MICHAEL SEEMANN

iRIGHTS media

DAS NEUE SPIEL

STRATEGIEN FÜR DIE WELT NACH DEM DIGITALEN KONTROLLVERLUST

Michael Seemann

Das Neue Spiel

Strategien für die Welt nach dem digitalen Kontrollverlust

Verlag iRights.Media

Oktober 2014

Teil II: 10 Regeln für das Neue Spiel

Regel 2 | Die Überwachung ist Teil des Spiels

These: *Die Überwachung wird im Neuen Spiel massiv zunehmen, und wir werden zähneknirschend damit leben lernen. Effektiv gegen Überwachung kämpfen bedeutet, die Wirkung von Überwachung zu schwächen.*

Es war eine aufwühlende Zeit, Anfang der 1980er, eine politische Zeit. Großprojekte wie die „Startbahn West“ des Frankfurter Flughafens, die Stationierung von Mittelstreckenraketen und die Atompolitik hatten soziale Bewegungen hervorgebracht, die sich immer lautstärker gegen die Politik eines aus ihrer Sicht immer repressiver werdenden Staates wandten. Und dann kam die Volkszählung. Die Gegnerinnen schafften es, weit über die üblichen Verdächtigen der Friedens- und Umweltbewegung hinaus zu mobilisieren. Bis März 1983 war von über 500 Initiativen bundesweit die Rede, und die Stimmung drohte zu kippen. Am 13. April 1983 stoppte das Bundesverfassungsgericht das Volkszählungsvorhaben mit einer einstweiligen Verfügung. Am 15. Dezember schließlich hob es das gesamte Volkszählungsgesetz als verfassungswidrig auf. Im Zuge dessen verfügte es ein neues Grundrecht: Das „Recht auf informationelle Selbstbestimmung“. Dieses Recht wurde direkt aus Artikel 1 des Grundgesetzes und dem daraus entstehenden Persönlichkeitsrecht abgeleitet. Das Recht, selbst über die Herausgabe und Verwendung unserer personenbezogenen Daten zu bestimmen, ist seitdem die rechtliche Grundlage unseres Rechts auf Privatsphäre und ein tiefer kultureller Anker im Selbstverständnis der Deutschen.

Am 22. September 2013, dreißig Jahre später, wählten die Deutschen einen neuen Bundestag. Wieder war es eine aufwühlende Zeit, und wieder hatte sie mit dem Sammeln von Daten zu tun. Vier Monate davor hatte Edward Snowden mit seinen Enthüllungen rund um die Geheimdienstspionage von NSA und GCHQ begonnen. Wir lernten, dass niemand mehr von sich behaupten kann, informationell selbstbestimmt zu sein. Die Welt wird abgehört, immer und überall, jede ist betroffen. Die denkbar größte Privatsphärenkatastrophe wurde Realität. Aber während sich die Medien mit Berichterstattung und Aufklärung überschlugen und Internetaktivisten deutschlandweit aus dem Hyperventilieren nicht mehr herauskamen, interessierte das in der Bevölkerung kaum jemanden. Die konservative CDU, die so unsouverän und behäbig auf den Skandal reagierte, wie es überhaupt nur möglich war, ging gestärkt aus der Bundestagswahl hervor. Die liberale FDP, die wenigstens Aufklärungswillen gezeigt hatte, wurde stattdessen aus dem Bundestag gewählt. Alle Oppositionsparteien, die versuchten, den Skandal politisch gegen die Regierung zu nutzen, wurden abgestraft. Die Piratenpartei – zu deren Kernkompetenzen Fragen rund um Datenschutz und Überwachung gehören – verpasste mit 2,0 Prozent der Stimmen erneut den Einzug in den Bundestag.

Das Privacy-Paradox

Das Ergebnis der Bundestagswahl erinnert an ein Phänomen, das Wissenschaftler das „Privacy-Paradox“ nennen: In allen Umfragen und Interviews wird der Schutz der Privatsphäre als extrem wichtig angegeben. Zugleich aber führt das nur in den seltensten Fällen dazu, dass Menschen auch nur das Geringste dafür tun. In einer Studie [65] wurden zwei fiktive Online-Shops erstellt. Einer verlangte weniger persönliche Daten von den Kundinnen, dafür waren die DVDs dort einen Euro teurer als bei dem zweiten Shop, der sehr viel mehr über seine Kunden wissen wollte. Fast alle wählten den billigeren Shop. Sogar wenn die Preise bei beiden gleich hoch waren, entschied sich nur die Hälfte der Versuchspersonen für die datenschutzfreundliche Variante.

Wir sind anscheinend nicht bereit, für unsere Privatsphäre einen Preis zu zahlen, egal wie niedrig dieser Preis ist. Es besteht gesellschaftlicher Konsens darüber, dass uns der Schutz unserer Privatsphäre wichtig ist; doch offensichtlich ist kaum jemand in der Lage, dieses Mantra mit Inhalt zu füllen. „Im Zuge des gesellschaftlichen Durchbruchs digitaler Kommunikation geht die Unterscheidbarkeit zwischen privatem und öffentlichem Raum vielfach verloren, wie zum Beispiel die Praxis sozialer Netzwerke oftmals zeigt“, sagt Alexander Hensel vom Göttinger Institut für Demokratieforschung. „Der Umgang mit Privatsphäre verändert sich so im Alltag der Menschen, was einen Normenwandel in diesem Bereich vorantreibt. Dabei scheint der Wert des Privaten an Bedeutung zu verlieren.“ [66] Viele haben im Internet die Erfahrung gemacht, dass die Preisgabe eigener Daten fast immer ohne Konsequenzen bleibt, ja, dass sie sogar Vorteile bringt. So veröffentlichen sie Details aus ihrem Privatleben und bekommen dafür Zuspruch, Tipps, Kommunikation und Anteilnahme.

Echelon und Moore’s Law

Der aktuelle NSA-Skandal ist nicht der erste. Bereits im Jahr 2000 kam heraus, dass der US-Geheimdienst weltweit satellitengestützte Telefonate abhört. Das weltweite Netzwerk aus Funkstationen und Radarkuppeln hieß Echelon. Als der Untersuchungsausschuss, den das Europäische Parlament dazu einsetzte, seinen Bericht am 5. September 2001 vorlegte, wurden seine Resultate schnell von den Ereignissen des 11. September überlagert. Echelon hinterließ ziemlich tiefe Spuren im kulturellen Gedächtnis der Nerdkultur, aber praktisch keine politischen Konsequenzen.

Auch nach den Erkenntnissen, die uns Edward Snowdens Veröffentlichungen gebracht haben und weiter bringen, sind weder politische noch technische oder juristische Maßnahmen gegen die Überwachung zu erwarten. Im Gegenteil. Sie wird sich weiterhin in dem Maße ausbreiten, wie die Verdatung der Welt aufgrund der technischen Möglichkeiten voranschreitet. Zu Zeiten von Echelon wurde genau dasselbe belauscht wie heute: Alles.

Nur enthielt dieses Alles damals viel weniger als heute. Überwacht wird, was überwachbar ist – das heißt: die digitalisierten Lebensbereiche. Und diese Digitalisierung schreitet nach den Gesetzen Moore's voran, verdoppelt also alle 18 bis 24 Monate ihre Kapazität.

Der Kontrollverlust hat gerade erst begonnen. Er wird sich weiter in alle Ritzen des Alltags fräsen und keine Nische undigitalisiert lassen. Weder die staatliche noch die wirtschaftliche noch die private Überwachung wird sich in irgendeiner Hinsicht zurückdrehen lassen. Die informationelle Selbstbestimmung, die dreißig Jahre zuvor mit so viel Verve und Pathos erstritten wurde, ist grundlegend zerstört. Und an den Gedanken haben wir uns Schritt für Schritt gewöhnt. Vermutlich werden die Leute mit den Schultern zucken, wenn sie in zehn Jahren erfahren sollten, dass die Geheimdienste Sensoren in unseren Blutbahnen abfragen können und auch Gehirnscanner kurz vor der Einsatzbereitschaft stehen.

Unser digitales Leben wird nicht erst seit gestern, sondern seit mindestens zehn Jahren lückenlos überwacht. Würde die komplette Überwachung des Menschen seine Freiheit und Individualität so grundsätzlich infrage stellen, wie es von digitalen Bürgerrechtlern seit vielen Jahren suggeriert wird, dürfte sich in der westlichen Hemisphäre niemand mehr frei fühlen. Mit anderen Worten: Die Frage, ob wir mit der Totalüberwachung leben können, ist schon lange keine hypothetische mehr, sondern empirisch beantwortet: Ja, können wir, und wir tun es schon seit zehn Jahren.

Überwachung ist eine Gefahr

Auch wenn manche Dramatisierung und das eine oder andere Horror-szenario sich als unzutreffend herausgestellt haben, bleibt Überwachung – insbesondere staatliche Überwachung – ein gesellschaftliches Problem. Sie ist nach wie vor eine Gefahr für die Demokratie und das Zusammenleben. Kronzeuge hierfür ist J. Edgar Hoover. Der erste FBI-Chef sammelte Akten über alles und jeden und hatte bald genug Material zusammen, um alle mächtigen Menschen in den USA zu erpressen. Er war unangreifbar, das FBI wurde unter ihm zum Staat im Staate.

Auch wenn es sicher nicht das Hauptanliegen der NSA ist, muss Ähnliches für die NSA vermutet werden. Im Gegensatz zum damaligen FBI besitzt sie nicht nur Material über US-Politiker. Sie hat die theoretische Möglichkeit, kompromittierendes Material über Parlamentarierinnen, hohe Politiker und Staatschefinnen aller Länder zu sammeln. Die Geheimdienste sind eine Bedrohung für die Demokratie, und zwar weltweit.

Für viele Menschen ist die Überwachung eine sehr konkrete Bedrohung. Mit ihrer Hilfe werden die Drohnenkriege im Sudan, in Afghanistan und Pakistan geführt. Eine falsche Korrelation – jemand hat das falsche Fest besucht oder mit den falschen Leuten telefoniert –, und das eigene Haus liegt in Schutt und Asche. Vor allem Flüchtlinge vor den europäischen Grenzen sind jeden Tag Opfer von Überwachung. Eurosur heißt das geplante

europäische Flüchtlingsabwehrsystem, bestehend aus Drohnen, Satellitensuchsystemen, Aufklärungsgeräten, und einem zwischenstaatlichen Datenaustausch der jeweiligen Grenzbehörden, das illegale Einwanderer schon früh aufspüren soll. Bereits jetzt arbeiten private Sicherheitsfirmen wie Frontex an den Grenzen der EU mit Hochtechnologie.

Wer sich politisch engagiert, gerät auch in Deutschland schnell ins Fadenkreuz übereifriger Beamter. So erging es dem Stadtsoziologen Andrej Holm, der 2007 wegen eines unbegründeten Terrorismusverdachts verhaftet wurde und einige Monate unter verstärkter Überwachung stand – zusammen mit seiner ganzen Familie. BKA und Verfassungsschutz versuchen immer wieder linke Aktivistinnen zu unterwandern und durch Schikanen und Ermittlungen zu demoralisieren.

Staatliche Überwachung fängt aber nicht erst beim Geheimdienst an, sondern ist ein viel alltäglicheres Phänomen. Mithilfe von Informationszwangsabgaben werden Hartz-4-Empfänger drangsaliert. Dazu gehören die Offenlegung ihrer gesamten Eigentumsverhältnisse, Rechenschaft über ihre Anstrengungen zur Jobsuche und unangekündigte Hausbesuche. Der ständige Überwachungsdruck, gepaart mit existenziellen Konsequenzen durch die Agentur für Arbeit, kann Menschen über die Zeit zermürben. Es gibt nach wie vor viele plausible – und keineswegs neue – Gründe gegen Überwachung. Die NSA ist dabei aber nicht das Hauptproblem.

Strategien

Die Strategien, die sich direkt gegen Überwachung richten, sind gescheitert. Zwar lässt sich hier und da noch ein Erfolg verzeichnen, wie etwa das Kippen der Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof 2014. Aber im Grunde ist Vollüberwachung jetzt ein dauerhafter Zustand, mit dem wir leben lernen müssen. Gegen manche Dinge jedoch kann immer noch gekämpft werden.

Kampf den Strafregimen

Die Formel „Überwachung führt zu Unfreiheit, Nicht-Überwachung zu Freiheit“ gilt in dieser Pauschalität nicht mehr. Überwachung ist nicht an sich freiheitsraubend. Sie ist kein abstrakter, binärer Zustand, der entweder an oder aus ist. Stattdessen müssen wir Überwachung als eine konkrete Beziehung zwischen mindestens zwei Parteien begreifen. Wenn wir Überwachung skandalisieren, konzentrieren wir uns auf den Aspekt der Beobachtung. Wir fragen nur, wie umfassend die Beobachtung ist, der wir ausgeliefert sind. Die Gefahr durch NSA, Amazon oder Online-Werbefirmen beurteilen wir ausschließlich danach, welches Wissen sie über uns haben. Das ist kurzsichtig, denn wir übersehen damit die wichtige Rolle der Machtverhältnisse. Überwachung ist nicht gleich Macht, sondern Macht macht Beobachtung erst zur Überwachung. Die Machtverhältnisse entspringen nicht

einfach der Überwachung, sondern sie sind per se vorhanden. Überwachung ist einerseits Symptom dieser Machtverhältnisse – nicht alle Personen und Institutionen befinden sich in der Position, jemanden überwachen zu können – und dient ihnen andererseits als Werkzeug, um Macht abzusichern.

Obwohl entrüstete Passanten es bei der Polizei melden könnten, wenn wir auf dem Fahrrad telefonieren oder bei Rot über die Ampel fahren, hält uns das nicht davon ab, es trotzdem zu tun – vor den Augen einer Polizistin jedoch nicht. Obwohl wir wissen, dass die NSA auf unsere Google-Daten zugreift, berichten wir Freunden per Google Mail auch über Rechtsverletzungen. Wir kalkulieren immer das Risiko mit, das heißt die Wahrscheinlichkeit und Intensität von Strafe. So wie es ein Unterschied ist, ob ein Passant oder eine Polizistin mich mit Handy Fahrrad fahren sieht, ist es ein Unterschied, ob Google meine Daten sammelt, um mir Werbung anzuzeigen, oder das Bundeskriminalamt, weil es mich eines Verbrechens verdächtigt.

Macht über mich hat, wer mich disziplinieren kann. Disziplinierung muss nicht immer physische Gewalt beinhalten. Auch sozialer Ausschluss, Liebesentzug oder ein abschätziger Blick können disziplinieren, solange es eine Auswirkung auf mein Verhalten hat. Erst, wenn die Überwachenden mich für meine Handlungen zur Verantwortung ziehen können, werde ich ihre Beobachtung überhaupt als Freiheitseinschränkung erleben. Die Macht, mich zu bestrafen, wenn ich mich nicht gemäß den Vorstellungen der Überwacher verhalte, ist der entscheidende Unterschied zwischen Überwachung und Beobachtung.

Genau aus diesem Grund hat Überwachung nur bedingt etwas mit Privatsphäre zu tun. Dem Schriftsteller Ilija Trojanow wurde die Einreise in die USA vermutlich aufgrund seiner öffentlichen Äußerungen zum Thema Überwachung verwehrt, nicht wegen Details aus seinem Privatleben.[67] In Hamburg werden Menschen wegen ihrer Hautfarbe von der Polizei ins Visier genommen, um Flüchtige aus Lampedusa in ihrem Bewegungsradius zu kontrollieren. Diese Praxis heißt „Racial Profiling“; Hautfarbe ist nichts Privates. Britische Touristinnen, die für einen auf Twitter geäußerten Scherz, Marilyn Monroe ausgraben zu wollen, in den USA stundenlang verhört wurden,[68] verdanken ihre Drangsalierung keiner Verletzung ihrer Privatsphäre. Wenn unsere sexuelle Orientierung sich von der des Mainstreams unterscheidet, können wir versuchen, das geheim zu halten, um Diskriminierung zu entgehen. Aber ist das die Welt, in der wir leben wollen?

Für die überwachende Instanz ist es egal, ob sie mich wegen eines öffentlichen Tweets oder einer privaten E-Mail zur Verantwortung zieht. Wichtig ist nicht die Herkunft der Information, sondern ihre Konsequenz. Gäbe es so etwas wie eine intakte Privatsphäre, könnte sie uns nur dann vor Unterdrückung bewahren, wenn wir unsere potenziell anstößigen Eigenschaften und Meinungen in ihr verbergen. Würden wir öffentlich dazu stehen, wären wir trotzdem dran. Freiheit sieht anders aus.

Statt also die Privatsphäre gegen Beobachtung zu verteidigen, sollten wir gegen die

Instanzen der Bestrafung kämpfen: Autoritäre Grenzkontrollen, rassistische Polizeianordnungen, homophobe Strukturen in der Gesellschaft, ungerechte Gesundheitssysteme und institutionelle Diskriminierung sind die eigentlichen Problemfelder, auf denen Überwachung gefährlich werden kann. Der Staat selbst mit seinem Gewaltmonopol und seinem allumfassenden Regulierungsanspruch ist Quell der meisten Drohpotenziale, die durch Überwachung zum Freiheitsverlust führen können.

Gegenüberwachung

Der New Yorker Künstler und Aktivist Trevor Paglen betreibt Gegenüberwachung. Viele seiner Projekte machen Geheimdiensttätigkeiten sichtbar. So fährt Paglen zu geheimen Stützpunkten und fotografiert Spionage-Satelliten. Er sammelt und dokumentiert geheimdienstliche Rangabzeichen und veröffentlicht Flugrouten von CIA-Flugzeugen zu Gefangenenlagern. Die Informationen, die er dabei zusammenträgt, stellt er der Öffentlichkeit zur Verfügung. Seine Arbeit kann die Machenschaften der Geheimdienste zwar nicht aufhalten, aber doch ihren Handlungsspielraum einengen. Die Wirkung der Überwachung funktioniert auch andersherum: Wenn die Geheimdienste jederzeit Angst haben müssen, dass ihre Tätigkeiten aufgedeckt, mitgeschnitten und der Öffentlichkeit zur Verfügung gestellt werden, müssen sie Strategien anpassen und eventuell höhere Kosten sowie größere Risiken auf sich nehmen.

Die besten Beispiele für die Macht der Transparenz sind Chelsea Manning und Edward Snowden. Sie haben eindrucksvoll gezeigt, dass der Kontrollverlust auf der Seite des Whistleblowings arbeitet. Egal, wie mächtig eine Behörde oder ein Staat ist: Dort, wo die Macht auf Geheimnissen beruht, ist sie fragil und wird dadurch in Zukunft immer angreifbarer sein. Gegenüberwachung zeitigt bereits Resultate: Auf der Anti-Überwachungsdemonstration „Freiheit statt Angst“ im Jahr 2009 in Berlin zum Beispiel wurde ein Demonstrant von der Polizei verprügelt. Nachdem die Polizei erst alles abgestritten und dann behauptet hatte, die Täter könnten nicht identifiziert werden, wurde sie mit mehreren Videoaufnahmen aus verschiedenen Perspektiven konfrontiert, deren geballter Evidenz sie nichts mehr entgegenzusetzen hatte. Zwei Polizisten wurden schließlich verurteilt.

Im Juli 2013 wurde die Anklage gegen den deutschen Pfarrer Lothar König, einen Aktivisten der antifaschistischen Szene, fallen gelassen. Ihm war vorgeworfen worden, bei einer Demonstration gegen Rechtsextremismus in Dresden zum Landfriedensbruch aufgewiegelt zu haben. Im Laufe des Prozesses tauchten dann allerdings Videos von der Demonstration auf, die den Darstellungen der Polizei diametral widersprachen.

Das Sammeln von Daten hat grundsätzlich einen schlechten Ruf. Daten können uns belasten, uns unter Verdacht und sogar ins Gefängnis bringen. Doch das ist nur die eine Seite der Medaille. Wir haben diese einseitige Sicht auf Daten, weil Datenverarbeitung

lange Zeit ausschließlich von großen Institutionen wie dem Staat und großen Unternehmen betrieben wurde. Das hat sich heute geändert: Seit einigen Jahren sammeln, tauschen und verarbeiten wir alle Daten jeden Tag – und jeden Tag ein bisschen mehr. Konsequent weiterentwickelt heißt dieser Trend „Sousveillance“. Der Begriff wurde vom US-amerikanischen Forscher und Erfinder Steve Mann geprägt. Mann trägt seit 36 Jahren Apparaturen zur ständigen Aufzeichnung seiner Sinneswahrnehmung mit sich. Er ist sozusagen der Prototyp des Google-Glass-Trägers, lange bevor Google überhaupt existierte. Sousveillance ersetzt die Vorsilbe sur- (frz. für „über“) aus surveillance (Überwachung) durch sous („unter“) und könnte folglich mit „Unterwachung“ übersetzt werden. Sie ist die Überwachung der Überwacher von unten.

Durch immer kleinere und billigere Aufzeichnungsgeräte entwickelte sich Sousveillance schon vor dem Start von Google Glass zur Anti-Überwachungsstrategie. In Quebec, Kanada, wurden 2007 die Polizeianordnungen reformiert, nachdem ein Youtube-Video zivile Beamte der Polizei enttarnte, die sich unter die Demonstranten gemischt hatten, um die Demonstration zu eskalieren (sogenannte Agents Provocateurs). Auch das Video, das Polizisten zeigt, wie sie ohne vorausgegehende Provokation Studierende der Universität von Kalifornien in Los Angeles (UCLA) mit Tasern malträtieren, hatte politische Auswirkungen. Den größten Zulauf bekam die Protestgruppe #OccupyWallStreet, nachdem Videos und Fotos von Polizeigewalt gegen sie im Netz auftauchten.

Post-Privacy: Selbsttransparenz als stoische Übung

Christian Heller schlägt in seinem Buch „Post-Privacy – Prima leben ohne Privatsphäre“ eine noch radikalere Strategie vor: sich ganz von der Privatsphäre zu verabschieden und die unvermeidbare Transparenz zu umarmen. Er zeigt auf, dass die Privatsphäre, wie wir sie bislang kennen, für eine historisch recht neue Form des Zusammenlebens charakteristisch ist – und dass sie nicht nur Vorteile gebracht hat. Die Privatsphäre war zum Beispiel lange Zeit auch der Ort der Unterdrückung der Frau. Dagegen beweise die Homosexuellenbewegung, dass sich gesellschaftlicher Fortschritt vor allem erzielen lasse, wenn eigentlich private Details öffentlich gemacht werden. Da wir es sowieso nicht schaffen werden, den technologischen Fortschritt aufzuhalten, sollten wir uns besser an den Gedanken der totalen Transparenz gewöhnen, meint Heller.

Heller lebt dieses Modell selbst. Er dokumentiert seinen Tagesablauf, seine Finanzen und viele seiner privatesten Informationen in einem öffentlich einsehbaren Wiki.[69] Das ließe sich leicht als reiner Selbsterfahrungstrip abtun – wenn dahinter nicht offenbar würde, dass Heller nur das radikalisiert, was durch die sozialen Medien sowieso immer mehr zur Norm wird: Früher private Belange werden gezielt mit der Öffentlichkeit geteilt.

Nur macht Heller sich dabei im Gegensatz zu den meisten Menschen beispielsweise auf Facebook nicht vor, er kontrolliere selber seine Daten. Er ist sich sehr bewusst, dass sie von jedem jederzeit für alle Zwecke ge- und missbraucht werden können. Insofern passt die Post-Privacy-Strategie zu Nikolas Talebs Diktum der Antifragilität: Post- Privacy zu praktizieren, wirkt wie eine stoische Übung: Wer von vornherein vom schlimmstmöglichen Szenario ausgeht – in unserem Fall also davon, dass alle Informationen öffentlich sind – wiegt sich nicht in falscher Sicherheit, sondern bereitet sich vor auf den Fall, in dem die maximale Öffentlichkeit tatsächlich eintritt. Ständig im Hinterkopf zu haben, dass auf alle Daten zugegriffen werden kann, reduziert die Angst und damit auch die Wirkung von Überwachung.

Es gibt keine Privatsphäre mehr, es gibt nur noch Verschlüsselung

„Verschlüsselung funktioniert. Korrekt implementierte, starke Krypto-Systeme gehören zu den wenigen Dingen, auf die wir uns verlassen können.“ Das sagte Edward Snowden in einer Frage- und-Antworten-Runde der britischen Zeitung The Guardian. [70] Von all den fragilen Strategien der Datenkontrolle ist gute Verschlüsselung die wahrscheinlich am wenigsten schlechte. Ende-zu-Ende-Verschlüsselung erfordert nicht, dass ich einem externen Dienstleister oder gar dem Staat vertrauen muss, dass sie meine Daten schützen. Ich muss an dieser Stelle nur der Technik vertrauen, dass niemand zwischen mir und meinem Kommunikationspartner die Daten entschlüsseln kann. Die Mathematik hinter den Verschlüsselungsalgorithmen gilt weiterhin als bombenfest. Selbst mit heute noch unvorstellbaren Superrechnern bräuchten diese zur Entschlüsselung einer einzigen E-Mail viele Tausend Jahre.

Das Problem ist weniger die Mathematik als die Integration der Software in E-Mail-Programme, Server oder Chats. Denn dorthin verschieben sich die Gefahren: Die Daten können zum Beispiel vor der Verschlüsselung oder nach der Entschlüsselung im Klartext ausgelesen werden. Hierbei kommt es immer wieder zu Fehlern oder zum gezielten Einbau von Hintertüren durch Hacker oder Geheimdienste. Verschlüsselung ist vor allem für Leute geeignet, die bereit und fähig sind, viel Wissen und Können zu versammeln. In gewisser Weise ist es eine Elitenlösung. Es ist niemandem zu wünschen, sich auf Verschlüsselung verlassen zu müssen, aber für alle, die auf vertrauliche Kommunikation angewiesen sind, ist es immer noch die beste – wahrscheinlich einzige – Methode im Internet so etwas Ähnliches wie Privatsphäre herzustellen.

Anhang

Literaturverzeichnis

Teil II – Zehn Regeln für das Neue Spiel

Regel 2 | Die Überwachung ist Teil des Spiels

Wikipedia, Echelon: http://de.wikipedia.org/wiki/Echelon
Wikipedia, J. Edgar Hoover: http://de.wikipedia.org/wiki/J._Edgar_Hoover
Wikipedia, Andrej Holm: http://de.wikipedia.org/wiki/Andrej_Holm
Wikipedia, Travor Paglen: http://de.wikipedia.org/wiki/Trevor_Paglen
Wikipedia, Steve Mann: http://de.wikipedia.org/wiki/Steve_Mann
Wikipedia, Sousveillance: http://de.wikipedia.org/wiki/Sousveillance
Christian Heller, Post-Privacy – Prima leben ohne Privatsphäre, München 2011.
Wikipedia, Asymmetrisches Kryptosystem: http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem

Impressum

Michael Seemann: Das neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust
ISBN 978-3-944362-21-2
Web: http://irights-media.de/publikationen/michael-seemann-mspro-das-neue-spiel/
Erschienen im Oktober 2014

Verlag

iRights.Media
Philipp Otto
Almstadtstr. 9-11
10119 Berlin
Kontakt: info@irights-media.de
www.irights-media.de

Redaktion iRights.Media: Valie Djordjevic
Gestaltung E-Book: Margarethe Giesler | www.typearea.de

Cover: Katharina Gabelmeier
Korrektorat: Christoph Trunk, Hans Jürgen Kugler

„Das neue Spiel“ erscheint gedruckt bei orange-press <http://www.orange-press.com/>
ISBN 978-3-936086-79-9.

Lizenz

65 Alastair R. Beresford, Dorothea Kübler, Sören Preibusch, „Unwillingness to pay for privacy: A field experiment“, in: Economics Letters, Elsevier, Vol. 117(1), S. 25-27, http://ideas.repec.org/p/iza/izadps/dp5017.html

66 Gespräch mit dem Autor.

67 Ilija Trojanow, „Willkür und Freiheit“, in: FAZ, 1.10.2013, http://www.faz.net/aktuell/feuilleton/buecher/autoren/einreiseverbot-fuer-ilija-trojanow-willkuer-und-freiheit-12599490.html

68 Rob Beschizza, „Tourists deported from U.S. for Twitter jokes (Updated)“, http://boingboing.net/2012/01/30/brits-deported-from-u-s-for-t.html

69 Christian Heller, „PlomWiki“, http://www.plomlompom.de/PlomWiki/

70 Edward Snowden, „NSA whistleblower answers reader questions“, 17.6.2013, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower