt. Die Reputation der Kund_innen, vorrangig staatliche Institutionen wie Polizei, Geheimdienste und Militär, spielt keine Rolle. Eine italienische Sicherheitsfirma preist ihre Trojaner mit dem Slogan an: „Der Krieg der Zukunft findet nicht auf dem Schlachtfeld statt sondern im Internet (…) In diesem Szenario ist die wichtigste Waffe Informationsgewinnung." Sie bietet für diesen Krieg Programme und Produkte an, mit denen die Computer der Gegner_innen angegriffen und überwacht werden können.

Fließende Grenzen zwischen Krieg, Aufstand und Kontrolle

Die Grenzen zwischen Krieg, Aufstand und Kontrolle sozialer Bewegungen sind in Zeiten der „asymmetrischen Konfrontationen" allerdings fließend geworden. Der Krieg der Zukunft ist in der Vorstellungswelt von Politik, Militär und Kapital nicht mehr unbedingt ein territorialer Konflikt. Die größte Bedrohung wird in Angriffen auf die digitalen Kommunikationsnetze gesehen, mit denen die materiellen Produktionsprozesse lahmgelegt werden kön-

nen. Insofern ist sowohl der Schutz der jeweiligen digitalen Netzwerke wie auch die Fähigkeit, in andere einzudringen und diese zu zerstören, von zentraler militärstrategischer Bedeutung. Auch der Krieg nach innen, die Kontrolle antagonistischer gesellschaftlicher Strukturen und sozialer Protestbewegungen wird mit diesen Waffen geführt.

Deutsche IT-Firmen wie Gamma International oder Trovicor gehören technisch zumindest zu den Weltmarktführer_innen im Bereich der Internetüberwachung. Beide haben ihren Sitz in München, einer Metropole konventioneller Rüstungsproduzent_innen wie Krauss-Maffei und EADS. Gamma und Trovicor gerieten im letzten Jahr noch vor Snowdens Enthüllungen über die NSA in die Schlagzeilen, weil sie Überwachungstechnik in Länder des „Arabischen Frühlings“ verkauft hatten. Sie bieten Produkte an, mit denen einzelne Menschen überwacht werden können, indem ihre Computer und Handys mit einem Trojaner infiziert werden. Dadurch können die Anwender_innen kontrollieren und protokollieren, mit wem und worüber eine „Zielperson“ kommuniziert. Es können die Passwörter ausgelesen werden, mit denen Computer oder Mails geschützt werden sollen. Es können aber auch Screenshots vom Bildschirm gemacht oder interne Geräte wie Kamera und Mikrofon aktiviert werden, um die „Zielpersonen“ zu kontrollieren.

In verschiedenen Erklärungen hat der Geschäftsführer von Gamma, Martin Münch, seine Verantwortung für den Einsatz von Überwachungssoftware seiner Firma in arabischen oder asiatischen Diktaturen abgestritten. So waren in Ägypten nach dem Sturz von Mubarak Kostenvoranschläge von Gamma aufgetaucht für Installation, Betrieb und die notwendigen Schulungen vor Ort. Auf Computern von Aktivist_innen aus Bahrain wurden Trojaner von Gamma entdeckt. Dort hatte die Regierung 2011 Demonstrationen mit Hilfe saudischer Panzer (von Krauss-Maffei aus München) niederschlagen lassen. Das geplante Geschäft mit Ägypten sei nie zustande gekommen, behauptet Münch. Die Software, die in Bahrain eingesetzt wurde, sei vorher auf einer Sicherheitsmesse den Mitarbeitern seiner Firma gestohlen worden.

Gegenüber der *Süddeutschen Zeitung* wurde Münch geradezu philosophisch: „Software foltert keine Leute.“ Er könne die Aufregung nicht verstehen. „Ich finde es gut, dass die Polizei ihren Job macht.“ Das will er wenigstens dem deutschen BKA ermöglichen. Nach der DigiTask-Pleite mit dem alten „Bundestrojaner“ soll nun eine Version des Gamma-Programms „FinFisher“ an die Wiesbadener Schnüffelbehörde ausgeliefert werden, die aber noch „den gesetzlichen Vorgaben der Bundesrepublik angepasst“ werden müsse.

Die Überwachungspraxis mit diesen „Remote Control Systems“ wird in Fachkreisen als „Lawful Interception“ (rechtmäßige Überwachung) bezeichnet. Es werden aber auch „Monitoring-Systeme“ eingesetzt, die zum Beispiel im größeren Stil die Aufenthaltsorte bestimmter Handys überwachen. Kommt es zu einer Ansammlung von mehreren als verdächtig registrierten Nummern auf engem Raum oder in der Nähe bestimmter Orte, gibt das System eine Alarmmeldung: „Bad-Guy-Gathering“. Es können die Datenströme im Internet in Echtzeit ausgewertet werden, um zu beobachten, ob bestimmte Webseiten besucht werden, Schlagwörter benutzt oder Verschlüsselungstechniken genutzt werden. Dann lässt sich schnell herausfiltern, von welchen Anschlüssen diese Kommunikation ausgeht. Solche „Deep Packet Inspection“ (DPI) Systeme werden zum Beispiel von der Leipziger Firma Ipoque angeboten oder von der französischen Firma Amesys, die ihr DPI-System EagleGlint an Ghaddafis Geheimpolizei nach Libyen geliefert hat. Ihre deutsche Niederlassung hat sie – der Weltgeist zwinkert – in München.

Schnüffeln für Syrien, Bahrain und Bayern

Die ebenfalls in München ansässige Firma Trovicor ist 2009 aus der Auflösung der Geschäfte der Siemens-Tochter Nokia Siemens Networks hervorgegangen und hat auch deren Kund_innen übernommen. Dazu zählen an prominenter Stelle die Regierungen von Iran und Syrien. 2012 berichtete das ARD-Magazin „Fakt“ über die Lieferungen von Netzüberwachungstechnik von Siemens beziehungsweise Trovicor nach Syrien seit dem Jahr 2000. Es sollen „Monitoring-Center“ an die Telefongesellschaften Syriatel und STE geliefert worden sein, die Mobil- und Festnetzkommunikation überwachen. Sie können nachgerüstet werden, verspricht die Trovicor-Webseite: „Populäre Anwendungen sind beispielsweise Location Tracking, Spracherkennung und Link-Analyse.“

Auf solche Dienste möchte keine Ordnungsbehörde gerne verzichten und zum Glück sind vor Gott und dem Eigentümer von Trovicor alle Kunden gleich. Neben Bahrain und den Vereinigten Arabischen Emiraten nimmt auch das seit 68 Jahren ausschließlich demokratischen Grundsätzen verpflichtete Landeskriminalamt des Freistaats Bayern die Dienste dieser Firma in Anspruch und lässt sich seine Überwachungseinrichtungen von Trovicor-Techniker_innen pflegen. Die Wurzeln dieser Zusammenarbeit liegen wahrscheinlich in der alten Verbundenheit mit dem Siemens-Konzern, von dem Trovicor auch das traditionsreiche Iran-Geschäft geerbt hat. Dort war Siemens schon seit den 50er Jahren tätig und baute das Telefonnetz auf. Bei der Gelegenheit gewährte die Firma dem deutschen Auslandsgeheimdienst BND, nur fünf Kilometer von der Siemens-Zentrale entfernt in Pullach ansässig, einen dauerhaften und exklusiven Zugang zur Überwachung des iranischen Telefonverkehrs. Gleichermaßen wurde auch mit den Telekommunikationseinrichtungen verfahren, die Siemens in anderen Ländern installierte.

Der BND unterhielt für den Zugang zu diesen Systemen auf dem Siemensgelände in der Münchner Hofmannstraße ein eigenes Büro unter der phantasievollen Bezeichnung ICM Voice & Data Recording, das 2009 von Trovicor übernommen worden sein soll. Über bestehende Verbindungen zwischen Trovicor und BND wird insofern nicht ganz zufällig spekuliert. In ihren Reaktionen auf die öffentlich gewordenen Verkäufe von Überwachungstechnik an folternde Diktaturen reagierten Siemens-Verantwortliche gerne mit dem zynischen Hinweis darauf, dass die Technik den Vorgaben des European Telecommunications Standards Institute (ETSI) entsprächen. In diesen Standards legen große Firmen wie Siemens oder Vodafone zusammen mit namhaften Geheimdiensten wie dem deutschen Verfassungsschutz und dem britischen GCHQ europaweit fest, welche Informationen aus den Telefonnetzen von den Betreiber_innen über elektronische Schnittstellen an Überwachungs- und Repressionsorgane bereitgestellt werden. Außerdem unterliege diese Technik auch keinen Exportbeschränkungen. Also alles kein Grund zur Aufregung?

Die Entwicklung von Trojanern, die sich erfolgreich und unerkannt in Computersysteme einnisten sollen, setzt das Wissen über Sicherheitslücken gängiger Soft- und Hardware voraus. Viele Firmen, die Kommunikationsüberwachungstechnik anbieten, haben ihren eigentlichen

Schwerpunkt in der Entwicklung und dem Verkauf kommerzieller Verschlüsselungs- und Anti-Viren-Programme. Das ist kein Widerspruch sondern konsequent, verfügen diese Firmen doch genau deshalb bereits über das nötige Know-how zur Herstellung von Virenprogrammen. Um immer auf dem aktuellen Stand der technischen Entwicklung zu bleiben, pflegen diese Firmen eine enge Zusammenarbeit mit profilierten Hacker_innen. Auch der Geschäftsführer von Gamma International, Martin Münch, stammt ursprünglich aus der Hackerszene und wurde vor einigen Jahren vom englischen Gamma-Mutterkonzern zunächst für Workshops und Software-Tests engagiert.

Allerdings kommen die großen Firmen auf dem Markt der Überwachung und Kontrolle direkt aus dem Bereich der Rüstungsproduktion. Der amerikanische Rüstungskonzern Boeing bietet Kommunikationsüberwachungstechnik über seine Tochter Naurus an, die unter anderem Ghaddafis Schergen in Libyen beliefert hat. EADS Defence & Security lieferte 2009 „Sicherheitssysteme zur Informationsgewinnung für organisationsübergreifende Einsätze“ von Polizei und Militär in die Vereinigten Arabischen Emirate. Sie könnten auch Aufstandsbekämpfungstechnik genannt werden.

Cyber-War aus dem Hause Siemens

Siemens lieferte nicht nur Überwachungstechnik in den Iran, mit der das Regime soziale Proteste kontrollieren will, sondern auch die Steuerungsgeräte für die Uranzentrifugen – wesentliche Bausteine im iranischen Atomprogramm – die vor drei Jahren mit dem Computervirus Stuxnet angegriffen wurden. Programmiert wurde der Virus höchstwahrscheinlich vom amerikanischen Militär. Fachleute gehen davon aus, dass auch Ingenieur_innen von Siemens daran beteiligt gewesen sein müssen, indem sie den Programmier_innen ihr Wissen über die Funktionsweise und Sicherheitslücken der Steuerungsgeräte zur Verfügung gestellt haben.

Stuxnet ist nur ein Beispiel für das, was sich Militärstrateg_innen unter Cyber-War vorstellen: die Zerstörung der Infrastruktur anderer Länder über das Internet. Auch die Bundeswehr rüstet sich inzwischen für dieses Kampffeld. In der Tomburg-Kaserne bei Bonn wird seit 2006 die Abteilung „Computernetzwerkoperationen“ aufgebaut, die die Aufgabe hat, im Ernstfall gegnerische Informations- und Kommunikationsnetze umfassend anzugreifen und zu zerstören. Und im letzten Jahr wurde an der Münchner Bundeswehrhochschule ein „Cyber Defense“-Forschungszentrum eingerichtet, in dem Militär, Industrie, Geheimdienste und Wissenschaft gemeinsam „Sicherheitslösungen gegen Cyber-Angriffe“ entwickeln wollen.

Hier wird auch eine vom BND beauftragte Studie zur „Automatisierten Beobachtung von Internetinhalten“ erstellt, mit deren Hilfe der BND im Rahmen der so genannten „Strategischen Initiative Technik“ in den nächsten Jahren seine Möglichkeiten ausbauen will, Weblogs, Foren und Portale wie Facebook und Twitter systematisch in Echtzeit zu beobachten und auszuwerten. Durch die Überwachung könne man sich ein genaueres Bild über die Lage im Ausland verschaffen, behaupten die Schnüffler_innen. Dass soziale Netzwerke nicht an nationale Grenzen gebunden sind, sollte allerdings auch in Pullach bekannt sein. Dass dort dann Daten von deutschen Staatsangehörigen vor der Analyse oder sogar schon während der Überwachung herausgefiltert und gelöscht werden, darf getrost bezweifelt werden.

Das Gejammer über den befürchteten „technischen Rückstand“ gegenüber NSA und GCHQ ist nicht glaubwürdig. Der BND ist seit Jahren in enger Kooperation mit diesen Diensten verbunden und die von ihnen eingesetzte Technik steht auch den deutschen Geheimdiensten zur Verfügung. Die Vorstellung, deutsche Datenschutzbestimmungen und klamme Kassen hätten uns bisher eine Massenüberwachung durch die eigenen Geheimdienste erspart, ist lächerlich.

Der nach dem 11. September 2001 begonnene weltweite „Krieg gegen den Terror“ ist zu einem Label geworden, mit dem der Drohnenkrieg in Pakistan und Jemen genauso gerechtfertigt wird wie die globale Kommunikationsüberwachung durch die verschiedenen Nato-Geheimdienste. Das Geschwätz von einem „Supergrundrecht Sicherheit“, zu dessen Verwirklichung alle anderen Grundrechte von Geheimdiensten und Militär jederzeit, überall und für alle ausgesetzt werden können (immerhin gilt das gleichermaßen für Staatspräsidenten und Kanzlerinnen wie für Bürgerrechtsaktivist_innen oder Facebook-User_innen) verweist darauf, dass es tatsächlich um die Sicherung von Herrschaft mit allen verfügbaren Mitteln geht.

In den als „asymmetrisch“ definierten Konfrontationen wird die umfassende Überwachung aller Menschen, die Kontrolle ihrer sämtlichen physischen und sozialen Äußerungen und Bewegungen als zentrales Mittel der Prävention gesehen und eingesetzt. Wer sich ein Bild von der geplanten Vernetzung der verschiedenen Überwachungstechniken zur Kontrolle und Aufstandsbekämpfung in der EU machen möchte, kann einfach mal den Wikipedia-Artikel zum EU-Forschungsprojekt INDECT lesen.

Der Widerstand gegen die bereits heute praktizierte Überwachung beginnt mit der Verweigerung, die persönlichen Daten freiwillig herzugeben. Egal ob beim Surfen im Netz, durch elektronische Kommunikation oder bargeldlosen Konsum. Eine umfassendere Widerstandsstrategie und -praxis fehlt allerdings bisher in der radikalen Linken weitgehend. Das müssen wir schnell ändern. ❖