Freiheit und Sicherheit –
Die Ambivalenz des Internets

Christoph Kappes

www.christophkappes.de

Vortrag

6. November 2012, IHC OWL, Bielefeld

Inhalt

Sehr geehrte Damen und Herren,

„Freiheit und Sicherheit - die Ambivalenz des Internets“, das ist ein furchtbar langweiliger Titel für einen Vortrag. Wenn etwas „ambivalent“ ist, dann hat es also gute und schlechte Seiten wie das berühmte zweiseitige Schwert, da kann man es sich einfach machen und ein paar gute und ein paar schlechte Punkte aufzählen. Genauso fange ich auch an. Aber danach will ich versuchen, ein paar Gedanken zu Technik und Freiheit generell zu sagen, bevor ich zu den Spezifika des Internets komme, und zwar erst zu den typischen Gefahren und sodann zu den typischen Taktiken zur Lösung.

Teil 1: Ein Internet – zwei Sichten

I. Freiheitsgefährdende Phänomene (Die negative Sicht)

Am einfachsten ist die Rolle des Warners über das Internet: Es sind seit Jahren vielerlei Straftaten zu beklagen, von Betrug bis Kinderpornographie, die nicht nur ohne, sondern auch mit dem Internet in irgendeiner Weise begangen werden, dass lässt sich nicht leugnen. (1) Für 2011 weist die amtliche Kriminalstatistik des BKA[1] das Internet in über 200.000 Fällen als Tatmittel aus, in vielen Tabellen ausgebreitet und nach Straftaten und Regionen sortiert. Im engeren Bereich „Cybercrime“ (das sind Computerbetrug, Daten-Ausspähung, Datenfälschung etc.) waren es 60.000 nachgewiesene Straftaten mit wirtschaftlichem Schaden von über 70 Mio. EUR. (2) Zu viel höherer Kriminalität kommen alljährlich in schöner Regelmäßigkeit die Anbieter von Sicherheitssoftware, zum Beispiel schreibt der Hersteller Norton in seinem „Cybercrime Report“ von 15 Millionen Opfern und einem Schaden von 2,83 Mrd. EUR, also gemittelt rund 50 EUR je Online-Nutzer[2]. Diese Studien zählen allerdings auch jeden Virus mit, jeden angeklickten Link auf Viren und Malware und auch täuschende SMS, auf die geantwortet wurde. (3) Hinzu kommt eine hohe Dunkelziffer, neben den o.g. Delikten vor allem Ehrverletzungen, die täglich massenhaft online begangen werden, sowie Gefährdungen unterhalb der Strafbarkeitsgrenze, zum Beispiel straffreie Fälle von Cybermobbing und soziale Desaster wie Facebook-Partys.

Und dann wären da noch Warnungen, die Sie aus den Feuilletons schon kennen. Erstens vor „Information Overload“ (ich nenne das „Informationsüberschwemmung“). Zweitens vor einer digitalen Spaltung unserer Gesellschaft zwischen verschiedenen Menschengruppen: außer denen, die das Internet gekonnt mit Medienkompetenz nutzen, gibt es auch Menschen, die gar keinen Zugang haben, und Menschen, die sich auch mit Zugang eher noch ausgrenzen. Drittens sind da Warnungen vor digitaler Demenz, vor dem Verlust von echten Beziehungen, vor dem Ausblenden relevanter Information durch falsche Informationsfilter, vor dem Verlust der Privatheit und vor der Macht der Algorithmen.

Diese Phänomene, wenn sie denn so existieren (einige halte ich für Behauptungen, die auf Denkfehlern beruhen), beeinträchtigen alle unsere Freiheit in irgendeiner Weise: Wer zum Beispiel keinen Zugang zum Internet hat, kann diese Art von Freiheit nicht leben. Wer falsche Filter setzt, engt seine Entscheidungsfreiheit selbst ein, ohne es zu merken. Wer die Privatheit aufgibt, und sei es

[1] http://www.bka.de/nn_231576/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2011,templateId=raw,property=publicationFile.pdf/cybercrime2011.pdf

[2] http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

versehentlich, kann sich erpressbar machen oder setzt sich – das ist gerade für Minderheiten immer wieder wichtig - sozialem Druck aus, der ihm Freiheit nimmt. Und schließlich ist gar kein „böses“ Verhalten Dritter nötig, sondern es ist schon problematisch, wenn wir private Daten abgeben und dann nicht wissen, ob und wie Dritte ihre Handlungen mit diesem Wissen ableiten. Wir diskutieren das gern vordergründig unter dem Stichwort „Datenschutz“ bei Google und Facebook, das eigentlichem dahinterliegende Problem ist aber: wir verlieren dann unsere Autonomie.

Zum problematisierenden Standpunkt gehört auch, dass immer mehr Handlungen und Äußerungen der Bürger durch das bzw. im Internet geschehen und dadurch Bürger für staatliche Organe immer besser überwachbar werden. Dieses Gefährdungsmuster „staatliche Überwachung“ wird seit der Rasterfahndung diskutiert, führte vor 30 Jahren zum Recht auf informationelle Selbstbestimmung und war auch dieses Jahr beim sog. „Staatstrojaner“ wieder Thema. In diesen Abzweig der Diskussion gehören leider auch Datensammlungen durch Private, weil sie für Staaten attraktiv sind. Besonders kritisch wird die Situation in totalitären Staaten, die auf beiden Wegen in die private Sphäre eindringen. Russland zwingt seit letzten Donnerstag die russischen Internetprovider zu Netzsperren und zu Filtertechniken, die jedes einzelne Datenpaket in Echtzeit analysieren und in Kopie Polizei und Geheimdiensten zur Verfügung stellen. Spiegel Online bezeichnet das zu recht als *Totalüberwachung im Internet*[3].

Ich denke, es ist recht einfach, alle diese Phänomene von Cybercrime, Informationsüberschwemmung etc. und staatlichen Eingriffen im Lichte von „Freiheit“ als irgendwie problematisch anzusehen.

II. Freiheitsfördernde Phänomene (Positiver Gegenstandpunkt)

Man kann auch den gegenteiligen Standpunkt annehmen und sagen: Kriminalität hat es immer gegeben, sie ist soziale Realität; Das Internet ist Teil der Realität, so daß es sehr folgerichtig ist, wenn es von Menschen auch zu kriminellen Zwecken erobert wird wie der Rest der Welt. Man muss die Kriminalität auch hier verfolgen und zurückdrängen, aber zunächst mal sollten wir uns freuen über die Chancen, sagen die Protagonisten. Über diese Chancen kann man großartige Reden halten. Hillary Clinton hat das beispielsweise getan, indem sie in Reden[4] das Internet als freiheitssichernde Infrastruktur betont, es in den Kontext von Menschenrechten stellt und indem Sie von „wahrem Fortschritt“ spricht, in dem jeder Mensch seine gottgegebenen Möglichkeiten ausschöpfen könne. Und es stimmt: Ich bin hin und wieder Podiumsteilnehmer bei politischen Stiftungen und habe dort immer wieder mit Oppositionellen zu tun, die persönlich bezeugen, dass sie Öffentlichkeit erreichen, wo totalitäre Regimes Desinformation und Informationsunterdrückung betreiben; und das betrifft Öffentlichkeit nach Innen und Außen (ins Ausland), aber auch noch einige andere Vorteile wie zum Beispiel den, sich mit Online-Mitteln besser organisieren zu können. In Ägypten, Tunesien, Syrien ist das Internet zusammen mit anderen Kommunikationsmitteln eine furiose Waffe gegen Unterdrückung, wenngleich es auch überzogen ist, gleich von „Facebook-Revolution“ zu sprechen und Geheimdienste natürlich den Spieß längst umgedreht haben und Facebook nutzen, um Bürgerrechtler zu identifizieren.

Ja, wenn man die Frage grösser formuliert, weg von einer antitotalitären Sicht mehr zu einer Vision der „freieren Gesellschaft“, könnte man sogar ein begeisterter Prediger werden, für den das Internet uns allen endlich Erlösung bringen wird: ein herrschaftsfreier Diskurs im Habermas´schen Sinne könnte möglich werden, Information als wichtigste Gut der modernen Gesellschaft stünde jeder-

[3] http://www.spiegel.de/netzwelt/web/internetzensur-russland-startet-schwarze-liste-fuer-websites-a-864903.html, weiterführend http://uncut.indexoncensorship.org/2012/10/russia-web-censorship-report/
[4] http://www.state.gov/secretary/rm/2010/01/135519.htm, http://www.state.gov/secretary/rm/2011/02/156619.htm

mann zur Verfügung (und das zu Null Grenzkosten), jeder könnte ein Massenmedium sein und alle wären formal gleich in ihrer Eigenschaft als Sender. Politik würde aus den Hinterzimmern herauskommen, transparent werden und Partizipation vieler Bürger als zentrales Merkmal einer gelebten Demokratie möglich.

Solche Hoffnungen finden sich auch heute immer wieder, und sie gab es schon in der Ursuppe des Internets, den bärtigen libertären Computerwissenschaftlern Kaliforniens, die gemeinsam und friedlich auf Staatskosten an Software bastelten, mit denen heute Ihr Handy von Apple, Blackberry oder mit Android arbeitet (vor allem die Programmiersprache C und Betriebssystem UNIX sind hier zu nennen). Diese Kultur des gemeinsamen Arbeitens an etwas, das für alle da ist, erinnert stark an den Umgang mit der Gemeinschaftswiese im frühen Mittelalter (die Allmende) und führt in eine hochaktuelle Diskussion um Gemeingüter als ergänzende Wirtschaftsform zur Marktwirtschaft. Auch ihre Kultur des offenen, für jedermann lesbaren Codes ist direkt mit der heutigen Urheberrechtsdiskussion verbunden. Die Computergeschichte zeigt nämlich wie die ganze übrige Technikgeschichte auch, dass wir nur selten Ideen aus dem Nichts schöpfen, sondern alle auf Riesen stehen, wie Isaac Newton einmal gesagt hat, *standing on the shoulders of giants*: Apple, die wertvollste Firma der Welt, baut auf dieser Software der Bärtigen auf, wie diese alle auf den Ergebnissen von Konrad Zuse, Charles Babbage, Lady Ada Lovelace, Blaise Pascal & Wilhelm Schickard aufbauen, die auf den Schultern von Leibniz usw. stehen.

Alle diese Phänomene lassen sich also auch irgendwie als freiheitsfördernd lesen. Da sind Bürger als Diskursteilnehmer freier als je zuvor von wirtschaftlichen Zwängen; mit Google Hangout kann heute jeder Fernsehsender sein, und das ist viel leichter als Stattzeitungen der 70er und Offene Kanäle der 80er – was für ein Fortschritt! Da erscheint Partizipation im Lichte einer nicht mehr nur statuarischen Freiheit, sondern diese Freiheit kann gelebt werden, indem man auf verschiedene Weise vor, bei und nach Entscheidungen mitwirkt. Und an den Gemeingütern, wo man teilhat an einem gemeinsamen Prozess der Wissensentwicklung, sieht man, dass Wissen sowohl eine Ressource ist, die durch Freiheit ermöglicht wird, als auch das Resultat von Freiheit ist. Wikipedia lebt dank Freiheit und sie erzeugt welche.

„Information will frei sein“, sagt ja sogar eine kleine Gruppe Technolibertärer. Das geht zurück auf Steward Brand[5] 1984, wobei der damit eher den Preis meinte als den Zugang, weil Information zu verbreiten praktisch nichts kostet. Diese Idee kam wenig später in ähnlicher Weise bei den sog. Krypto-Anarchisten[6] auf, die durch Verschlüsselung aller Kommunikation eine Kommunikation der Bürger untereinander ermöglichen wollten, die dem Staat entzogen ist. Und heute finden Sie beispielweise unter dem Begriff „DataLove“ ein Mantra, das ich wörtlich zitieren möchte: „*Love Data / Data is essential / The data must flow / data must be used / Data is neither good or bad /…/ Data is free / Data can not be owned / No man, machine or system shall interrupt the flow of data / Locking data is a crime against datanity*“[7]. Dieses Mantra ist von einer kleinen Gruppe Internet-Aktivisten namens Telecomix aus dem Jahre 2009. Ihr Slogan wurde gleich gekapert von der wichtigsten deutschen kommerziellen Online-Konferenz, der Next in Berlin, deren Motto 2011 auch „DataLove“ war. Hier geschieht also zweierlei: Daten werden als Träger von Freiheitsrechte proklamiert und Daten sind ein Objekt der Libido. Ob das wirklich die Speerspitze einer Internetavantgarde ist, sei dahingestellt, auf jeden Fall zeigt dieses Beispiel, wie stark Internet emotional mit Freiheit aufgeladen wird.

[5] http://en.wikipedia.org/wiki/Information_wants_to_be_free
[6] Guter Einstieg hier http://www.sueddeutsche.de/digital/wikileaks-gruender-julian-assange-der-gegenverschwoerer-1.1031477
[7] Deutsche Version irgendwo im Internet, bitte selbst suchen.

Da mag ein Übriges tun, dass uns mit „freiem WLAN“, „freiem Zugang“ und „offenen Standards“ wir auch mit unserer Sprache eine solche Assoziation provozieren. „Das freie Internet“ wird es manchmal auch genannt, da ist es auch sprachlich nicht weit zum Internet als Freiheitsinstrument, obwohl die Begriffe anderes meinen.

Teil 2: Technik und Freiheit

Meine Damen und Herren, ich habe große Schwierigkeiten mit beiden Standpunkten, obwohl ich – anders als vermutlich die meisten von Ihnen – beruflich vom Fach bin und Netzdiskussionen sehr genau verfolge. Warum habe ich Schwierigkeiten? Weil die Perspektive falsch ist.

I. Technik schafft Freiheit durch Optionen

Der Begriff „Freiheit“ steht in gar keinem klaren Zusammenhang zum „Internet“. Es sind zwei Wörter, die wir in Beziehung setzen müssen. Sie stehen da ohne Beziehung zueinander wie Freiheit und Auto, Freiheit und Anti-Babypille, Freiheit und Pistole (...) - Sie merken, wie unser Gehirn sofort kleine Geschichten erfindet, obwohl ich gar keine These aufgestellt habe. So auf diesem Niveau ist die öffentliche Debatte. Stellt man die Frage ganz präzise: „Fördert das Internet die Freiheit?“ wird es erst richtig interessant. Denn offenbar handelt es sich um einen Vergleich zweier Zustände, den mit und den ohne Internet. Und da sind wir schnell mitten in der Technikphilosophie: Jedes Werkzeug, dass Menschen erfinden, schafft zunächst neue Möglichkeiten und erweitert insofern unsere Freiheit. Ich muss, seit es das Auto gibt, nicht mehr zu Fuss gehen, Fahrrad fahren, eine Pferdekutsche benutzen – jede Technik schafft neue Optionen. Den Vergleich mit dem alten Zustand „prä Internet“ einfach wegzulassen ist übrigens ein grober Fehler vieler Internet-Thesen, zum Beispiel blendet die Theorie von der Filter-Bubble einfach aus, dass sowohl alte Medien weiter existieren, als auch, dass ich im Internet nicht auf Filtertechnik angewiesen bin, sondern immer auch direkt auf die Quelle zugreifen kann; ich habe also den Filter *zusätzlich* zum Ungefilterten. Sogar der „Information Overload“ ist nur eine Option, die ich gewählt habe. Das ist die eine Seite der Technik, sie schafft neue Optionen. Marshall MacLuhan, der große Medientheoretiker, ordnet denn auch die Medien als „Extensions of Man“[8] ein, auch das Internet würde man heute hier einreihen.

II. Technik ist Grundlage neuen sozialen Zwangs

Die andere Seite ist, dass sie uns mit ihrer Existenz auch Handlungsmöglichkeiten nimmt. Einen Frankfurter Bankentower bis in die zwanzigste Etage zu Fuß zu erklimmen, ist nur eine rein theoretische Option. Die Praxis ist, dass unser soziales Umfeld und auch unser eigener Plan uns diese Option nicht lässt. Wir planen unsere Zeiten, indem wir Fahrstuhlbenutzung und nicht Treppensteigen planen, und Flugzeugbenutzung statt sehr langer Fußwege. Wir schreiben auch geschäftlich kaum noch Briefe, sondern nutzen E-Mail. Wir fotografieren mit der DigiCam und kaum noch analog. Wir gucken auf die Uhr und nicht nach dem Stand der Sonne. So gibt es viele Dinge, ich anders mache als mein Großvater. Ich habe viel von ihm gelernt, aber wie ich die Uhrzeit mit der Sonne erkennen kann, habe ich mir als Kind schon nicht gemerkt, genauso wenig wie die Bedienung seines Rechenschiebers. Genauso ist es mit dem Internet: wie jede neue Technik kann es sozialer Standard werden, und zwar für den einen Nutzungszweck mehr, für den anderen weniger. Neuer Standard wird neue Technik vor allem dann, wenn ihre Nutzung effizienter ist als die Nutzung ihrer Vorgänger. Dadurch kann sich Freiheit schnell in Zwang verwandeln: Wir kennen dies von der Erwartung ständiger Erreichbarkeit, seitdem es Handys gibt. Und wir können richtig wütend werden, wenn das Auto nicht anspringt, die

[8] http://en.wikipedia.org/wiki/Understanding_Media:_The_Extensions_of_Man

Plastiktüte reißt, der Computer abstürzt. Denn Alternativen bestehen zwar, wir könnten ja zu Fuß gehen; das ist aber in praxi keine Option, weil wir die zusätzliche Zeit dafür nicht geplant haben und uns darauf eingestellt haben, den Kofferraum zu benutzen. Es ist paradox: dieselbe Technik, die uns Freiheit gibt, nimmt sie uns auch wieder. Oder besser: nicht die Technik, wir selbst nehmen uns die Freiheit.

Unsere Massenmedien schreiben zwar täglich Überschriften wie „*E-Mail-Terror – Nur Sklaven sind ständig erreichbar*" (eine aktuelle Überschrift bei Spiegel Online), die vermeintliche Ambivalenz der Technik ist aber kein Internetproblem, sondern Ergebnis der Ambivalenz des Menschen. Der Mensch in der Moderne ist auf Technik angewiesen, und er muss sich ohne sie – das ist auch die Geschichte von Robinson Crusoe - alte Technik aneignen, die er nie gelernt hat. Wie zum Beispiel sollte ich überleben, wenn man mich in der Wildnis aussetzt? Das könnte schief gehen, weil ich verhungere.

Noch mehr: Ich als Städter und Internetmensch fühle mich frei, wo keine Technik ist, wo „nichts" ist, nur Natur. Sollte ich endlich ein Wochenendhaus haben, dann wird es richtig paradox, denn ich freue mich auf das Gärtnern, das Hüttenbauen und das Bäumefällen – also all das, wovon sich der Moderne Mensch ja zu befreien glaubte. Für mich ist Freiheit der Zustand, von dem sich mein Großvater befreit hat. Mein Zustand unterscheidet sich nur subjektiv von seinem, denn wir täten ja objektiv das gleiche, empfänden es nur anders. Wenn es mit dem Gemüsegarten nicht klappt, geh ich halt schön Essen, vom Waldhaus per Handy mit Opentable gebucht, per Kreditkarte bezahlt und mit Navi gefahren. So wird dann Freiheit ein ganz subjektives Gefühl, das nur davon abhängt, ob Technik mich befreien könnte, wenn ich wollte. Ganz pointiert: Wenn ich keine Technik nutze, aber alle sofort haben könnte, bin ich frei.

Mir kommt dabei auch ein Zitat aus Frischs *Homo Faber* in den Sinn. Da sagt Hanna: „*Technik als Kniff, die Welt so einzurichten, dass wir sie nicht erleben müssen.*" Und „*Technik als Kniff, die Welt als Widerstand aus der Welt zu schaffen, beispielsweise durch Tempo zu verdünnen, damit wir sie nicht erleben müssen."* Und Faber notiert dazu: „*Was Hanna damit meint, weiß ich nicht*.". Dieser Fall ist kein sozialer Zwang, aber hier zwingt sich jemand selbst zur Technik, und wenn ich Max Frisch hier richtig verstehe, weil seine Figur Faber Angst vor Emotion und Nähe hat. *(Übrigens ist dieses Buch, das uns den kalten Ingenieur vorführt, der am Ende reuig ist, eine der Wurzeln deutscher Anti-Technik-Haltung.)*

Ein Bekannter von mir, mit dem ich das Thema diskutierte, schrieb letzte Woche den Satz: *Die Unfreiheit beginnt innen*. Ich möchte das hier nicht entscheiden, aber will darauf hinweisen, dass wir uns in einen uralten philosophischen Streit begeben. Bestimmt das Sein das Bewusstsein, weil uns die tatsächlichen Verhältnisse gar keine Wahl lassen, oder ist das Bewusstsein vom Bewusstsein bestimmt? Marx oder Buddha, um es ketzerisch auszudrücken? Als Pragmatiker sage ich: das ist beides richtig und oberhalb von, sagen wir, 1.000 EUR netto pro Person im Monat eine Bewusstseinsfrage. Vielleicht ist so eine ähnliche Erkenntnis auch ein Grund für zwei Positionen der Piratenpartei, die sich scheinbar wenig vertragen: eine liberale Haltung und ein Bedingungsloses Grundeinkommen (BGE) für alle. Sie vertragen sich nämlich doch, weil von einem klar liberalen Standpunkt (und ich sage nicht: wirtschaftlichen Standpunkt) aus Freiheit nur geringem sozialen oder wirtschaflichen Zwang möglich ist, weil man sonst gar keine Optionen hat, zwischen denen zu wählen man frei sein könnte.

Noch eine letzte Anmerkung. Vielfach wird auch behauptet, dass neue, komplexere Technik mit Wissensmonopolen einhergeht, und das halte ich auch für zutreffend, zum Beispiel bei modernsten Software-Architekturen, und anspruchsvollen (z.B. selbstlernenden) Algorithmen – und Sie kennen

das Thema auch durch die vielen kritische Pressebeiträge zu Google, das ist ein brandaktuelles Thema. Hier entsteht durch Wissensdifferenzen ein potentielles Machtgefälle und hierdurch eine Bedrohung von Freiheit. Das wird im Falle des Internets auch nicht dadurch gemindert, dass durch das Internet viel mehr Wissen als bisher zugänglich wird. Es finden vielmehr zwei Effekte parallel statt: ein gehobenes Wissensniveau wird für jedermann verfügbar und das höchste bleibt wenigen vorbehalten.

Allerdings meine ich, dass das Wissen um die Technologie nicht einseitig Ursache für ein Machtgefälle ist, sondern umgekehrt Machtgefälle solche Wissensdifferenzen auch erzeugen. Wer also etwa die Ressourcen für Forschung einsetzt, erhält exklusive Resultate. Wir dürfen nicht vergessen, dass das politisch gewollt ist, das ist unter anderem Konsequenz des Patentrechts. Der Ausgleich muss auf politischer Ebene gefunden werden, durch Wettbewerb, durch Regulierung und durch Ablauf von Schutzfristen.

III. Technische Entwicklung ist Evolution

Wir haben gesehen: Nutzung bestimmter Technik kann zum sozialen Standard werden. Dadurch kommt noch eine weitere Dimension ans Licht. Haben wir zum Beispiel noch die Wahl, ob wir Facebook als Paradebeispiel eines „sozialen Netzwerks“ nutzen oder nicht? Datenschützer Weichert hat gerade vor zwei Wochen wieder gesagt: Natürlich besteht kein Nutzungszwang, auch kein faktischer[9]. Ich selbst zum Beispiel habe mich vor zwei Jahren mit lautem Getöse aus Protest bei Facebook abgemeldet aber ich bin dann nach drei Monaten sehr leise wieder zurückgekehrt. Was war der Grund? Mein Umfeld hat mir immer wieder Links geschickt, die ich nur auf Facebook sehen konnte. Warum gibt es diesen Sog? Weil Facebook die effizienteste Kommunikationsform ist, um Links auszutauschen, E-Mail wäre einfach umständlicher für alle Beteiligten. Ganz allgemein gesprochen: Online-Kommunikation ist effizient, und zwar unabhängig davon, wie wertvoll nun der Inhalt ist. Die Sogwirkung entsteht, weil Kommunikationsaufwand sinkt. Man kann mit ein paar Klicks mehr Kontakte mit schwachen Bindungen pflegen, und das in Pausen, Leerlaufzeiten, zwischendurch. Genauso ist es mit Twitter: Es gibt kein Medium mit derart hohem Datendurchsatz, das man nebenbei benutzen kann - in der U-Bahn, in der Pause, wartend im Café. Die Nutzungseffizienz[10] entscheidet darüber, was sich was sich durchsetzt.

Die Erkenntnis ist, dass wir als Gattung aller Menschen nicht die Wahl haben, ob wir das, was wir tun, auch lassen könnten. Zwar hat der Einzelne die Wahl, für die Menschheit zeigt aber die ganze Geschichte des technischen Fortschrittes in eine andere Richtung: der Mensch baut seit Jahrtausenden anspruchsvollere Werkzeuge, um sich das Leben zu erleichtern. Ob es Hochhäuser, industrielle Fertigung oder Nahrungsmittelproduktion sind: wir senken seit Jahrtausenden Kosten und erhöhen Vielfalt. Und wo es Fehlentwicklungen gab, wurden sie bald abgelöst, beispielsweise Hochhäuser, die zu ihrer damaligen Zeit ein Fortschritt waren, dann aber verschwanden. Das ist bei jedem Werkzeug so. Es gibt dazu eine Extremposition von Leuten wie Kevin Kelly, einen der Gründer der Zeitschrift Wired, der daran glaubt, dass sich alle Technik wie ein Organismus evolutionär entwickelt[11], das Technium. Solche und moderatere Thesen werden von vielen vertreten. Die Frage ist immer: steuert der Mensch die Technik oder die Technik den Menschen, wie sind die Zusammenhänge? Nehmen Sie bitte als Anregung die Frage mit: Sind wir Menschen wirklich frei darin, uns zu entwickeln? Unter-

[9] Thilo Weichert gemäß Tweet
[10] Damit ist gemeint, wie ein Ziel mit minimalem Aufwand erreicht werden kann. Meines Erachtens der Grund, warum sich unberechtigtes Kopieren nicht eindämmen lässt, weil die Täter völlig rational handeln.
[11] http://en.wikipedia.org/wiki/What_Technology_Wants

scheidet uns das Zweckhafte, Zielgerichtete in einer mittlerweile ungeheuren Komplexität nicht von allen anderen Lebewesen? Ich glaube: Ja, das macht uns aus, das kennzeichnet unsere Kultur.

Die Frage nach „Freiheit oder Sicherheit" stellt sich also gar nicht hinsichtlich dessen, *ob* wir Technik einsetzen, weil sie eine Wahl suggeriert, die wir als Gesellschaft gar nicht haben. Auch die Politik hat diese Wahlfreiheit nicht, weil sie Teil des ganzen Prozesses ist. Ihr Repertoire ist beschränkt, ihre Eingriffsmöglichkeiten gering, ihr Wirken langfristig, denken Sie nur an das Dauerthema Straßenverkehr. Politiker und Juristen hören das nicht gern - und ich auch nicht, denn es wird nach so einer Erkenntnis schwierig, überhaupt Forderungen aufzustellen, weil es gar keine konkreten Empfänger gibt.

IV. Mensch und Maschine als soziotechnisches System

Jetzt werden manche sagen: wieder so ein Technikoptimist. Nein, ganz falsch, sage ich dann, ich bin kein Technikoptimist, sondern Menschoptimist. Wie das?

Die Vorstellung, hier sei der Mensch und dort die Technik, der man positiv oder negativ gegenüber eingestellt sein könnte, ist häufig anzutreffen, aber recht naiv. Technik, das sind zunächst nicht allein Metallhämmer und Maschinen, sondern Technik ist all das, was wir entwickeln, um Ziele zu erreichen. Technik umfasst also auch Prozesse und Verfahren und sie muss nicht einmal mit Werkzeugen stattfinden, weil wir ja Hände haben (Zähltechnik) oder eine Stimme (Stimmtechnik).

Bei einem weiten Kulturbegriff (als Gegenbegriff zur Natur) ist auch Technik Teil von Kultur, es gibt keinen Antagonismus zwischen beiden - daher gründet das Internet einen Kulturraum, und es ist ein Kulturwerkzeug! Was wir entwickeln, ist nie von uns zu trennen: Der Hammer, Prototyp des Werkzeugs, ist nur ein Stück aus Holz und Eisen, das erst zum Werkzeug wird, wenn wir den Menschen mit hinzudenken, der den Hammer nutzt. Und der Hammer wiederum war nicht einfach so „da", sondern ist die Verwirklichung, die Verkörperlichung einer Handlung. Im Hammer ist das Hämmern für uns enthalten; das zeigt uns sein Anblick so klar, dass wir beides, Werkzeug und Handeln, gedanklich gar nicht mehr trennen können.[12]

Ich will am Beispiel von Software zeigen, welche Zusammenhänge zwischen Mensch und Technik bestehen:

(1) Bevor Software in die Welt kommt, muss sie der Programmierer gedacht haben.[13] Er hat im Kopf ein Modell davon, was sein soll, zum Beispiel eine Rechenoperation, eine Anlagensteuerung, einen Workflow. Software ist die Ver-Wirklichung dieses Modells, zum Beispiel bildet sie soziale Modelle ab, wie in Organisationen zusammenzuarbeiten ist. Ganz klar wird das, wenn SAP Ihnen *Best Practice* verkauft: es ist die Praxis anderer Unternehmen, die in ein Modell gegossen wird.
(2) Umgekehrt wirkt Software auch auf ihr Umfeld, in dem sie eingesetzt wird. Durch Software gewinnen manche Menschen Fertigkeiten (manche fühlen sich geradezu gottgleich oben am

[12] Drittens: Der menschliche Kulturprozess der Weiterentwicklung von Technik setzt voraus, dass Wissen zwischen Generationen weiter getragen wird. Dieser Prozess hat nun eine neue Stufe erreicht, denn nun konservieren Computer unsere Kultur und dokumentieren jeden noch so abseitigen Ausdruck bis in alle Ewigkeit. Wahrscheinlich fördert das Internet auf diese Weise die Entwicklung der Technik.

[13] Eine solche Formulierung scheint unproblematisch, ist sie aber bei genauem Hinsehen nicht. Denn gerade nach dem zuvor gesagten bilden Software und Gehirn eine Einheit: das psychische System (-> Gehirn) steuert Bewegungen für Symbolerzeugung (auf -> Monitor) und verarbeitet dann diese Symbole wieder. Hier ist der Mensch mit seiner Maschine der *Computer*.

Dashboard), durch Software verlieren Menschen Fertigkeiten (z.B. Kopfrechnen und Navigation). Und Software verändert soziale Gefüge. Das ist ja sogar ein Hauptzweck bei Facebook, dass Menschen mehr Kontakte aktivieren – wobei Facebook leider höchst naiv die „Beziehung“ vorgibt, obwohl es vielfältigere Facetten gäbe. Das Paradebeispiel ist, wie „Es ist kompliziert“-Schalter natürlich auch dadurch wieder Beziehungen verändert. Auch Organisationen ändern sich, sie sind ja auch eine Form sozialer Gefüge. Deren Veränderung, vor allem ihrer Prozesse, ist meistens ja auch das eigentliche Ziel.

(3) Software bestimmt Konzepte der nächsten Software in unseren Köpfen, da ist also eine Rückkoppelung.

Ich glaube: für viele Fragen ist es nicht richtig, das Werkzeug, die Software, das Internet als etwas vom Menschen getrenntes zu betrachten. Beide bilden eine soziotechnische Einheit, wie einige Techniksoziologen sagen. Ein soziales und ein technisches *Sub*system beziehen sich aufeinander. Das klingt vielleicht etwas weltfremd, aber im Grunde machen wir das gleiche, wenn wir einen Kommunikationsakt festmachen, wenn jemand einen Satz auf Papier schreibt: Die Handlung und die Schrift auf dem Papier empfinden wir auch als zusammengehörigen Akt.

Ein anderes Beispiel: die ethischen Grenzen von Kampfrobotern sind momentan ein heißes Eisen. Manche fragen, ob es nicht „humaner“ sei, dass bald Roboter gegen Roboter kämpfen, andere finden genau das pervers. Ich glaube nun, dass die Vorstellung von einem „Krieg der Roboter gegen Roboter“ nur vordergründig richtig ist. Die Akteure sind nämlich nach wie vor Menschen, die miteinander Krieg führen, auch wenn sie dabei Roboter benutzen. Für ein moralisches Urteil, für Zurechnung und Verantwortung kann ich nur Lebewesen als Akteure gelten lassen. (Das Konzept „Verantwortung“ macht bei Maschinen keinen Sinn, solange ich Ihnen keine Handlungsfreiheit zugestehe, wonach sie allein haften könnten. Was viele Menschen „Roboterethik“ nennen, kann also nur eine Ethik für Menschen sein und keine Ethik für Roboter. Obwohl der Code im Roboter ausgeführt wird, kann er nicht handelndes Subjekt sein.)

Da Menschen verantwortlich sind, gibt es also keinen „Technikoptimismus“ oder „Technikpessimismus“, es gibt nur „Menschoptimismus“ oder „Menschpessimismus“! Gern spielt uns die menschliche Psyche ersteres vor, weil sie die Verantwortung von uns Menschen auf die Technik leiten will. Das ist geschickt von der Psyche, aber falsch.

Zwischenergebnis:

(1) Nicht das Werkzeug „Internet“ ist zu beurteilen, sondern Menschen, die mit ihm jeweils handelnd eine Einheit bilden. Und zwar mitsamt den sozialen Normen, Prozessen und Institutionen, die dazu gehören.
(2) Viele Menschen bilden in sehr unterschiedlichen Zusammenhängen solche soziotechnischen Einheiten mit dem Internet. Das Internet ist nur *eines* auf einer gegenständlichen Betrachtungsebene, wie unser Straßennetz, dass natürlich auch jede Straße mit jeder verbindet. Eigentlich zerfällt das Internet in viele solcher Einheiten, die wir getrennt betrachten können, je nachdem, wer was benutzt.

Eine Nagelprobe: Bei Google lesen Computer unsere E-Mails mit, bei Facebook gilt das ebenso für Pinwand-Einträge und bei Providern packen vielleicht bald Computer jedes Datenpaket aus und analysieren es. Die Frage ist: liegt hier überhaupt ein Eingriff in Freiheit vor? Das BVerfG bejaht dies wohl, aber das kann man nur tun, wenn man die Überwachungsinfrastruktur nicht als toten Gegenstand ohne Bewusstsein sieht, sondern als Werkzeug von Menschen. Ein Computer, der Datenpakete

„mitliest“ (= *Deep Packet Inspection* macht), verletzt Freiheit nicht. Eine Verletzung ist aber dann gegeben, wenn man die Maschine zusammen mit dem überwachenden Menschen als soziotechnische Einheit betrachtet. Auch die Telefonwanze ist ja nie Verletzer, sondern sie wird es erst mit einem Menschen, der sie benutzt.

Teil 3: Freiheit – eine politische Frage

I. Verhältnis von Freiheit zu Sicherheit

Wer nach „Freiheit oder Sicherheit“ fragt, fragt in mehrerlei Beziehung falsch.

Zum einen sind beide Güter rechtlich nicht gleichrangig. Sicherheit ist verfassungsmäßig kein eigenständiges Rechtsgut, wogegen Freiheit sich in vielen Grundrechts-Artikeln unserer Verfassung findet. Nach den Ideen der Staatsphilosophie und der Aufklärung - nehmen wir den Gesellschaftsvertrag von Rousseau als Ausgangspunkt – sind Freiheitsrechte unveräußerlich und vorstaatlich existent. Staatliche Gewalt dient nicht einer „Sicherheit“, sondern soll Freiheit gewährleisten. Sicherheit ist also Mittel zur Freiheit, weil wahre Freiheit nur in Sicherheit möglich ist, das ist der Kerngedanke. Wir sind nur frei, wenn wir keine Gewalt befürchten müssen. Das wird auch an einem ganz einfachem Beispiel deutlich, wenn wir nämlich im Dunkeln nur die Wege gehen, an denen wir uns sicher fühlen. Eine Freiheit, nur auf bestimmten Wegen zu gehen, ist bereits eine eingeschränkte Freiheit.

Sicherheit ist auch nicht auf einer Ebene der Gegenbegriff zu Freiheit. Als „sicher“ bezeichnen wir einen Zustand einer geringen Wahrscheinlichkeit der Verletzung anderer Rechte. Sicherheit ist also, wie Vertrauen, in die Zukunft gerichtet. Aber während Vertrauen die innere Erwartungshaltung einer Person in Bezug auf das Verhalten einer anderen Person ist („*Ich vertraue Dir, dass Du (nicht) so handeln wirst*“, entsprechend gilt das auch für Organisationen), kennzeichnet Sicherheit einen objektiven Erwartungs-Zustand von Integrität vom Standpunkt des Verletzten aus („*es wird zu keiner Rechtsverletzung kommen*“). Sicherheit als Institution wirkt auf den inneren Zustand aller Subjekte zurück, weil diese sich frei und angstfrei fühlen können. Sicherheit kennzeichnet einen allgemeinen Zustand, bei dem es nicht zu einem Verlust von subjektiven Freiheitsrechten kommen wird.

Sicherheit ist eher die kleine Schwester, die Vorhut der Freiheit. Diese Sicherheit ist also nicht der Gegenbegriff zu Freiheit, beide sind kein Antagonismus. Wir erliegen also einem Irrtum, wenn wir meinen, dass Freiheit und Sicherheit in Balance zu sein hätten. Vielmehr ist auch Sicherheit von der Freiheit her definiert.

II. Freiheit und Staatsverständnis

Wohl jede politische Grundströmung nimmt den Begriff der Freiheit für sich in Anspruch und interpretiert ihn anders. Wenn wir ihn einmal ein wenig von der Unveräußerlichkeit von Menschenrechten abrücken, indem wir ihn versuchsweise durch den weniger aufgeladenen Begriff „Freiraum“ ersetzen, können wir die Freiheit auch andersherum erfragen, nämlich: wie ein Staatswesen organisiert sein sollte. Sieht man einmal von radikal anarchistischen Positionen ab, gibt es hierauf eher libertäre und eher autoritäre Antworten.

Das hat Auswirkungen auf Grundsatzfragen der Netzpolitik. Von meinem eher libertären Standpunkt aus ist es nämlich immer von denjenigen, die Sicherheit als Eingriff in Freiheitsrechte fordern, zu beweisen, dass andere Freiheiten konkret gefährdet sind. Daher sehe ich wie viele aus der „Netzgemeinde“ die Vorratsdatenspeicherung kritisch, weil sie flächendeckend Freiheit einschränkt, ohne

dass eine konkrete Gefährdung nachweisbar wäre. Man braucht schon sehr starke Belege, eine abstrakte Gefährdungslage ins Blaue hinein reicht nicht. Und glauben Sie mir, ich bin Experte für Regierungsparteien und bin auf genau diesen Mangel gestoßen.

Eine andere Fraktion die ich (wertfrei) als eher autoritär denkend bezeichnen möchte, wünscht sich einen starken Staat und vertraut seinen Institutionen, solange sie rechtsstaatlich funktionieren. Für diese Fraktion ist Vorratsdatenspeicherung ein akzeptabler, geringfügiger Eingriff, es werden ja nur IP-Adressen mitgeschrieben. Ich fürchte, dieser Standpunkt ist ebenso vertretbar wie der meinige. Ich halte ihn nur für falsch. Warum? Weil ich jeder Zusammenballung von Gewalt mit Misstrauen begegne, aus einer historischen Perspektive ist das übrigens ein klassisch konservativer Standpunkt. Und weil dies erst Recht für sensible Daten gilt, die im Zweifel für bis zu 100 Jahre gegen Missbrauch gesichert werden müssen, nämlich vom Gendefekt des Ungeborenen bis ins Greisenalter, bei dem eine Lebensprognose über Gesundheitsmaßnahmen entscheidet. Die Geschichte unseres Landes lässt für mich kein besseres Menschenbild zu. An diesem VDS-Thema sieht man sehr gut, dass die Diskussion nicht um Internet – und auch nur vordergründig um den Rechtsstaat - geht, sondern um Menschenbilder und um Staatsbilder, ja sogar um geschichtliche Kontinuität.

III. Freiheit als gesellschaftliche Eigenschaft

In diesem Zusammenhang ist auch die Frage zu erwähnen, ob wir nämlich bei „Freiheit“ die individuelle oder die kollektive Ebene betrachten. Ich habe dazu eingangs schon die polaren Standpunkte des Warners und des Propheten formuliert. Die Propheten sagen ja auch, dass die Gesellschaft „freier“ würde, wobei sie damit Offenheit, Flexibilität, Transparenz, Durchlässigkeit und mehr Zugang und weniger Barrieren zu Ressourcen meinen. Hierauf habe ich aber zwei ganz verschiedene Antworten anzubieten. Die eine ist positiv, denn je mehr Wissen verfügbar ist und je transparenter politische Prozesse werden, desto besser ist das, um gute Partizipation und hohe Legitimation in der Demokratie zu erreichen. Die andere ist, dass wir hier keine Wunder erwarten dürfen, weil – lassen Sie es mich klassisch konservativ sagen – Leben auch immer ein Kampf um Ressourcen ist, oder – ich kann es auch marxistisch formulieren – das Bewusstsein das Sein nicht ändert. Hier sind wir also mitten im ideologischen Gemetzel, jedoch mit gleichem Ergebnis. Zum anderen mache ich mir auch Sorgen über Meinungsschwankungen und Empörungen, die eine leitende, systematische und planerische Politik unmöglich machen und zu einer direkten Koppelung der Repräsentanten so an den Souverän führen, dass wir ins Chaos gleiten. Als Ausweg sehe ich nur eine radikale Systemreform, welche die Politik professionalisiert und das Wahlsystem nach den neuen Möglichkeiten des digitalen Zeitalters radikal neu organisiert.

Eine ganz andere Frage ist, welche Freiheit gemeint ist: Eine politische Freiheit, sich äußern zu können (über das Partizipieren und bis zum Funktionieren der Demokratie), und/oder wirtschaftliche Freiheit, über Geld und Waren frei verfügen zu können? In diesem Punkt redet halb Deutschland aneinander vorbei. Die einen loben die wirtschaftliche Freiheit, wir haben aber auch hier Probleme zum Beispiel bei der Sammlung von Bonitätsdaten – wollen wir das? Die anderen feiern die Möglichkeiten der Meinungsartikulation, sind aber auch in Sorge um Diskriminierung und „Zensur“ sowie Marktmacht der großen Internetanbieter.

Ich kann das nicht en passant diskutieren, das wäre ein eigener Vortrag. Daher jetzt nur mein Standpunkt: die Internetgiganten (vor allem Google und Facebook) sind nicht so stark, dass sie gefährlich würden, es ist noch kein Kind in den Brunnen gefallen. Ich meine aber, wir sollten diesen Wirtschaftsbereich mittelfristig international so regulieren wie jeden Mittelständler auch. Was das im

Detail heißt, können wir gern nachher diskutieren, hier nur so viel: Informationsansprüche, Betretungsrechte, Auflagen, organisatorische Gebote und Diskriminierungsverbote.

IV. Freiheit als Idee vs. pragmatischer Handlungsfreiheiten

Zum anderen geht es ja nie um „die Freiheit" als Idee allein. Soziale Realität ist nämlich, dass 24 Mio. Facebook-Nutzer das Werkzeug, dass sie möglicherweise gefährdet, für viele Freiheiten nutzen: die Freiheit zum Beispiel, des Nachts noch kurz mit Freunden zu plauschen und die Freiheit, Veranstaltungen planen zu können. Es verbergen sich unter „die Freiheit" eine Vielzahl von Handlungen, die sich auf völlig verschiedene Interessen richten können. Manche sprechen hier auch von einer Freiheit *zu* etwas (positiver Freiheitsbegriff) als Alternativkonzept zu einer Freiheit *von* etwas (negativer Freiheitsbegriff).

Fast immer wird übersehen: Das Internet ist nicht nur Kommunikations-, sondern auch Transaktionsmittel. Wir leben und erreichen Freiheit ja schon dadurch, dass wir Waren und Leistungen im Internet kaufen. Wenn 38 Millionen Deutsche für fast 30 Milliarden EUR einkaufen[14] und dazu noch Online-Banking betreiben oder Verlagsangebote kostenlos lesen, dann spart das Zeit und Geld und schafft so auch Freiheit. Hinzu kommt, dass die Vielfalt der Güter überhaupt nur durch digitale Shops und Logistik erschlossen wird (der sog. Long Tail). Es gilt also auch: ein „freies Internet" fördert diesen Handel auch, worauf zum Beispiel Neelie Kroes, die EU-Kommisarin mit Zuständigkeit für die Digitale Agenda hinweist[15].

Erlauben Sie mir dazu eine kleine Anmerkung. Ich finde es auffällig, daß über materiellen Wohlstand als Ausdruck von Freiheit keiner reden mag und über Effizienz als Treiber vielen Fortschritts rümpft man die Nase, weil sie nach Technokratie klingt. Und gegen Innovation haben alle großen Parteien weltanschaulich begründete Bedenken; dort redet man nämlich lieber von Kulturen, die zu bewahren seien, von Nachhaltigkeit und von Deliberation im Habermas'schen Sinne. Es gibt Tage, an denen ich rufen möchte: *Hey, Effizienz ist eine tolle Sache*! Und die Warenwelt, die sich immer weiter ausweitet, weitet unsere Freiheit aus: *Bananen sind Freiheit*! *Ein Mausklick spart 20 Minuten Gang in die Stadt*! Aber leider halten diese Tage nicht lange. Zum einen sitzen Adornos Konsumfeindlichkeit und auch das religiöse Ideal des Asketen tief in mir. Priester und Intellektuelle haben bewirkt, dass ich nicht „*vorn*" denken kann, ohne gleich ein „*aber*" hinterherzusetzen. Zum anderen ist unserer Gesellschaft irgendwo auf der Höhe der Ölkrise und des Club of Rome ein Fortschrittstrauma widerfahren, das durch die großen Technikunfälle seit den 1980ern zu einer Art Lähmung geführt hat. Schon die Frage nach Fortschritt ist ja heute anrüchig, obwohl genau sie ja die richtige Frage wäre, wenn es um die Richtung der Zukunft geht. Wo ist „vorn"? Probieren Sie diese Frage nach Fortschritt mal in Ihrem Umfeld aus - und achten Sie auf die Reaktionen.

Der Zusammenhang gilt auch in kollektiver Hinsicht, weil Nischen, in denen Menschen frei miteinander Güter tauschen, ganz langfristig von Diktaturen weg in Demokratien führen. Wer nicht von Zuweisungen des Staates abhängig ist, erlebt sich als freien Menschen. Über diesen Weg fördert das Internet meines Erachtens auch die Freiheit, genauer: freiheitliche(re) Systeme.

[14] http://etailment.de/2012/e-commerce-in-deutschland-die-wichtigsten-zahlen-auf-einen-blick/
[15] http://europa.eu/rapid/press-release_SPEECH-12-326_de.htm?locale=de

Teil 4: Die spezifische Gefährdungslage durch Eigenschaften des Internets

Natürlich ist es nicht richtig zu sagen, das Internet gefährde uns nicht. Das tut es sogar in besonderer Weise. Es tut es wie jede neue Technik, die neue Risiken birgt. Das Auto brachte solches ja auch mit sich, Juristen sprechen von „Betriebsgefahr“. Lassen Sie uns das Phänomen genauer betrachten:

I. Der Kopiervorgang als Grenzverletzung

Ein zentrales Merkmal der Computer ist, dass sie Information kopieren, und zwar untereinander, und so Sphären verbinden. Das ist häufig der Grund, warum wir sie einsetzen, eine E-Mail nämlich wird kopiert, damit sie ankommt. Dabei überschreitet eine solche Information immer Grenzen zwischen Personen oder Organisationen. Dieser Kopiereffekt wirkt nur in eine Richtung, dass nämlich eine Information in einer anderen Sphäre ebenso zugänglich ist. Information geht vom Privaten ins Öffentliche, von Klaus zu seiner Clique, vom Inneren eines Unternehmen nach außen zu anderen Unternehmen, von einer Parteivorstandssitzung in die Öffentlichkeit der Medien, von US-Behörden in die Öffentlichkeit (immer durch Menschen und Maschinen, im letzten Fall z.B. durch Wikileaks). Das Internet ist der große Informationsgleichmacher, es gleicht informatorische Differenz zwischen Sphären aus wie ein U-Rohr, so dass innen und außen den gleichen Pegel haben.

Durch das Kopieren lösen sich immer Grenzen auf - die Wände werden durchsichtig, hellhörig, sind ganz verschwunden. Das ist ein Problem, denn viele Grenzen haben einen Sinn. Manchmal kann es zwar richtig sein, wenn Information diese Grenzen verlässt, denn im Geheimnis verbirgt sich gern das Unsittliche (Georg Simmel hat dazu geschrieben[16]) – wir kennen das vom „schmutzigen Geheimnis“ und vom „Mitwisser“ der kriminellen Tat. Man muss daher natürlich auch über „Ethik der Leaks“ diskutieren, die das Geheime zu recht in die Öffentlichkeit tragen.

Trotzdem ist die Grundregel andersherum: Das Geheimnis als Institut taucht in vielen Ausprägungen auf, als Amtsgeheimnis, Briefgeheimnis, Beichtgeheimnis, Redaktionsgeheimnis, Arztgeheimnis und so weiter. Die „Privatsphäre“ zum Beispiel schützt Menschen vor sozialer Repression, die Abtrennung einer Kinderwelt von einer Erwachsenenwelt soll Kinder schützen. Kommunikationsräume und –formen wie Hintergrund-, Hinterzimmer- und Vier-Augen-Gespräch sollen vertraulich sein, damit Vertrauen überhaupt erst entstehen kann, weil sich in der modernen Welt Menschen begegnen, die einander noch fremd sind – Vertrauen wie in einem biblisch-paradiesisch Urzustand ist eben leider nicht mehr natürlich „da“, wenn wir nicht mehr nur mit Vertrauten der Familie kommunizieren! Im Kommunikationsprozess können die Beteiligten Schutz wollen, weil sie ihre Standpunkte im Dialog erst erarbeiten müssen, langsam tastend – unterschiedliche Standpunkte gibt es nämlich erst, wo die Stand-Fläche gemeinsam vermessen wurde. Das bestätigt übrigens sogar die neuere Gesetzgebung zu Computerstraftaten, indem sie schon das Eindringen in fremde Computer strafbar macht; der Computer ist nicht nur Teil einer menschlichen Sphäre, sondern sozusagen als „Gefäß“ schon geschützt - wie der Brief, anders als Beichtstuhl und ärztliches Untersuchungszimmer. Ganz zu schweigen davon, dass wir Informationswände ganz allgemein brauchen, damit uns die Vielfalt und Komplexität der Gesellschaft nicht überfordert, sondern damit wir uns nur mit solchen Informationen befassen, die für uns relevant sind.

In all diesen Fällen kann das Internet sicherheitsgefährdend sein, weil es eben einen Kopiermechanismus zum Prinzip hat, der nur in eine Richtung wirkt. Ob es Grund zur Sorge ist? Ich denke nein,

[16] Georg Simmel, Das Geheimnis und die geheime Gesellschaft, http://socio.ch/sim/unt5a.htm

denn der Kopiereffekt ist die Verlängerung der Mediengeschichte: Schon die Schrift brachte den Gedanken weit weg, das Foto löste den Blick aus dem Kontext und das Fernsehen bringt jede Bewegung in die Welt, die von einer Kamera erfasst wird.

Doch nun kann es beinah jeder, beinah ohne Aufwand, beinah von überall nach überall, so daß Grenzverletzungen mehr werden und stärker wiegen.

II. Schutzmittel und falsches Vertrauen in diese

Gegen Informationskopie helfen aber Schutzmittel. Zum Beispiel Verschlüsselung, Steganografie, Passwortschutz.

Der Haken daran ist aber, dass es immer auch Gegentechnik gibt, die den Schutz aufhebt, indem sie die Schutztechnik außer Kraft setzt. Beispiel für solche Gegentechnik sind Codeknacker (statt Entschlüsselung) oder Steganalyse oder sog. „Jailbreaks“ für Apple-Handys, welche die Nutzungsbeschränkungen umgehen. Das ist das Gesetz, ein bisschen wie bei Hegel: wo die These ist, lässt die Antithese nicht lange auf sich warten. Das ist völlig logisch, denn wo einer eine Information anderen entziehen will, muss es zwingend diese anderen geben, sonst macht der ganze Schutz keinen Sinn.

Dadurch weiß man leider nie, welche der beiden Seiten gerade die Oberhand hat. Vielleicht das berühmteste Beispiel ist die Enigma-Verschlüsselungsmaschine der Deutschen, deren Inhalte im zweiten Weltkrieg von Engländern unerkannt mitgelesen werden konnten. An diesem Beispiel sehen Sie schon, dass das kein Internetphänomen ist, aber seit dem Internet hat das Problem eine neue Qualität: Jedermann hier verlässt sich auf Sicherheits-Zertifikate, deren Ausgabestellen vielleicht längst korrumpiert sind, und in Syrien vertrauen Bürgerrechtler auf Verschlüsselung, die der Geheimdienst vielleicht längst geknackt hat. Dieses Vertrauen auf den falschen Anschein wurde schon Siegfried zum Problem, als er sich durch Drachenblut in Sicherheit wähnte und das Lindenblatt zwischen seinen Schulterblättern übersah. Im Internet ist eben heute unsere Standard-Kommunikation, der Schutz hält nicht so lange und es ist auch jede Information gleich überall. Was Sie heute mit Passwörtern schützen, wird in einigen Jahrzehnten von jedermann geknackt werden. Das muss man wohl als neue Qualität von Sicherheitsproblem bezeichnen.

III. Nervensystem und Risikokumulation

Das Internet ermöglicht nicht nur private und massenmediale Kommunikation, sondern es ist auch das Werkzeug für viele Transaktionen von Unternehmen, Einzelpersonen und staatlichen Organisationen. Was sind Finanzströme anderes als Information über Buchungsstände bzw. Anweisungen für Buchungen in IT-Systemen? Auch die Warenströme fließen nicht ohne Gegenbuchung im Finanzsystem, ohne digitale Anweisung und ohne IT-gesteuerte Logistik, wenn man etwa auf unbemannte Fahrzeuge in der Hafen-Intralogistik schaut. Man kann daher wohl sagen: vernetzte IT-Systeme sind das Nervensystem aller Industriestaaten.

Die Risikokumulation führt zu einer hohen Verletzlichkeit. Diese Risikokumulation ist wahrscheinlich ein typisches Phänomen der Moderne: besonders angreifbar sind wir, seit wir Hochhäuser haben, mit Flugzeugen fliegen, tausende von Menschen U-Bahn-Systeme nutzen und wir Energie nicht mehr mit Wasserkraft, sondern mit Atomkraft erzeugen. Die Folgen krimineller Handlungen sind daher immer weitreichender, wenn man keine besonderen Maßnahmen gegen die Verletzung ergreift.

IV. Digitales Panopticum

Ein Aspekt, der mir gewisse Sorgen macht, ist das Zusammenwachsen einer Reihe von Technologien, die eine Überwachung von Menschen ermöglichen. Da ist zum einen die Möglichkeit von Bürgern, sich gegenseitig zu überwachen, und zwar ohne die jeweilige Kenntnis des anderen. Die Technikbausteine von mitschneidender Software und Mikrokameras sind heute für wenige Euro verfügbar und es wird auch nicht lange dauern, bis Gesichtserkennung auf Standbildern und konkrete Objekterkennung auf Bewegtbildern allgemein verfügbar werden. Das bekannteste Beispiel ist wohl Googles „Project Glass“[17], das den Stand der Technik auch Laien vorstellbar macht; in der Forschung sind noch ein paar mehr Dinge.

Ich persönlich habe auch Zweifel, dass der Widerstand gegen sog. „Gesichtserkennung“[18] auf die Dauer bleibt. Durch all diese Technologien wird jedermann einerseits im Privatbereich unerkannt öffentlich gemacht werden können und andererseits auch jederzeit in der Öffentlichkeit identifiziert werden können. Auch diese Veranstaltung hier kann ich schon so ins Internet streamen, daß Sie es erst hinterher merken. Genaugenommen erweist sich damit unsere Vorstellung von Öffentlichkeit hier und Privatheit dort als viel zu naiv, Öffentlichkeit war immer schon sehr vielfältig und nun lösen sich sogar einige Konzepte auf. Ich merke das immer, wenn man mich als Referent auf Internet-Veranstaltungen einlädt: ich werde zunehmend gar nicht mehr gefragt, ob mein Beitrag gefilmt und veröffentlicht wird.

Noch bedrohlicher sind Szenarios mit Technologien in staatlicher Hand, die zum Beispiel private und öffentliche Räume überwachen, Personen erkennen, Verhalten analysieren und hierzu auch mit Drohnen und Datenbanken ein einheitliches Verhaltenskontrollsystem ermöglichen. Es gibt auch Lösungen, die Internet-Kommunikation überwachen, und es gibt Pilotprojekte mit Straßenlaternen, die Kameras, Mikrofone und Lautsprecher enthalten, und es gibt Kameras, die auf 200 m Nasenhaare erkennen können. Das ist die *Realität*[19].

Verstehen Sie mich nicht falsch: ich bin kein Alarmist und ich habe sogar Verständnis für einzelne Maßnahmen, wie sie etwa die polnische Polizei gegen Nazis in Fußballstadien ergriffen hat. Es ist auch egal, ob es das EU-Projekt INDECT[20] ist oder ein anderes[21], ob die biometrischen Daten bei Facebook sind oder nicht. Wir laufen in jedem Fall in ein paar Jahrzehnten auf fundamental neue Szenarien hinaus, zumal es inzwischen sogar auf UN-Ebene erste Versuche gibt, Standards der Kommunikationsüberwachung zu etablieren, um Verbrechen zu bekämpfen[22]. Niemand wird sich mehr dem Gefühl des Unbeobachtetseins hingeben können, die „*Privatheit in der Öffentlichkeit*“[23] verschwindet. Wir haben auch - anders als noch bei Schusswaffen - nicht mehr die Möglichkeit des Verbotes, weil Verbote ins Leere gehen. Wir haben dann eine andere Welt, in der man sich ständig aktiv versichern muss, wo man sich wie verhält – der Bürger beobachtet sich permanent selbst. Vielleicht kennen Sie das Prinzip des Panopticons. [24] Wir werden dann nicht nur wie in einem

[17] http://de.wikipedia.org/wiki/Google_Project_Glass
[18] „Gesichtserkennung“ ist ein Euphemismus, es handelt sich in Wahrheit um Identitätserkennung
[19] Nasenhaare im Grossformat, heise, http://www.heise.de/tp/artikel/37/37653/1.html m.w.N.
[20] Heise zu INDECT, http://de.wikipedia.org/wiki/INDECT
[21] s.o. Fn 20.
[22] http://www.heise.de/newsticker/meldung/UN-Gremium-fordert-global-einheitliche-Vorratsdatenspeicherung-1735065.html
[23] „Privacy in Public“, wie Helen Nissenbaum das genannt hat. Diverse Texte hier http://www.nyu.edu/projects/nissenbaum/main_cv.html#pub
[24] http://de.wikipedia.org/wiki/Panopticon

Panopticon beobachtet, bei dem ein einziger Beobachter zur Überwachung vieler genügt. Wir werden uns auch gegenseitig beobachten, so dass jeder zugleich Überwacher und Überwachter ist.

Die Frage ist nur, was davon zu halten sein wird: Wird das überhaupt ein Problem, weil Computer immer mehr Daten erzeugen als sie analysieren können (das Mengenproblem gibt es heute schon bei Videoaufzeichnungen)?[25] Ist das dann eventuell doch entstehende Szenario eine Neuauflage des Überwachungs-Buchklassikers von George Orwell? Oder ist das alles unter „Transparenz" einzuordnen – einem Prinzip der nächsten Gesellschaft, die ja in diesem Punkte gar nicht so viel anders als die tribale Gesellschaft unserer Vorfahren ist, die viel voneinander wussten? Und bei Drohnen haben einige seit kurzem auch Hoffnungen in sog. *Drohnenjournalismus*[26], die Zukunft der Berichterstattung, die alles öffentlich macht, während andere mit Drohnen Medikamente und andere Infrastruktur in andere Länder bringen wollen.[27] Ich persönlich tippe, dass Drohnen als universelles Transportmittel normal werden

Wir werden daher wohl irgendwann auch damit rechnen, von oben beobachtet und in der Öffentlichkeit auch dauerhaft Informationen zu hinterlassen („*Datenspuren*" sage ich gern dazu). Das ist einer der Punkte, in denen sich das Konzept von Privatsphäre in der fernen Zukunft verändern wird, die Gesellschaft hat sich ja in diesem Punkt historisch immer verändert.

V. Ambient Intelligence

Mit den Schlagwörtern *Ambient Intelligence* und *Ubiquitous Computing* ist noch einen Trend bezeichnet, der noch gar nicht bei uns angekommen ist. Zusätzlich zum Arbeits-PC gibt es schon Handys, den Tablet-PCs und bald auch webbasiertes Heim-TV, weil Computer weiter kleiner und billiger werden (*Moore´sches Gesetz*). Das geht noch eine Weile weiter, es kommen PCs in Kleidung (*Wearables*), in der Haussteuerung, in der Verkehrssteuerung, in der Landwirtschaft - eigentlich überall, um spezielle Aufgaben zu übernehmen. Zur Identifikation setzt man reiskorngroße Chips ein (*radio-frequency identification = RFID*), die zum Beispiel seit zwei Jahren auch in Bundespersonalausweisen eingebaut sind, und seit der Umstellung des Internets auf einen neuen IP-Standard kann jeder Gegenstand auf der Welt eine eigene Adresse bekommen. Niemand weiß, wo es genau hinführt, aber wir werden in normalen Haushalten ganz sicher viele Endgeräte haben, die direkt untereinander sprechen können. Und dadurch weitet sich das Internet in die Welt physischer Gegenstände aus, weswegen die Abhängigkeit und die Gefährdung grundsätzlich zunehmen. Was mit dem Virus *Stuxnet* bei Zentrifugen angerichtet werden konnte, ist dann vielleicht auch bei ganz anderen Geräten möglich – vielleicht gehen irgendwann durch ein solches Sicherheitsproblem irgendwo keine Garagentore mehr auf oder Haushaltsroboter machen sehr eigenwillige Späße, indem sie Haustiere mit geraden Registriernummern in Mikrowellen zur Explosion bringen. Das ist die nächste Stufe des Internets.

[25] vgl. Glaser, Peter, Wollt Ihr die totale IT? http://carta.info/22131/wollt-ihr-die-totale-it/

[26] http://www.drohnenjournalismus.de/ und http://www.guardian.co.uk/media-network/media-network-blog/2012/oct/29/drone-journalism-take-off als Einstieg. Vgl. auch eine Ankündigung von Philip Banse für das Refugeecamp in Berlin Wir machen morgen etwa 10-11 Livestream vom #refugeecamp, evtl. mit Drohne und mehreren Cams, https://twitter.com/philipbanse/status/263026380281880576

[27] Und zwar Matternet.us, bis hin zu Dönercoptern, einführend http://t3n.de/news/lieferservice-zukunft-unbemannte-424120/

VI. Komplexität und Unbeherrschbarkeit

Es wäre Unsinn, wachsende Komplexität nur in Digitalien zu verorten, die Komplexität wächst überall in der Gesellschaft. Sie wächst aber in atemberaubendem Tempo auch in Digitalien. Ich selbst habe in den 80ern noch die Prozessorarchitekturen verstanden und konnte für jedes Register bei jedem Programmschritt deren Inhalte sagen, während ich den Programmcode las. Heute ist der Aufwand zum Verständnis um Zehnerpotenzen höher. Nun kennen wir dieses Phänomen von jeder Technik, bei Computern ist aber die Komplexität des Codes und die Fehleranfälligkeit ein auffälliges Phänomen, an das sich auch Fachleute schon gewöhnt haben. So gibt es Systeme, deren Ergebnisse wir nicht voraussagen können, etwa im Bereich lernender Algorithmen, obwohl man sie wohl als logisch vorherbestimmt (*deterministisch*) ansehen muss. Und in Echtzeit kann nur Software das Funktionieren von Software überwachen - die ja dann, wenn sie andere Systeme steuert, auch noch bis zu 1.000 externe Komponenten wie Sensoren berücksichtigen muss[28]. Obwohl es einige Strategien gibt, mit dieser steigenden Komplexität zurechtzukommen (Software testet Software, Redundanz etc.), liegt hier doch ein Potential für Missbrauch und „Fehlgehen“ von Software.

VII. Kontaktdichte, Auflösung

Durch das Internet hat sich, wie vorher schon durch das Telefon, unser sozialer Interaktionsraum erweitert. Jeder kann mit jedem in Interaktion treten und häufig tun wir es auch, allein schon durch die Spannweite sozialer Netzwerke mit durchschnittlich 200 Kontakten pro Person. Wir werden in ein paar Jahren erleben, wie sich in der „realen Welt“ noch viel mehr Menschen verbinden, wenn sie sich als Passanten begegnen. Sogenannte „Body-To-Body“-Netzwerke, bilden sich ad hoc und automatisch. Vorher bilden Handys solche Netzwerke, sog. *Mash-Ups*, mit denen man spontan Daten tauschen kann. Das stellt man sich seit Jahren für Visitenkarten-Austausch vor, die Chancen und Risiken sind aber noch gar nicht einschätzbar, beispielsweise werden vielleicht ausgerechnet Konzerthallen zu den größten Musiktauschbörsen, wird *Instant-Dating* an Kulturplätzen normal, informieren uns Systeme automatisch über Passanten mit den gleichen Spezialinteressen?

Das ist nicht weit weg, das könnte alles Facebook sein und dann als Protokoll auf verteilte Systeme übergehen. Durch diese neue, sehr hohe Kontaktdichte kommen auch Sicherheitsprobleme in einer neuen Dimension, weil viele Software-Systeme miteinander sprechen müssen.

Teil 5: Taktiken für Lösungen

Natürlich arbeiten IT-Industrie und Politik an Lösungen. Ich versuche im Folgenden die Taktiken strukturiert darzustellen.

Auf Lösungen, die nicht Internet-spezifisch sind, will ich nur jetzt kurz eingehen. Wir brauchen natürlich ganzheitliche Lösungen. Darüber hinaus sind natürlich die wichtigsten Lösungen normativ und/oder institutionell: man schafft Gesetze zur Regulation oder zu den Bedingungen des Technikeinsatzes, man verhängt Meldepflichten (gerade im Bundestag für Cyberattacken von Minister Friedrichs vorgeschlagen[29]), man verbietet Technologien oder verhängt ein Moratorium, man schafft Steuervergünstigungen, man weist erwünschten Stellen ausreichende Ressourcen zu und so weiter. Auf dieses Instrumentarium gehe ich aber heute nicht weiter ein.

[28] Embedded Software Engineering, http://de.wikipedia.org/wiki/Embedded_Software_Engineering
[29] http://www.sebastian-blumenthal.de/content/experten-best%C3%A4tigen-allgemeine-meldepflicht-nicht-zielf%C3%BChrend

I. Grenzen

Die naheliegendste Taktik gegen Gefährdungen ist es, das gefährdete Gut gar nicht erst in Gefahrzonen zu bringen. Also Daten gar nicht erst in IT-Systeme einzuspeisen und etwas dem Internet von vornherein nicht zugänglich zu machen, so dass es von der Ubiquität des Internets und der „Echtzeit-Sofortyness“ gar nicht erst umfasst werden kann. Das kennen wir aus der analogen Welt auch, wenn wir unsere Gespräche in die Einsamkeit der Wildnis legen.

Diese Grenzziehung ist auch innerhalb von IT-Systemen möglich, so kann man etwa Netze auf der untersten (der physischen) Ebene entkoppeln. Das Prinzip findet sich im Großen als Containment, das wir von Atomkraftwerken kennen, um Schäden zu begrenzen. Und wir finden es im Kleinen, in dem man jede Software-Routine von anderen so zu kapseln versucht, das keine unvorhergesehenen Wechselwirkungen entstehen. Dabei sind häufig innerhalb der Grenzen wieder abgegrenzte Teile, etwa hat ein Leichtwasserreaktor mehrere Barrieren (Druckbehälter, Schild, Sicherheitsbehälter, Stahlbetonhülle etc.) und bei Software trennt man Funktionen von Modulen und Komponenten.

(Diese Grenzen dürfen jedoch nicht einen Millimeter offen sein, sonst tritt das Gegenteil ein: schutzwürdige Kommunikation offenbart sich und gibt sich ungeschützt preis. Überall, wo es ein Innen und ein Außen gibt, ist das Einbrechen systeminterner Barrieren möglich, dann kann es gewaltige Löcher geben. Zum Beispiel können Dritte die Kontrolle über einen *Staatstrojaner* gewinnen oder ihren Computer zu Angriffen mit *Bot-Netzen* missbrauchen. Das gilt natürlich auch für legal durchlöcherte Grenzen, etwa *SWIFT* für europäische Finanztransaktionen, Zugriffe amerikanischer Sicherheitsbehörden auf Google & Co nach dem *Patriot Act* und für eine in Europa von einem Standardisierungsinstitut namens *ETSI* gerade vorgeschlagene Schnittstelle.[30])

Hin und wieder wird angesichts solcher Szenarios vorgeschlagen, doch von vornherein eine Grenze ins Internet einzuziehen: neben das Internet tritt ein zweites Netz für kontrollierte, identitätsgeprüfte Interaktionen. Das ist ein Thema für sich.

Ganz wichtig: Sie kennen vielleicht die Möglichkeit, mit einem Smartphone eine Internetverbindung für ihren PC aufzubauen, das Smartphone wird hier zum WLAN-Sender. In der nächsten Stufe der Entwicklung, ich erwähnte es bei *Ambient Intelligence*, wird es Netzwerke geben, die von Handys untereinander nach Bedarf aufgebaut werden. Hier entstehen dann geschützte Zonen, die von außen nur aufgehoben werden können, wenn eines der beteiligten Handys kompromittiert ist. Ich glaube, hier wird auf Dauer viel Potential für Bürger liegen, die nicht wollen, dass jeder jedes Datenpaket mitlesen kann, wie es heute im Internet ist.

Anders sieht die Situation hinsichtlich *Cyberwar* aus. Hier gibt es zwar Angriffe über das Internet auf wichtige Infrastruktur (Zahlungsverkehr, Strom, Kommunikation), aber hier gehen auch Staaten mit Geheimdiensten und Militär so vor, dass sie USB-Speicher direkt am Ziel an die Rechner anschließen.[31] Man darf also nicht annehmen, dass „*das Böse durch das Netz*“ geht; vielmehr operiert das Böse mit vielen Tatwerkzeugen, auch dem Internet.

II. Geschlossene, proprietäre Systeme und Monokulturen

Eine weitere Möglichkeit ist, sensible Funktionen nur auf bestimmten Geräten ausführen zu lassen, auf spezieller Hardware, die in irgendeiner Weise „versiegelt“ ist. Das war lange bei Handys so, bevor sie Smartphones wurden, und das wird als Strategie wieder kommen. So etwas wendet man

[30] http://blog.zdf.de/hyperland/2012/08/europa-will-geheime-hintertuer-fuer-die-cloud/
[31] http://www.zeit.de/2010/48/Computerwurm-Stuxnet/komplettansicht

beispielsweise bei *Device Control* an, wo z.B. nur bestimmte Speichermedien vom System zugelassen sind.

Eine andere Art, sich weniger angreifbar zu machen, ist, möglichst viele Elemente eines Systems so untypisch zu machen, dass es mit Knowhow über Standards nicht geknackt werden kann. Je mehr spezifische Kenntnisse man zum Knacken braucht, desto mehr steigt der Aufwand.

Wird das allerdings bekannt oder – wie im Falle von Sicherheitsbetriebssystemen[32] – aktiv vermarktet, fällt ein Teil des Vorteils weg, weil sich viele Angreifer mit dem System befassen.

Aus diesem Grund sollte man auch Monokulturen vermeiden, sagen Security-Spezialisten. Hohe technische Diversität fördert die Sicherheit.

Und ein Sonderfall, dessen Bedeutung noch unklar ist, ist Hardware, die nur bestimmte Funktionen erlaubt: Zum Beispiel hat Apple ein Patent darauf, dass die iPhone-Kamera an bestimmten Orten nicht funktioniert. Hier kann man also zentral jedem Endgerät mitteilen, wo es Grenzen zu beachten hat. Man spekuliert, dass Apple das Patent als Entgegenkommen zur Musikindustrie angemeldet hat, damit IPhones auf Konzerten keine Aufnahmen mehr machen können.

III. Mediale Rückwärtsbewegung

Jeder kann zurück. Vom Netz zum Telefon, von der Schrift zur Mündlichkeit, von der Sprache zu den Zeichen. Füllen Sie zum Beispiel Überweisungsträger von Hand aus oder machen Sie Phonebanking. Das ist kein Witz, so haben sich Mönche mit Schweigegebot beholfen, indem sie einfach eine Fingersprache entwickelt haben[33]. Diese Taktik benutzt zwar immer die aufwendigere Lösung, ist aber auch sicherer.

IV. Aktualität der Lösungen

Verwenden Sie immer die neueste Software, hier haben Sie die höchsten Sicherheitsstandards und gleichzeitig die geringsten Sicherheitsprobleme zu erwarten. Ein iPhone, sagte mir gerade ein Security-Spezialist, sei derzeit nicht zu knacken. Dort eine Software einzuschmuggeln, die in bestimmten Bereichen ausgeführt wird, sei noch zu schwierig.

In diesem Zusammenhang herrscht aber wieder die Ambivalenz: Zum einen hat die neueste Technik häufig auch die meisten Fehler, man sollte also die zweitneueste Technik bevorzugen. Zum anderen wird die neueste Technik von der allerneuesten Technik geknackt: Gerade ging durch die Presse, dass die Verschlüsselung eines älteren Sicherheitsprotokolls durch mächtige Cloud-Dienst binnen 24 Stunden geknackt werden kann (PPTP).[34] Die Konsequenz hieraus ist auch, dass ein Stehenbleiben auf einer Softwareversion die Wahrscheinlichkeit von Sicherheitsproblemen erhöhen kann.

V. Gehärtete Lösungen

Angesichts des heutigen Vortragstitels wird es sie nicht verwundern, dass ich Ihnen nun einen wichtigen Vorteil der Risikokumulation nenne, die ich vorhin noch als kritischen Faktor beschrieben habe. Dieser Vorteil tritt durch die Cloud ein, weil durch diese Art von Zentralisierung Dienstanbieter wie Google überhaupt erst einen sehr hohen IT-Sicherheitsaufwand betreiben können. Große Anbieter

[32] http://eugene.kaspersky.com/2012/10/16/kl-developing-its-own-operating-system-we-confirm-the-rumors-and-end-the-speculation/
[33] Fundstelle im Gesichtsforum, reg 3.11.
[34] Der Todesstoß für PPTP, heise Security, http://www.heise.de/security/artikel/Der-Todesstoss-fuer-PPTP-1701365.html

mit vielen Nutzern und mehr Umsatz können sich einfach mehr Ressourcen leisten als kleine Anbieter. Daher kann man Cloud-Systemen häufig mehr Vertrauen als den Systemen vom Anbieter um die Ecke entgegenbringen. Misstrauen ist aber immer noch bezüglich Einhaltung deutscher Datenschutzbestimmungen und der Möglichkeiten geboten, seine theoretischen Rechte in einem gerichtlichen Verfahren auch wirklich durchzusetzen.

VI. Exklusivität

Nur Staaten, Tyrannen oder Terroristen können sich den Luxus dieser Strategie leisten, die Exklusivität. Sie gilt für das High End an Sicherheitstechnologie, z.B. lange Zeit für kryptografische Verschlüsselung bestimmten Standards. Auf der Liste der Exportverbote sind beispielsweise Supercomputer und Verschlüsselungstechnik für Funknetze[35].

Wird Exklusivität noch möglich sein, wenn Kriminelle auch nur 1% der 150 Milliarden EUR, die Gadaffi gehabt haben soll, in Softwaretechnik investiert werden sollen? Auf der einen Seite ist die Komplexität eine Hürde, meistens die beste Hardware erforderlich und ihre Beschaffung könnte ähnlich erschwert sein wie die von Atomwaffen-Zutaten. Auf der anderen Seite ist Software-Technik präzise nachvollziehbar und sie passt auf eine Fingerspitze. Es ist also mit gewisser Wahrscheinlichkeit möglich, dass Exklusivität ausgehebelt wird.

Interessant, nebenbei: Computertechnik wird mit Computertechnik überwacht, nämlich mit Satelliten, Videodrohnen und Echelon (für den Datenverkehr). Hier zeigt sich das wieder das Verhältnis mehrerer Technologien zueinander: der Missbrauch des Computers wird durch Computer verhindert und neuere Technik überwacht die ältere. Auch Atomwaffen werden, so vermute ich jedenfalls, durch den Computer nicht nur besser (d.h. gefährlicher), sondern sie werden auch sicherer, weil der Computer bessere Beobachtungs-, Steuerungs- und Alarmfunktionen ermöglicht.

VII. Kontrolle und Kontroll-Kontrolle

Das Prinzip „Überwachung“ funktioniert auch zwischen Software-Modulen. Software überwacht Software, Sie kennen das vom Virenscanner und vom Windows-7-Kompatibilitätscheck. Das Prinzip ist ein Erfolgsgeheimnis des Internets, es laufen Monitoringsysteme auf allen Servern, und es läßt sich beliebig verschachteln. (Leider funktioniert auf diese Weise auch Abhör-Software, indem sie nämlich die Ergebnisse anderer Software mitschneidet und analysiert, so dass wir auch hier wieder auf Ambivalenz stoßen.)

VIII. Identitätsprüfung, -täuschung

Das Internet - in seiner Grundlagen-Technik mindestens zwei Jahrzehnte alt – wird sich in einem Punkt sicherlich noch ändern. Es betrifft die Ermittlung von Identität der Nutzer. In der Vergangenheit hat sich an Endgeräten viel getan. Fingerabdruck-Scanner sind nichts ungewöhnliches (bei Edeka soll das normal sein). Facebook und Google registrieren sehr genau, wann welche Geräte sich einloggen und erhalten so Hinweise auf unberechtigte Nutzung durch andere Identitäten. Das künftige Internet wird vermutlich Identitätsmanagement mitbringen.

(Natürlich versuchen auch Kriminelle, über ihre Identität zu täuschen, es steigen jedoch die Anforderungen an diese Methoden. Je nach Kontext kann die Identitätstäuschung sogar moralisch richtig sein. Eine Lösung gibt es also auch hier nicht.)

[35] U.S.A. – Einstieg hier http://www.bis.doc.gov/policiesandregulations/ear/index.htm

IX. „Störkommunikation“, „Noise“

Ein Verfahren, sich gegen Überwachung zu schützen, kann in Störkommunikation gesehen werden, also einer solchen, die die Kommunikation anderer stört. Das geschieht zum Beispiel mit Fake-Accounts oder mit DDoS-Attacken, also genau denjenigen Methoden, die wir oben noch als sicherheitsgefährdend gesehen hatten, auch das ist leider Ambivalenz. Ähnlich ist die systematische Erzeugung von Daten, welche andere Systeme irritieren. Das klingt recht akademisch, nichts anderes tue ich aber in der Praxis, wenn ich absichtlich falsche Standorte auf Twitter poste. Das ist meine Taktik, um den Ort meiner Anwesenheit generell zu verschleiern. Auch Stördaten durch Computer sind möglich, Sie können zum Beispiel mit einer kleinen Browser-Erweiterung[36] Google falsche Suchabfragen unterschieben, so dass Google falsche Profildaten von Ihnen erzeugt. Oder ein Hersteller wie Apple setzt Nutzungsbeschränkungen ein, die „hart verdrahtet“ sind. Es sind verschiedene Verfahren, immer mit demselben Ziel. Das hat natürlich Grenzen, weil es auch die Zielgruppe von Information unbeabsichtigt irritiert.

X. Redundanz

Redundanz ist immer schon ein Mittel gewesen, kritische Technik gegen Ausfälle abzusichern, und sie hilft daher auch gegen Angriffe. In der Internet-IT ist Redundanz vieler Komponenten der Normalfall und sorgt für sehr hohe Verfügbarkeit. Im Falle von Fukushima sieht man aber, wie auch die beste Redundanz nicht hilft, wenn unvorhergesehene Risikokumulationen auftauchen: Notstromaggregate springen zwar nach einem Erdbeben alle an, doch aufgrund eines Tsunamis fallen sie dann aus - und dann, weil auch keine Generatoren mehr beschafft werden können, fällt die Kühlung aus und das Unglück nimmt seinen Lauf. Das Beispiel zeigt: Gegen gezielte Angriffe der Infrastruktur im Cyberwar hilft Redundanz wohl nicht, wenn mehrere Komponenten angegriffen werden.

XI. Jedermann-Waffen

Den nächsten Punkt nenne ich „Jedermann-Waffen“. Eine Taktik ist nämlich, Waffengleichheit zu erreichen, indem jedermann über das gleiche Werkzeug verfügt. Das ist das Prinzip, das wir schon in Bürgerwehren und amerikanischer Waffengesetzgebung finden. Hans Magnus Enzensberger schreibt 1970 als Lösung gegen Manipulation: *„Ein unmanipuliertes Schreiben, Filmen und Senden gibt es nicht. Die Frage ist daher nicht, ob die Medien manipuliert werden oder nicht, sondern wer sie manipuliert. Ein revolutionärer Entwurf muß nicht die Manipulateure zum Verschwinden bringen; er hat im Gegenteil einen jeden zum Manipulateur zu machen.“* Ist es wirklich so abwegig, wenn jeder seine Störsender und seine Drohne hat? Vielleicht ist das doch die Zukunft: formale Waffengleichheit. Bei Fotohandies haben wir es ja schon, beim Hochladen von privaten Adressbüchern, warum nicht auch bei Gesichtserkennung, Störsendern, Peilsendern, Drohnen? Mir persönlich ist kontrollierte und mehrfach abgesicherte Gewalt lieber, aber in kommunikativen Fragen wird es vielleicht einfach so kommen.

Teil 6: Schluss

Meine Damen und Herren, ich habe gesagt, was ich zu sagen hatte. Es gibt keinen Appell zum Schluss, keine Warnung, keine Mitnahme-Ratschläge. Ich kann nicht weit nach vorne gucken. Technik ist kein Leben, aber sie entwickelt sich aus ihm heraus, daher ist sie ungewiss.

[36] Das Browser-Plugin TrackMeNot, http://cs.nyu.edu/trackmenot/

Es ist sinnlos, sich mit Extrempositionen zu streiten, wie das in der Öffentlichkeit geschieht, googeln Sie bitte *Jeff Jarvis* und *Evgeny Mozorov,* die sich wie die Kesselflicker schlagen und dabei vor allem mediale Bedürfnisse befriedigen. Genauer: Unser Bedürfnis nach Einfachheit der Erscheinungen und einfacher Kausalität bei gleichzeitig maximaler Unterhaltung. Vielleicht muss diese mediale Polarisierung sein, damit unsere Gesellschaft sich selbst steuern kann, denn das Schauspiel wiederholt sich seit Urzeiten. Die Argumentationsmuster wirken heute zum Teil recht komisch, und jetzt nehme ich nur die Utopisten, von *Hiram Maxim*, der sagte, das Maschinengewehr werden den Krieg unmöglich machen, über *Georg Gissing*, der das gleiche über das Flugzeug sagte, bis zu *Guglielmo Marconi*, der meinte, mit der Erfindung des Radios werde Krieg lächerlich.[37]

Es ist richtig zu sagen: Für einen einzigen Menschen bietet Technik vor allem neue Optionen und somit mehr Freiheit. Im Hinblick auf mehrere Menschen muss man meines Erachtens sagen: Alle Werkzeuge können freiheitseinschränkend und freiheitsfördernd wirken, Technik ist neutral. Das liegt ganz einfach daran, dass Menschen mehr oder weniger ethisch richtig handeln und Technik immer in Konflikten eingesetzt wird, wo sie auf beiden Seiten stehen kann. Wo sie eingesetzt wird, verdrängt sie meistens altes Handeln und erzeugt Abhängigkeit, die zum einen aus Verlernen resultiert, zum anderen aus sozialem Druck. Schon hier sieht man, wie Mensch und Technik sich gar nicht trennen lassen.

Wie beide zusammengehören, sieht man auch an folgendem: Menschen mindern mit neuer Technik alte Technikrisiken, wobei sie natürlich neue Risiken erschaffen. Ein Beispiel: die *Mashup-Netze* der nächsten Generation werden private Kommunikation noch schwerer überwachbar machen. Ich finde diese Beobachtung ermutigend. Ein Beispiel für neue Risiken ist der Mail-Spam, der mit der Mail kam, weil die Internet-Technik dazu geradezu herausgefordert hat.

Sie findet sich auf der Haben-Seite des Computers an vielen Stellen: Computer wirken zum Beispiel dabei mit, die Todesrate im Straßenverkehr drastisch zu senken (*eingebettete Gegentechnik*). Mir scheint es ohnehin eher fragwürdig, „das Internet“ zu bewerten. Richtiger wäre: viele soziotechnische Systeme wären zu bewerten. „Das Internet“ ist eine naiv-technische Sicht, Erwachsene sollten es als viele Teilsysteme begreifen, wenn sie politisch oder sozial diskutieren.

Ebenso ermutigend finde ich, dass neue Technik unvorhergesehene Lösungen produziert. Das Internet selbst ist das beste Beispiel, die E-Mail und das Web sind beide nicht geplant gewesen, sondern beiläufig geschehen. Natürlich muss das so nicht sein, es ist erlaubt uns aber mehr Gelassenheit und Zuversicht.

Die Idee von der Technikneutralität, von der ich oben gesprochen habe, ist aber leider auch viel zu simpel. Technik wird aus sozialen Systemen geboren und sie wirkt auf sie zurück. Daher entscheiden Ressourcen darüber, was entwickelt wird (Geld, Macht, Wissen etc.), und wir können gewisse Leitentscheidungen treffen sowie Einzelfälle regulieren. Wir können Forschung in „Richtungen“ lenken, und wir können Einzelfälle z.B. verbieten (biometrische Datenbanken, Internetfilter etc.), wobei „wir“ alle Bürger oder Teilsysteme der Gesellschaft sind. Außerdem haben wir immer die Möglichkeit, in technische Prozesse einzugreifen – selbst im Hochfrequenzhandel kann der Schaden begrenzt werden.

[37] Unbedingt lesenswert ist übrigens dazu *Kathrin Passigs* Aufsatz „*Standardsituationen der Technologiekritik*, MERKUR, zweitveröffentlicht auf http://www.eurozine.com/articles/2009-12-01-passig-de.html sowie das Gegenstück „*Standardsituationen der Technologiebegeisterung*“[37] in diesem Jahr

Was wir jedoch berücksichtigen müssen ist, dass sich Menschen auf neue Situationen einstellen (sich anpassen, lernen, neue Nischen finden etc.), die ganze Geschichte der IT-Sicherheit ist ein Fall von Lernen: Jeder Betriebssystem-Patch ist das, der ein Sicherheitsleck stopft und anschließend weltweit automatisch verteilt wird. Menschen stellen ihr WLAN sicherer ein oder installieren Virenscanner. Fehler, die Programmierer früher öfters mal machten (zum Beispiel, Klarwörter in einer Browser-URL mit zu übertragen), sind heute durch den Stand der Technik begriffen. Dass Handys von Ferne ausgelesen oder deaktiviert werden können, ist erlernt aus den Problemen bei Verlust. Neuere Technikentwicklung ist häufig eine Reaktion auf Mängel von alter Technik. Ich möchte hier niemanden provozieren, aber an Extremfällen deutlich machen, worum es geht: die Atombombe hat einen kulturellen Schock ausgelöst, so dass sie sechzig Jahre nicht zum Einsatz kam, die Entscheidungen nach Fukushima kennen Sie und die Neutronenbombe kam erst gar nicht zum Einsatz. Es gibt unendlich viele Theorienstreit über Evolution und Entwicklung, aber eins steht wohl doch fest: Menschen lernen, die Zivilisation schreitet voran.

Und es lernt das gesamte soziale System, indem es neue Gesetze und Institutionen schafft. Ein gutes Beispiel ist die Entwicklung des Automobils, wo außer der immanenten Gegentechnik alles dazu gehört, was wir heute an Verkehr kennen: Ampeln, Schilder, Fahrtenschreiber, Leitplanken und Mittelstreifen. Ganz zu schweigen von Normen wie dem StVG und der StVO, von Bedingungen wie Führerscheinen – und dem TÜV als ein Beispiel für eine Institution, die technische Risiken überwachen und begrenzen soll (wie auch die Polizei, soweit sie präventives Ordnungsrecht ausführt). Das ist, wenn man genauer hinguckt, nicht nur im soziaotechnischen System „Auto“ so, sondern ebenso bei Strom, Atomkraft, Flugzeugen.

Die Lösung wird wie bisher in der Richtung zu suchen sein, dass wir die Werkzeuge nach ihrer Gefährlichkeit abgestuft behandeln: manche müssen gar nicht geregelt werden, manchen bedürfen Verordnungen oder Gesetzen, mal als Verbot mit Erlaubnisvorbehalt, mal mit und mal ohne Strafen, in verschiedenen Höhen. Manche dürfen nur in bestimmte Hände, vielleicht nur in staatliche (bei Panzern und Atombomben klappt das im Westen ja auch), und solange wir auf jeder Ebene der Kontrolle dafür sorgen, dass die Beteiligten sich austarieren, wird sich durch das Internet strukturell nichts ändern. Es ist eine ständige gesellschaftliche Aufgabe, für das die Politik eine ruhige Hand braucht.

Ich habe auch versucht zu zeigen, dass Technik nicht einfach dummes, vom Himmel fallendes Blech ist, dass mit einzelnen Menschen zusammen als eine Einheit anzusehen ist, sondern auch, dass Technik aus den Teilen der Gesellschaft kommt: das Wissen kommt häufig aus Wissenschaft, die Herstellung technischen Gerätes meistens aus der Wirtschaft, die Normen mit Technikbezug meistens aus der Politik[38]. Und Technik wirkt auf alle Akteure der Gesellschaft zurück und verändert sie so – der Politiker mit Gesetzgebungstechnik, der Wirtschaftsmensch mit Powerpoint und der Pfarrer mit dem Beichtstuhl.

Die letzten vier Punkte bedeuten, dass fast alle Menschen involviert sind und viel mehr Zeit brauchen, um die Veränderung zu vollziehen. 20 Jahre Internet sind für eine Gesellschaft „nichts“, verglichen mit anderen Umbrüchen. Wir müssen mit Distanz auf die Dinge schauen. Und wie ich zeigen wollte, es ist eine irgendwie gemeinschaftlich geartete Aufgabe von Teilsystemen der Gesellschaft, wo *Fingerpointing* nicht hilfreich ist. Normalerweise würde ich jetzt sagen: schönen Gruss nach Bielefeld, aber da bin ich ja.

[38] Besser wäre es wohl, Technik bei einem weiten Technikbegriff als Teil eines jeden Teilsystems zu sehen, dass sich die Technik selbst entwickelt und selbst Normen setzt

Ich persönlich habe keine Angst vor Dystopien irgendwelcher Hollywood-Filme. Die größten Katastrophen der Menschheit waren bisher nicht moderne Technikkatastrophen, obwohl es uns vor allem seit den 1980ern so scheint, von Seveso über Tschernobyl bis Estonia (darunter sind einige wie Seveso vor allem ein Medienereignis). Die größten Katastrophen sind kriegerisch oder auf Naturereignisse zurückzuführen, das größte Schifffahrtsunglück war 255 vor Christus der Untergang einer ganzen *römische Flotte* im Sturm mit 100.000 Toten, gefolgt von Abschuss des deutschen Wilhelm *Gustloff* 1945 mit bis zu 9.000 Toten. 39 Und wir vergessen auch gern noch mehr „antike Technikkatastrophen" wie die, dass 1578 in *Buda* 2.000 Menschen durch eine Explosion in der Pulverkammer starben. Ich bezweifele also, ob der Eindruck richtig ist, dass die Risiken durch Technik zunehmen. Und zwar, weil unser kulturelles Gedächtnis die *mediale Übertreibung ohne Analyse* speichert, bevor es gleich die nächste Katastrophe serviert bekommt. Wo wir planen und Risiken minimieren können, tun wir das. Weil Menschen klüger sind als viele glauben. Einem vollständigen *Panopticum* wird niemand zustimmen, auch einer anlassfreien Online-Überwachung nicht.

Schwierig wird es mit dem *Cyberwar* und *Terrorismus*, für beide ist das Internet natürlich Werkzeug und Handlungsraum. Ich fürchte, und das macht mich selbst etwas traurig, hier gibt es zwei Antworten.

Die eine ist, dass wir nur die Chance haben, keine Schäden zu erleiden, wenn wir *maximales Wissen* (neudeutsch: einen *Knowhow-Vorsprung*) haben, und zwar sehr langfristig, unabhängig von der Frage einer tatsächlichen Bedrohung. Wir verlieren sonst die Autonomie als Gesellschaft, weil wir auf Partner angewiesen sind.

Die zweite Antwort ist, dass das Versagen des Menschen eine historische Konstante ist. Wir können, ja wir müssen *Werte* in Technikentwicklung integrieren und dem Utilitarismus entgegenstellen, der *nur* in Effizienz und ähnlichem denkt. Aber es gibt keine Erlösung im Diesseits. Ich habe Ihnen vorhin drei Zitate von Technikvisionären genannt und möchte dem kein viertes dieser Art hinzufügen. Das Internet verhindert keinen *Krieg*. Es wird *Teil* desselben sein. Das Leben ist nicht *sicher*.

[39] http://de.wikipedia.org/wiki/Kategorie:Liste_(Katastrophen) ; http://de.wikipedia.org/wiki/Liste_der_gr%C3%B6%C3%9Ften_nicht-atomaren_Explosionen; http://de.wikipedia.org/wiki/Liste_der_schwersten_Katastrophen_der_Schifffahrt