Dietrich Meyer-Ebrecht

Besteht die Chance einer demokratischen Gestaltung und Kontrolle unserer Kommunikationsnetze?

If you think technology can solve your security
problems, then you don't understand the problems
and you don't understand the technology.
(Bruce Schneier)[1]

Edward Snowden hat uns mit seinen Enthüllungen gelehrt: Geheimdienste, allen voran die NSA, sind mit der Massivität ihrer personellen und finanziellen Mittel, mit ihrer Aggregation an Expertise und Kreativität in der Lage, jeden Datenstrom anzuzapfen, sich Zugang zu jeder Datensammlung zu verschaffen. Nur mit einem unverhältnismäßig hohen Aufwand und mit erheblichen Einschränkungen könnten wir uns dagegen schützen, und es bleibt offen, ob ein 100%iger Schutz überhaupt erreicht werden kann. Bürgerrechte im Digitalen – so können wir Bruce Schneiers Statement interpretieren – sind nicht technisch zu haben, sie sind zwischen Politik und Gesellschaft auszuhandeln.

Nicht verhandelbar in einer freiheitlichen Gesellschaft ist die Privatsphäre. Der Schutz der informationellen Privatsphäre stellt jedoch eine ganz besondere Herausforderung dar. Anderes als im Physischen gibt es im Digitalen zwischen öffentlichem Raum und privatem Raum keine Türen, die verriegelt werden können. Die Abgrenzung ist eher eine Art semipermeable Membran, vergleichbar mit der Hülle einer biologischen Zelle. Denn für den Informationsaustausch bedarf es einer selektiven Durchlässigkeit, wenn die Optionen der Kommunikationsnetze sowohl einen individuellen als auch einen gesellschaftlichen Nutzen haben sollen. Schutz und Nutzen zugleich kann jedoch nur gewährt werden, wenn die digitale Außenwelt demokratischen Spielregeln folgt, einer demokratischen Kotrolle unterzogen wird. Dies fordert den Staat. Der Schutz seiner Bürger muss durch eine angemessene Gesetzgebung – und ihre Durchsetzung! – garantiert sein. Dazu gehört ein politischer Wille. Unverzichtbar ist aber auch das gesellschaftliche Engagement. Beides ist derzeit schwer zu haben. Wollen wir die Chancen für eine demokratische Gestaltung und Kontrolle der Netze abwägen und Lösungswege skizzieren, müssen wir uns mit den Problemen und Missverständnissen auseinander setzen, die diesem Ziel im Wege stehen, die gleichsam als 'Bedrohung von innen' wirken.

Die Politik – handlungsunfähig?

Hier treffen wir auf drei Komplexe. Der erste ist die innen- und außenpolitische Dimension: das Themas betrifft die Sicherheitspolitik. Ausspähung ist ein wesentliches Element des Cyberwarfare, der digitalen Kriegsführung. Die wiederum ist eine zentrale Säule der strategischen Doktrin für eine neue, technologieorientierte Kriegsführung. Die strategischen Szenarien beschreiben den Einsatz von Cyberoperationen in Phasen: Phase 0 „Konditionierung" dient dem Erkennen der Absichten des potentiellen Gegners – oder auch Freundes. Geheime Zugänge zu dessen Netzwerken werden angelegt, auch als Vorbereitung der folgenden Phasen. In Phase 1 „Abschreckung" werden dem Gegner mit spürbaren Operationen ‚die digitalen Muskeln gezeigt'. In Phase 2 „Dominieren" werden Operationen eingeleitet, die den Gegner schwächen sollen, wie Sabotageakte oder die Übernahme der Kontrolle über kritische Systeme. Aus dieser Sicht müssen wir die gegenwärtige ungebremste

Ausspähung staatlicher Institutionen, Wirtschaft und Industrie, Forschungseinrichtungen und privater Personen bereits als Cyberkrieg in der Phase 0 verstehen.

All diese hoch geheim gehaltenen Operationen schwimmen gleichsam mit in den zivilen Informationsströmen. Sie stellen ein Fundamentalrisiko für die Zivilgesellschaft dar! Militärische Überlegungen waren zwar der Ursprung des Internet. Längst ist es aber zu einem kaum verzichtbares Instrument der Zivilgesellschaft geworden. Mit der regelmäßigen Nutzung für militärische Cyberoperationen unterliegt es spätestens heute wieder eindeutig militärischen Herrschaftsansprüchen und militärischen Denkkategorien. Militärisches Denken bestimmt bereits die Ausspähungsaktivitäten. Kennzeichnend dafür sind die Erfolgskriterien: Sie sind nicht wie im Zivilen orientiert am bestmöglichen Erreichen eines Zieles unter geringst möglichen Schäden – der Erfolgsfall ist, wenn das Ziel überhaupt erreicht wird, unter Inkaufnahme jedweder Kollateralschäden. Verständlich wird unter dem militärischen Aspekt auch die üppige Ausstattung der Geheimdienste. Und auch die Freistellung von zivilrechtlichen Normen. Als US-Präsident George W. Busch unmittelbar nach dem 9/11-Attentat den damaligen Direktor der NSA, Michael V. Hayden fragte, „was braucht ihr, damit so etwas nie wieder geschieht?“, war es unter anderem die Autorisierung, US-amerikanische Bürger auch gegen geltendes Recht ausspähen zu dürfen. Und er bekam, was er sich wünschte, an allen demokratischen Institutionen vorbei.

Einer wirksamen parlamentarischen Kontrolle entziehen sich auch unsere eigenen Geheimdienste. Aus Snowdens Enthüllungen wurde auch offensichtlich, dass sich BND und NSA gegenseitig darin zuarbeiten, Bürger und Institutionen auszuspähen. Dies bestätigte auch William Binney, früherer technischer Direktor der NSA, heute ihr vehementer Kritiker, in einer Anhörung im NSA-Ausschuss des Deutschen Bundestages. Die Zusammenarbeite des BND mit US-Geheimdiensten hat historische Wurzeln. Sie stützt sich auf schon sehr alte bilaterale Verträge, Zusatzabkommen zum Nato-Truppenstatut und, wie kürzlich im SPIEGEL berichtet, auf Geheimverträge zwischen BND und NSA – ein Tabuthema für unsere Politik! „Deutschland braucht dringend einen Snowden aus dem BND,“ empfahl in einem Interview kürzlich Thomas Drake, als Whistleblower der NSA ein Vorgänger von Snowden.[2] Unsere Gesellschaft muss Aufklärung einfordern, um einschätzen zu können, wo politische Hebel angesetzt werden müssen. Derzeit kann unsere Regierung ihrem Schutzauftrag gegenüber uns Bürgern gar nicht nachkommen, denn sie müsste den Diensten die Arme binden und damit gegenüber den amerikanischen Freunden vertragsbrüchig werden. Ohne sehr massiven gesellschaftlichen Druck wird sich eine Bewegung in der Politik auf diesem Feld nicht erzielen lassen.

Die Gesellschaft – veränderungsunwillig?

Leider lässt sich auch die Gesellschaft dazu kaum bewegen – der zweite Komplex. Denn wir werden auch etwas aufgeben müssen. Zur Disposition stehen private Verhaltensmuster und wirtschaftliche Interessen. Wir haben uns an den Komfort und den Effizienzgewinn gewöhnt, die uns die Netze bieten, und wir sträuben uns gegen jede Einschränkung. Wir wollen ja nicht wieder Briefe schreiben müssen und versenden deshalb weiterhin vertrauliche Information unverschlüsselt, für den 'man-in-the-middle' ohne große Mühe mitlesbar. Oder wir ‚posten’ sie samt intimer Bildern gleichsam an Anschlagbrettern auf öffentlichen Plätzen. Schon wird es schwierig, sich dem sozialen Druck zu entziehen, die private Kommunikation nur noch über soziale Netze abzuwickeln, Bilder und Videos auf Plattformen wie Flickr oder YouTube zu 'teilen', regelmäßig 'Lebenszeichen' zu tweeten.

Unsere persönlichsten Daten laden wir in die 'Cloud', um von überall her darauf zugreifen zu können. Aber so wolkig wie der Name sind unsere Vorstellung davon, wo und wie unsere Daten gespeichert werden, wie sicher unsere Daten dort bewahrt werden. Ein Beispiel, wie wohlfeil Ausspähtechnologie ist: Auf ihren Webseiten bietet die russische Firma Elcomsoft ein Programm an, mit dem man in die Cloud-Backups von iOS- und Blackberry-Geräten einbrechen kann, in der 'forensischen' Version auch, ohne die Kontrolle über die Geräte zu besitzen – für nicht einmal 400 €.[3] Und wer unter den Smartphone-Besitzern jetzt noch keine weichen Knie hat und meint, in den Gigabytes an Songs, Fotos und Filmchen sind seine wenigen interessanten Dokumente doch gut versteckt: Elcomsoft bietet auch gleich die notwendigen Softwarewerkzeuge an, um für ein schnelles Herausziehen der vermutlich interessanten Dokumente die Spreu vom Weizen zu trennen. Auch in der Wirtschaft kommen inzwischen viele Geschäftsprozesse ohne die 'Cloud', ohne Plattformen für das kooperative Arbeiten und ohne Online-Datenbanken gar nicht mehr aus. Das sind hochergiebige Angriffsziele! Wir reichen den Geheimdiensten unsere vertraulichen Informationen quasi auf dem Silbertablett.

Und wenn wir schon bei den Tabletts sind: Smartphones und Tabletcomputer, demnächst auch Smartwatches, ausgestattet mit GPS-Lokalisation, Mikrofon, Camera und Mobilfunkzugang, tragen wir als potentielle Taschenwanzen beständig mit uns herum. Die NSA-Experten sollen, wie aus den von Snowden enthüllten NSA-Dokumenten hervorgeht, gejubelt haben, als die Smartphones den Markt eroberten, und kaum war das erste iPhone erschienen, war es bereits gehackt. Wer etwas die Babyphone-App einschaltet – mit Ton und Bild! – oder die App zum Auffinden des eigenen Telefons, macht sich vermutlich wenig Gedanken darüber, dass dabei u.a. gerade die technischen Eigenschafen dieser Geräte genutzt werden, die die Geräte bestens geeignet zur Ausspähung unserer Intimsphäre und unserer Bewegungsmuster machen. Wer Heizung oder Herd per Smart - phone aus der Ferne steuert, denkt vermutlich kaum daran, dass das heimische IT-Netz durch die dafür notwendigen Öffnungen in seiner Firewall angreifbarer wird.

Es muss aber gar nicht sofort in unsere Geräte und Systeme eingegriffen werden, für eine ‚aktive' Überwachung. Die ‚passive' Überwachung, die Beobachtung des aus den Netzen abgegriffenen Datenverkehrs unserer Mobiltelefone gibt bereits Auskunft über unsere Kommunikationspartner, über unsere Aufenthaltsorte und mehr. Dazu kommen Suchanfragen, Internetkäufe, Finanztransaktionen und Schlüsselwörter in unseren Emails. Allein die Auswertung dieser Metadaten und Datenspuren liefert bereits sehr detaillierte persönliche Profile.

Nun könnte auch der willigste Gesetzgeber uns nicht wirksam schützen, wenn wir alle potenziellen Schutzmaßnahmen durch leichtfertigen Umgang mit unseren Daten unterlaufen würden. Weil wir auf den privaten Komfort nicht verzichten wollen. Weil wir dem wirtschaftlichen Gewinn Priorität einräumen. Weil wir uns den Kommunikationstrends nicht verweigern möchten oder uns einem sozialen Druck schon nicht mehr entziehen können. Seinerseits wird der Gesetzgeber jedoch nicht tätig werden, solange der Willen der Gesellschaft nicht erkennbar wird, durch Veränderung von Verhalten und Konsum ihrerseits einen Beitrag zum Schutz der Privatheit zu leisten.

Unser Ego – im Selbstbetrug bequem eingerichtet?

Und dann ist da noch ein dritter Komplex: unsere Psyche. Was sich in den digitalen Netzen abspielt und dahinter, in den Superrechnern der Geheimdienste, entzieht sich weitgehend unseren

Vorstellungen. "Wir hätten es wissen können, …" schreibt die GI in einem Aufruf an ihre Mitglieder. Aber nicht einmal wir InformatikerInnen und IngenieurInnen haben das Ausmaß und die Tiefe der Ausspähung sehen wollen. Dabei lassen wir uns auf interessante Widersprüchlichkeiten ein: Mit geschickt kombinierten Suchbegriffen lassen wir uns durch Google genau die gerade benötige Information in dem unüberschaubaren Datenuniversum des Internet suchen – und in Sekunden finden. Geht es aber um unsere eigenen Daten, verlassen wir uns gerne auf das Gefühl, „je mehr Daten, desto unwahrscheinlicher, dass zufällige unsere eigenen herausgefischt werden". Und dieser Glaubenssatz ist falsch: Je umfassender die abgegriffenen Daten, desto größer wird sogar die Wahrscheinlichkeit, dass Daten, die mit vorgegebenen Merkmalen und Mustern korrelieren, identifiziert werden – und dass wir durch das Zusammenspiel von Zufällen unbescholten ins Fadenkreuz geraten können. Das widerspricht der Intuition, ist 'counterintuitive', und damit schwer vermittelbar.

So wird dieser Glaubenssatz auch gerne politisch bedient. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, illustrierte dies jüngst in einem SPIEGEL-Beitrag: „[…] bedeutet das Speichern schon Überwachung?" fragt er, und er wiegelt ab, „Ich bin der Überzeugung, dass selbst ein Nachrichtendienst wie die NSA überfordert wäre, wollte sie den gesamten Telekommunikationsverkehr der Deutschen mitlesen und mithören."[4]

Naiv? Nein, bewusst irreführend! Auch Maaßen weiss vermutlich mittlerweile, dass längst nicht mehr Analysten anhand von gegebenen Verdachtsmomenten ermitteln, sondern Big-Data-Tools mit hoch entwickelten Statistikmethoden und komplexen Mustererkennungsverfahren. Der Verdacht wird gleichsam erzeugt, konstruiert, von Automaten! Sie analysieren alle erfassten Daten unmittelbar, suchen nach Korrelationen, stellen Verknüpfungen her, berechnen Gewichtsfaktoren für die Verdächtigkeit aller erfassten Personen. Diese 'scores' hängen z.B. von den 'scores' der Personen ab, mit denen wir kommuniziert haben, und sogar von deren Kommunikationspartnern, die wir nicht einmal kennen müssen. Sie hängen – über unsere Geodaten – von Personen ab, neben denen wir zufällig im Café gesessen haben, von Ländern, die wir bereist haben, von den Suchbegriffen unserer Internetrecherchen.

Wir werden zu gewichteten Punkten in einem Beziehungsnetz, dem so genannten *social graph*, und je enger das Netz, desto ergiebiger wird es. Nachvollziehbar daher die Sammelwut der Dienste. "Mehr ist immer besser […]. Da man Punkte, die man nicht besitzt, nicht verknüpfen kann, versuchen wir grundsätzlich, alles zu sammeln und behalten es für immer," sagt Ira Hunt, Chef-Techniker der CIA. Geheim bleibt, welche Faktoren relevant sind, mit welchen Algorithmen ausgewertet wird, welche Annahmen der 'Verdachtskonstruktion' zu Grunde liegen.

Soweit sprechen wir von 'passiver' Überwachung, die wir nicht spüren, von der wir nicht erfahren – muss sie uns dann überhaupt kümmern? „Ich haben ja nichts zu verbergen", das kann ein fataler Irrtum werden. Denn gezielt nehmen sich die Dienste Personen vor, die von den Automaten ausgesiebt werden, weil ihr 'score' einen Schwellwert überschritten hat. So kann jeder von uns in die 'aktive' Überwachung geraten, ohne sein Wissen, einfach durch die Kombination von dummen Zufälligkeiten – mit ziemlich ungemütlichen Konsequenzen.

Wie ernst wir dieses persönliche Risiko nehmen, ist vielleicht jedes Einzelnen Sache. Ein allgemeines, die Gesellschaft betreffendes Risiko ist jedoch, dass Gleichgültigkeit und Unwissen dazu zu führen droht, dass wir in einen totalen Überwachungsstaat abgleiten. Können wir wirkliche davon aus-

gehen, dass unsere westlichen Demokratien immer stabil genug bleiben, reaktionären Kräften zu widerstehen, sich der Überwachungseinrichtungen als willkommenes Werkzeug für eine Machtergreifung zu bedienen? Selbst wenn wir uns auf ein solches Szenario nicht einlassen wollen, führt nicht, wie Rolf Gößner anlässlich der Verleihung des Berliner Preises für Zivilcourage an Edward Snowden ausführte, bereits das Bewusstsein, überwacht zu werden, über eine allmähliche Änderung des kollektive Verhaltens zu einer unfreien Gesellschaft?

Und dennoch – es gibt Handlungsoptionen!

Was tun? Die Technik muss vor der Übermacht des Angriffspotenzials passen, unsere Regierung will ihre innen- und außenpolitischen Positionen nicht aufgeben, die Gesellschaft will auf das Gewohnte nicht verzichten. Hinzu kommen sozialer Druck und Unverständnis gegenüber den Risiken. Die Hände in den Schoß legen? Veränderung können wir erreichen, aber wir müssen dazu auf allen Ebenen ansetzen, konzertiert – Politik, Gesellschaft, Technik sind gleichermaßen aufgerufen.

Einmischen in die Politik, Kampagnenarbeit für eine gesellschaftliche Bewusstmachung sind zwei unverzichtbare Komponenten. Jedoch, genau wie die Politik sich nicht rühren wird, bevor die Gesellschaft ihren Veränderungswillen demonstriert, so wird sich die Gesellschaft nicht bewegen, ohne dass ihr technische und funktionale Alternativen an die Hand gegeben werden, die akzeptable Kompromisse zwischen dem 'weiter so' und dem Verzicht auf eingespielte Prozeduren und lieb gewonnene Gewohnheiten bieten. Insofern muss Bruce Schneiers vorangestelltes Statement relativiert werden: Auch die Technik muss Beiträge leisten, um Wege zu ihrer demokratischen Gestaltung und Kontrolle zu ebnen, auf mehreren Ebenen:

Offene Systeme sind die Grundlage für Kontrollierbarkeit. Erst wenn der Programmcode von Betriebssystemen und Anwendungsprogrammen offengelegt wird, kann Software wirkungsvoll auf Hintertüren und versteckte Schadfunktionen geprüft werden. Opensource-Software ist mittlerweile etabliert, findet aber immer noch nicht die wünschenswerte breite Akzeptanz. Mit komfortableren Installationspaketen für Betriebssysteme auf gängigen PCs, Notebooks, Tablets und Smartphones könnte die Schwelle zum Umstieg reduziert werden. Besser noch, wenn Aufklärung eine marktrelevante Käuferschicht für Produkte entstehen lässt, die bereits mit einer kompletten Grundausstattung offener Software ausgeliefert werden. Dies gilt nicht nur für den privaten Konsum, sondern ebenso für Unternehmen, die schon aus wirtschaftlichen Erwägungen interessiert sein sollten, Sicherheitsrisiken zu reduzieren.

Wahlmöglichkeiten innerhalb eines Angebots alternativer Dienste sind eine Voraussetzung für eine Abkehr von den derzeitigen monopolistischen sozialen Netzen, Suchmaschinen, Clouds, Appstores. Dass für alternative Dienste bereits heute Bedarf ist, beweist eine Vielzahl kleiner und mittlerer Unternehmen, die Email-Konten, Upload-Speicherplatz, Webhosting etc. anbieten. Wichtig ist die Etablierung öffentlicher Kontrollinstanzen. Es sollte ein von den Kunden eingefordertes Qualitätskriterium werden, dass sich die Unternehmen freiwillig regelmäßigen Sicherheitsaudits unterziehen.

Digitaler Selbstschutz ist eine Sofortmaßnahme. Er sollte so selbstverständlich werden wie das Anbringen eines Sicherheitsschlosses an der Wohnungstür. Auch hier wieder obliegt es der Käufergemeinde, eine Grundausstattung an Mitteln für den digitalen Selbstschutz bereits bei der Auslieferung von Neugeräten zu erwarten (kein Vermieter wird heute eine Wohnung ohne

Türschloss anbieten …). Bis dies erreicht ist, kann mit bereits heute erreichbaren Werkzeugen begonnen werden, wenigstens mit den einfachsten. Auch wenn gegen aktive Ausspähung vermutlich alle uns realistischerweise verfügbaren Mittel versagen, erschweren 'Hausmittel' zumindest die passive Ausspähung. „Macht es den Geheimdiensten schwer, verdunkelt das Netz!", ist die Parole der Initiative „Reset the Net", die dazu eine Grundausstattung an einfach zu handhabenden Schutzfunktionen anbietet.[5] Aufwändiger, aber auch wirkungsvoller ist die Email-Verschlüsslung. Erforderlich ist jedoch die Installation der Verschlüsslungssoftware auf *beiden* Seiten der Kommunikation. Für Verbreitung muss daher geworben werden. Dazu müssen Installation und Handhabung mit guten Anleitungen leicht gemacht werden. Einen hilfreichen Beitrag dazu leistete nun, gerade ein Jahr nach Snowdens Enthüllungen, die *Free Software Foundation.*[6]

Wir haben es in der Hand …

Es läge an den Bürgern selbst, Überwachung zu stoppen, schrieb Edward Snowden. Und dies sei mithilfe der Naturgesetze einfacher als mit staatlichen Gesetzen. Letztlich hat die Gesellschaft den Schlüssel für eine Veränderung in der Hand. Loslösen müssen wir uns von der verführerischen Annehmlichkeit des scheinbaren Umsonst von Internetdienstleistungen und -werkzeugen. Sicherheit kostet. Und auch ein Stück Komfort müssen wir bereit sein aufzugeben. Denn, so schreibt Ulrike Meyer, Professorin für IT-Sicherheitsforschung an der RWTH Aachen, „Sicherheit kostet oft auch die Benutzerfreundlichkeit eines Programms." Die erforderlichen neuen Produkte werden eine Herausforderung an die Wirtschaft sein. Und so wird vermutlich schneller als die Politik der Markt reagieren, sobald sich eine sicherheitsbewusste Käuferschicht etabliert. Der politische Einfluss der betroffenen Wirtschaft wird dafür sorgen, dass die Politik nachzieht. Aber beginnen müssen *wir*!

Selbst tätig zu werden, andere dazu zu ermutigen, zu unterstützen – das hat mindestens zwei Effekte über den konkreten Nutzen hinaus: Wir erfahren Technik und ihre Mechanismen, wir holen die Technik ein Stück heraus aus ihrer Abstraktheit. Und uns wird bewusst, dass wir uns ein Stück Freiheit zurück erobern. Denn „beobachtet werden macht unfrei", sagt uns Glenn Greenwald.

Erweiterte Fassung eines Vortrag auf dem 3. Gustav-Heinemann-Forum der Humanistischen Union, Rastatt, 20./21.06.2014, "Weltweite Kommunikationsüberwachung: Rechtliche Bewertung & politische Handlungsoptionen". Zur Veröffentlichung in *vorgänge*, Hrsg. Humanistische Union e.V.

---

1 Bruce Schneier, US-amerikanischer Experte für Computersicherheit, Vorwort seines Buches "Secrets and Lies", 2000

2 „Ihr braucht einen Snowden aus dem BND!", Thomas Drake, Interview in FR 10.06.2014

3 Elcomsoft Phone Password Breaker, *http://www.elcomsoft.de/eppb.html*

4 DER SPIEGEL 14/2014, *http://www.spiegel.de/spiegel/print/d-126267966.html*

5 Initiator der Kampagne war Fred Barlow, Mitbegründer der Electronic Frontier Foundation, *http://resetthenet.org*

6 Inzwischen ist unter Mitwirkung des *FIfF* auch eine deutsche Fassung der Anleitung der FSF für die Installation und Handhabung der (freien!) GnuPG-Software für das heute standardmäßig verwendete PGP-Verfahren verfügbar, *https://emailselfdefense.fsf.org/de/*