IV. Corpus Mundi: Die technologische Verkörperung der Globalität

Technologische Innovationen in den Bereichen Informations- und Kommunikationstechnologie, Gen- und Nanotechnologie, Gesundheitstechnik, Logistik und Weltraumtechnologie, Medienentwicklung oder Verkehrstechnologie bilden die Antriebsmotoren der neuen Globalisierung (Steinmüller/Steinmüller 2006). Entstanden ist so ein technologischer Organismus, der die Stofflichkeit und Begrenztheit der realen Welt durch eine neue Dimension erweitert. Technologie formt die Globalisierung zu einem neuartigen Corpus Mundi. Als Metapher drängt sich das Bild des menschlichen Nerven- und Durchblutungssystems auf, das über die Nervenzellen, Gliazellen und die Blutbahnen sowie besonders die Herzkranzgefäße die einzelnen Teile eines Organismus in einen Zusammenhang bringen. Ohne Blutbahnen gibt es kein Leben für den Organismus, ohne Nervenzellen keine Information. Das Nervensystem übernimmt dabei die Aufgabe, den Organismus mit Sauerstoff zu versorgen sowie Veränderungen der äußeren und inneren Umwelt als Signale zu erkennen, aufeinander zu beziehen und schließlich Reaktionen zu veranlassen. Das Nervensystem hält somit die Interaktion aller Teile des Organismus in Gang. Durch Steuerung der Konzentrationen von Ionen und Transmittern sowie der Regulation des lokalen Blutflusses, von dem Sauerstoffversorgung und Verfügbarkeit hormonaler Neuromodulatoren abhängen, beeinflussen sie auch die Signalweitergabe von Neuron zu Neuron. Im Verlauf der Evolution ist eine Tendenz zur Konzentration und Spezialisierung von Teilen des Nervensystems beim Menschen festzustellen. 5,8 Millionen Kilometer lang sind die Nervenbahnen eines Gehirns. Damit ließe sich die Erde 145 Mal umwickeln. Sie verbinden etwa 100 Milliarden Nervenzellen, die wiederum durch 100 Billionen Synapsen miteinander verknüpft sind.[1]

Bleibt man bei diesem Bild, ist die Globalisierung ein weiterer Schub in der Evolution des Weltsystems. Bodenschätze, Klima, Energie- und Nahrungsmit-

1 | Vgl. Süddeutsche Zeitung vom 2./3. Mai 2015.

telvorräte sind die Ressourcen des Organismus Mensch – Erde. Siedlungsformen wie Megacities und ihre hochkomplexen technologischen Organisation sind Herz und Gehirn der Weltgesellschaft. Sie treiben den Puls der Globalisierung über die Nervenbahnen und koronaren Kranzgefäße von Servern, Glasfaserkabeln, Info-Highways, Satellitenverbindungen, Schiffsrouten, Autobahnen und ihren Schnittstellen sowie Endgeräten und Transportmitteln an.

1. Eine Infrastruktur der Superlative

Das Internet zählt (1.) dabei zu denjenigen Technologien, die das Zusammenleben der Menschen nicht nur verändert, sondern über die qualifizierte Summe seiner einzelnen Teile revolutioniert. Ohne das Netz gäbe es die neue Globalisierung nicht. Vom Einzelhandel über die Börse, Banken und Rohstoff- oder Devisengeschäfte über zahllose private Nutzungen bis hin zur Politik hat das Internet die gesamte Gesellschaft total verändert (Castells 2002, 2003a, 2003b). Dabei geht es nicht nur um die Bereitstellung einer neuen Superinfrastruktur in der Welt; im Angesicht all der neuen Möglichkeiten und Versuchungen löst die Netzwerkgesellschaft einen gewaltigen Adrenalinschub für alle möglichen Formen menschlicher Interaktionen aus. Sie rationalisiert oder verbessert viele Angelegenheiten, so dass eine Menge an Umständlichkeiten, Zeitverlusten oder Anstrengungen im Alltag entfallen. Dies können Behördengänge sein, Kommunikationen mit Krankenkassen oder auch die Versorgung mit den Sachen des alltäglichen Lebens. Bemerkenswert hierbei ist der Schub in der Evolution im Gesundheitswesen, der im wesentlichen über Informations- und Kommunikationstechnologien getrieben und allgemein als der 6. Kondratief der Industriegesellschaft bezeichnet wird. Angesichts des demographischen Wandels kommt diesem Schub ohnehin eine besondere Bedeutung zu, da er die Versorgungssituation älterer Menschen erleichtern oder verbessern kann und im übrigen Treiber eines digital getriebenen Wirtschaftswachstums werden wird.

Augenfällig ist das veränderte Konsumverhalten vieler Menschen. 2011 lag die Zahl der Personen, die Waren und Dienstleistungen im Internet über das Mobiltelefon bestellten bei 18,2 Millionen. Online-Singlebörsen setzten bereits 2011 mit 202,8 Millionen Euro gegenüber 2003 das zwanzigfache um. Die weltweiten Ausgaben für digitale Werbung betrugen 2011 rund 76 Milliarden US-$ gegenüber zehn Milliarden US-$ im Jahr 2000 (Schönbohm 2013). Grundlage für das Netz ist die Digitalisierung der Information, die einen hohen Datenaustausch in Lichtgeschwindigkeit ermöglicht und theoretisch an jedem Ort der Welt verfügbar ist. Was hierbei zählt: nicht nur der veränderte Konsum prägt das Netz. Das Netz prägt auch den Konsum, der nicht nur eine sachliche Entscheidung für den Erwerb von Waren und Dienstleistungen ist, sondern auch eine emotionale Hinwendung sein kann für die Umstände ihrer

Produktion oder ihren immateriellen Wert. ›By politically correct‹ ist zum Beispiel eine Errungenschaft der Globalisierung der Information, das gelegentlich totale seelische Abtauchen von Menschen in die virtuelle Welt der Avatare im Kosmos von ›World of Warcraft‹ dagegen für den ein oder anderen ein problematisches Nebenprodukt.

Der Neurologe Manfred Spitzer warnt in diesem Zusammenhang gar vor der Entstehung einer digitalen Demenz. Wenn man Demenz als eine Entrückung aus Gegenwart und Vergangenheit versteht, dann kann man verstehen dass der Gehirnforscher – der mit seinen Thesen in Deutschland nicht unumstritten ist – eine Warnung ausspricht vor den manipulativen Wirkungen von zu viel Fernsehen, Surfen und Computerspielen (Spitzer 2012). Nach seiner Meinung kommt hinzu, dass das Internet zudem der Größte Rotlichtbezirk und der größte Tatort unserer Zeit geworden sei, so dass zusätzlich zur digitalen Entrückung kriminelle Verführungen das Internet füllten.[2] Das Internet gründete fast still und zunächst bescheiden eine neuartige und fundamentale Grundstruktur für die wesentlichen Interaktionen einer Gesellschaft. Hier entstanden die Bahnen der elektronisch organisierten Information und somit Räume der Rationalisierung, Optimierung und Veränderung von gesellschaftlichen Sachverhalten. Hinzu kamen seine kommerziellen Subsysteme, seine militärische Verwendung und die hohe Zahl der Intra-Netze in Unternehmen und Institutionen.

Das Internet der Dinge erschafft eine selbstständig agierende technologische Umwelt

Die Entwicklung des Internet erreicht mit dem ›Internet der Dinge‹ (Internet of Things, IoT) nun eine neue Dimension der digitalen Revolution (Fleisch/Mattern 2005; Ashton 2011; Andelfinger/Hänisch 2014). Das Internet der Dinge bezeichnet die Verknüpfung physischer Objekte mit einer virtuellen Repräsentation in einer elektronisch vernetzten Struktur. Das Internet besteht also nicht mehr ›nur‹ aus menschlichen Teilnehmern (Subjekten), sondern auch aus Dingen (Objekten), die in eine Interaktion mit Folgen und Ergebnissen eintreten. Mit dem Internet der Dinge geht es um die Verknüpfung von allem und jedem unter möglicherweise völlig neuen Vorzeichen. Dabei setzt nun ein Wettlauf ein mit dem Ziel, das goldene Zeitalter des Internet der Dinge gut gerüstet zu betreten oder, vielleicht sogar, zu beherrschen.

2 | So Manfred Spitzer in der ZDF-Talkshow »Lanz« am 27. Oktober 2015.

Das magische Zauberwort des Internet der Dinge für die Wirtschaft ist: Industrie 4.0

Durchsetzen wird sich nicht mehr derjenige, der die besten Produkte baut, sondern derjenige, der die interessantesten und leistungsstärksten Servicepakete anbietet. Mehr noch: derjenige, der überhaupt völlig neue Geschäftsideen hat (Beise/Schäfer 2015a). Das Internet der Dinge findet heute bereits in fast allen Lebens- und Arbeitsbereichen statt. Das wohl prominenteste aber auch simpelste Beispiel dafür ist der Kühlschrank, der nach den Bedürfnissen seines Besitzers Füllstände und Vorräte überprüft und gegebenenfalls selbstständig Ersatz ordert. Oder Fitnessarmbänder, die mit der Cloud kommunizieren, bis zu Parksensoren, die Informationen für übergeordnete Parkleitsysteme bereitstellen und Verkehrsflüsse besonders in großen Städten optimieren können.

Das interessanteste Betätigungsfeld im Internet der Dinge ist aber die Industrie, die verglichen mit den industriell revolutionierenden Produktionsprozessen des 19. und 20. Jahrhunderts mit der Industrie 4.0 nun einen weiteren Schub der digitalen Revolution umsetzen wird (Bauernhansl/ten Hompel 2014). Ein Beispiel dafür ist das selbststeuernde Automobil, das 2015 auf der Industriemesse in Las Vegas von dem Automobilhersteller Mercedes Benz als Prototyp präsentiert worden ist. Google hat ähnliche Pläne und strebt ebenfalls die Herstellung eines vollautomatischen Autos an. Während die Industrie 3.0 davon geprägt war, erstklassige Produkte automatisiert herzustellen, geht es in der Industrie 4.0 nun um eine intelligente Verknüpfung der automatisierten Produktion erstklassiger Produkte mit erstklassigen digitalisierten Prozessen oder Dienstleistungen. Zukunftskonzepte von Cyber-physischen Systemen und dem Internet der Dinge in der Produktion sprechen von komplett vernetzten, sich selbst organisierenden Produktionssystemen mit dem Ziel der ›Smart Factory‹. Im Internet der Dinge werden 2020 rund 50 Milliarden Dinge angeschlossen sein, nicht bloß Smartphones und Tablets, sondern auch Maschinen, Autos, Kraftwerke, Roboter, Verkehrstechnik, Fabriken. Und der Mensch, der die Kommunikation der Dinge im Auge zu behalten hat. Lange Zeit galt das zuverlässige Steuern von industriellen Prozessen als Hauptaufgabe in der Automatisierung. In der Industrie 4.0 geht es nun darum, Applikationen und Logiken aufzusetzen, die es ermöglichen, Ressourcen zu sparen, effektiver zu werden und flexibler zu produzieren.

Dabei spielt die intelligente Robotik eine immer stärkere Rolle. Auf 1.000 Mitarbeiter kommen in der deutschen Automobilindustrie derzeit 114 Roboter. Der Karosseriebau ist heute ausnahmslos in der Hand von Maschinen. Sie schweißen, kleben oder schneiden die Stahlteile so exakt und schnell, wie dies keinem Menschen gelingen kann. Im nächsten Schritt werden Maschinen mit Maschinen interagieren. Sie erkennen sich gegenseitig, tauschen sich aus, lernen und erarbeiten gemeinsam Lösungen. Findet ein Roboter einen Defekt, re-

pariert ein anderer Roboter das kaputte Teil oder ersetzt die defekte Maschine durch eine neue oder bessere Maschine. Die Folge dabei ist, dass in der roboterisierten Produktion erhebliche Produktivitätssprünge zu verzeichnen sind. Aufsehen erregte 2015 ein Projekt, mit dem die chinesische Firma Changying Precision Technology Company fast alle menschlichen Arbeitsplätze zugunsten von roboterisierten Fertigungsfeldern wegrationalisiert hat. Der Mensch spielt bei dieser Firma fast keine Rolle mehr. »Roboter ersetzen Menschen« heißt das firmeneigene Programm. In der chinesischen Stadt Dongguan, wo das Unternehmen seinen Sitz hat, sollten bis 2016 bis zu 1.500 solcher Programme umgesetzt werden. Ein Roboter ersetzt dabei den Job von sechs bis acht Menschen. Früher fertigten in der Fabrik 650 Menschen Telefonmodule. Nun sind es nur noch 60, demnächst sollen es nur noch 20 sein. Ihre Arbeit haben 60 Roboter übernommen. Durch die Umstellung ist die Fehlerrate in den Produkten von 25 Prozent auf fünf Prozent gesunken.[3]

In der Smart Factory der Industrie 4.0 kommunizieren Maschinen, Infrastrukturen und Produkte selbstständig in einer sich selbst organisierenden Netzstruktur

Mit anderen Worten: angestrebt wird die ›Smart Factory‹, in der Maschinen und Produkte miteinander kommunizieren, sich selbstständig reparieren oder Nachschub bestellen, Kunden und Geschäftspartner in den Prozess der Produktion mit einbeziehen und – vor allem – lernen und das Gelernte behalten und im Rahmen intelligenter ›Denkprozesse‹ optimieren! Es geht also um weit mehr als eine weitere Stufe der Computerisierung. Industrie 4.0 erfasst dabei alle Bereiche der produzierenden Wirtschaft und moderner Dienstleistungen. Während sich einerseits im produzierenden Bereich alle Blicke auf die Realisierung der ›Smart Factory‹ richten, arbeiten auch Dienstleister wie Banken, Versicherungen, Unternehmensberatungen, Krankenkassen und Kommunikationsunternehmen oder Werbeagenturen bereits am ›Smart Service‹ der Zukunft.

Ein anschauliches Beispiel dafür bietet die Entwicklung im Banken- und Versicherungsbereich. Maschinen fragen in Zukunft den Anleger, wie viel er mit seinem Geld verdienen will und wie viel Geduld er dabei mitbringt. Nach diesen Anforderungen durchforstet der ›Assistent‹ den Kapitalmarkt. Er stößt Aktien ab, die an Wert verlieren, sucht den Ausgleich bei steigenden Papieren und zwar so, dass die Steuerlast bei möglichen Gewinnen möglichst gering

3 | Vgl. »China sets up first unmanned factory; all processes are operated by robots«, in: The Economic Times vom 27. Juli 2015 unter http://economictimes.indiatimes.com/news/international/business/china-sets-up-first-unmanned-factory-all-processes-are-operated-by-robots/articleshow/48238331.cms, aufgerufen am 1. August 2015.

bleibt. Solche Maschinen sind nicht nur schnell. Sie reduzieren alle Fragen zur Geldanlage auf eine nüchterne Kosten-Nutzen-Analyse. Frei von Emotionen, frei von Fehlern, wie sie Menschen gelegentlich machen (Bernau 2015). Allerdings: es ist nicht wie das Duell zwischen Mensch und Maschine beim Schach, wo der Mensch gegen die Maschine kaum noch eine Chance hat. Rein statistische Sachverhalte im Rahmen von Charts werden von Algorithmen heute für automatisch ablaufende Transaktionen an den Kapitalmärkten bewertet und durch Kauf- oder Verkaufsorders abgeschlossen. Die vielschichtigen psychologischen Komponenten des internationalen Kapitalmarktes und menschliches Verhalten können Algorithmen in absehbarer Zeit wohl kaum kalkulieren, es sei denn, dass dies auch in ein differenzierteres Kalkül der Maschinen und Programme integriert werden könnte.

Ein entsprechendes Szenario entwarf dabei die schweitzer Bank UBS. Ihr ›Think Tank‹ UBS Y arbeitet an der Frage, ob man eine Bank ohne Menschen betreiben könne. Die Idee dahinter ist: wenn mit dem Einsatz von Big Data – also dem Einsatz von Algorithmen –, der Cloud und smarten Technologien Google, Mercedes und Toyota Autos bauen können, die keinen Fahrer mehr brauchen, dann könnten Banken doch ohne Personal auskommen?[4]

Die Industrie 4.0 ist der Tsunami einer zweiten industriellen Revolution im 21. Jahrhundert

Die Industrie 4.0 wird zunehmend relevant. Es geht dabei um die digitalisierte Produktion der Zukunft. Dies erfasst in Deutschland und Europa sowie weltweit die gesamte Industrie. Auf ihr lastet einerseits der Druck, smarter, günstiger, innovativer zu sein als die internationale Konkurrenz; andererseits machen im Rahmen der intelligenten Digitalisierung die potenziellen Umwälzungen der industriellen Möglichkeiten auch deutlich, wie sehr sich das Bild industrieller Produktion im 21. Jahrhunderts ändern wird. Allerdings deutet heute wenig darauf hin, dass die gesamte deutsche und europäische Wirtschaft das revolutionäre Potenzial in vollem Umfang erkennt und strategisch für die kommenden 20 bis 30 Jahre entsprechend disponiert. Diese Aufgabe avanciert nach allgemeiner Meinung zu einer der gewaltigsten Aufgabe der Industriegesellschaften im digitalen Wandel.

John Chambers, der Vorstandsvorsitzende des Internetausrüsters Cisco im amerikanischen Silicon Valley hat das revolutionäre Potenzial der Industrie 4.0 betont und deutete die seiner Ansicht nach mangelnde Umsetzung an einem so hervorragenden Industriestandort wie Deutschland an.[5] Dabei rech-

4 | Vgl. www.finews.ch/news/banken/19329-ubs-y-daniel-ott-menschen-personal-maschine-computer-szenario, aufgerufen am 21. September 2015.

5 | Vgl. Süddeutsche Zeitung vom 28. November 2014.

nen die Amerikaner damit, dass die Effekte des Internet der Dinge noch größer sein könnten als die des uns bekannten und nunmehr vertrauten Internet, das vornehmlich Menschen zusammengeführt hat und keine Maschinen mit künstlicher Intelligenz (Brynjolfsson/McAffee 2014). Cisco hat errechnet, dass Deutschland in den nächsten Jahren von der konsequenten Wende hin zur intelligenten Vernetzung der Industrie mit 700 Milliarden Euro zusätzlicher Wertschöpfung profitieren kann. Das wäre ein Wachstum der Volkswirtschaft von zwei Prozent pro Jahr – zehn Jahre lang! Das sei für Investoren einfach unwiderstehlich.

Wirtschaft und Öffentlichkeit sind nach Meinung von Unternehmungsberatungen auf die Industrie 4.0 schlecht vorbereitet …

Zwei Studien der Unternehmensberatungen Roland Berger und McKinsey haben in diesem Sinne 2015 Defizite der Umsetzung der digitalen Möglichkeiten für die Wirtschaft in Deutschland und Europa moniert. Verglichen mit den USA sei die digitale Landschaft in Europa zersplittert und geprägt von der Heterogenität der Akteure. Eine entscheidende Voraussetzung des Bestehens in der digitalen Welt sei eine effektive Allianz von Innovatoren, Wagniskapital (Venture Capital) und Talenten. Diese Innovationskultur sei hierzulande wenig ausgeprägt. In Zusammenarbeit mit dem Bundesverband der deutschen Industrie (BDI) untersuchte Roland Berger in der Studie »Die digitale Transformation der Industrie« Ursachen und Auswirkungen der Digitalisierung auf die Industrie in Deutschland und Europa und erkannte Defizite bei der digitalen Reife. McKinsey stellte in seiner eigenen Studie »Industry 4.0 – How to navigate digitalization of the manufacturing sector« fest, dass sich nur sechs von zehn Unternehmen in Deutschland gut vorbereitet fühlen. Viele Unternehmen fingen erst jetzt zögerlich an, sich konkret mit der Industrie 4.0 auseinanderzusetzen. Vorteile der digitalen Technologien wie 3D-Drucker, Big Data und Internet würden zu oft als Risiko und nicht als Chance gesehen. Diese Kritik griff dann auch der Wirtschaftsrat der CDU in Deutschland mit einer Stellungnahme auf. Er forderte, ein »digitaler Ruck« müsse durch Deutschland und Europa gehen. Der Rat vermisst in einem Positionspapier alles das, was Deutschland in einer digitalen Welt wettbewerbsfähig macht. Viele Firmen riskierten, ihre Wettbewerbsfähigkeit zu verlieren, wie es bereits in den Bereichen Musik, Medien, Reisedienstleistungen oder Einzelhandel geschehen sei (Wirtschaftsrat Deutschland 2015).

… was allerdings nicht die ganze deutsche Wirtschaft betrifft

Diese generelle Kritik betrifft allerdings nicht die gesamte Wirtschaft. Gerade deutsche Firmen haben begriffen, dass die Zukunft der Digitalisierung nicht

in der Entwicklung von Apps oder Gadgets[6], sondern in der großformatigen Einbeziehung der digitalen Netzwerkstrukturen in industrielle Produktionsprozesse liegt. In Deutschland bieten dafür die ›Hidden Champions‹ des Mittelstands und die großen Technologiekonzerne wie Siemens oder Bosch mit ihrem Know-How und ihren Technologieerfahrungen die besten Voraussetzungen. BMW oder Siemens arbeiten deshalb an der Smart Factory der Zukunft. Joe Kaeser, Vorstandsvorsitzender von Siemens, bringt die Kernproblematik der Adaption der amerikanischen Innovationspotenziale in Deutschland auf den Punkt wenn er sagt: »wir müssen das Silicon Valley nicht kopieren, aber kapieren« (Beise/Schäfer 2015b). Insofern werden viele industriellen Aktivitäten in Deutschland nicht bemerkt, sind aber, wie die digitalen Vernetzungsaktivitäten der Deutschen Bahn (DB), des Hamburger Hafens oder der Firma Klöckner, für eine zeitgemäße Digitalisierung industrieller Produktionsprozesse zielführend. Früher nahm der Stahlkonzern Klöckner zum Beispiel Aufträge nur per Telefon und Fax entgegen. Nun dient dazu eine digitale Handelsplattform für etwa 15.000 Stahlprodukte. Klöckner will nach eigenem Bekunden in Zukunft eine Art Amazon für den Stahlhandel sein (ebd.).

Der Mensch nutzt mit der globalen Kommunikationsstruktur im Wasser, in der Atmosphäre und im Weltraum entsprechend den heute gegebenen technologischen Möglichkeiten derzeit gut aus

Flankiert wird das Netz (2.) durch die kontinuierliche Entwicklung der weltweiten Kommunikation über Kabel, Mobilfunk oder Satellit. Besonders das All ist als Ort der globalen Kommunikation von wachsender Bedeutung. Seitdem Russland am 4. Oktober 1957 seinen ersten Sputnik-Satelliten ins Weltall geschossen und den sich technologisch überlegen wähnenden Westen geschockt hatte, und damit das Zeitalter der Erdsatelliten anbrach, sind über 3.000 Satelliten in ihre Umlaufbahn gebracht worden. Abzüglich der enormen Verschleißerscheinungen weltraumbasierter Technologien und das exorbitant gewachsene Problem des Weltraumschrotts sind hiermit wichtige Voraussetzungen für eine globale Verknüpfung der Menschen über Information, Kommunikation und Orientierung gelegt worden.

Mit der Vernetzung über das amerikanische GPS-System erreichte die Welt in den 2000er Jahren eine dichte technische Infrastruktur im Weltraum, die momentan mit dem europäischen Gallileo-Programm komplettiert (bzw. konfrontiert) wird. Diese ermöglicht eine flächendeckende zivile und militärische Nutzung und ist ein weiteres, mächtiges Symbol der neuen Globalisierung. Die

6 | Apps sind Applications, also mikroelektronische Anwendungen, Gadgets bezeichnen die Palette von Geräten, die die Benutzung von Apps ermöglichen (also Smartphones, Tablets oder Laptops).

Digitalisierung ermöglicht hier eine optimierte Verbindung unterschiedlicher Informations- und Kommunikationssysteme. Ihr globalisierender Charakter entsteht durch das Verschmelzen der Informations- und Kommunikationstechnologien (IKT) über stationäre und mobile Computer, Satelliten, Smartphones, Tablets, Notebooks und digitale Datenautobahnen.

Die gigantischen ›Zwerge‹ der Nanotechnologie

Ein hoch innovativer Teil der IKT ist die Nanotechnologie (oft auch als Nanotechnik bezeichnet und aus dem Griechischen von »Nano = Zwerg« abgeleitet). Diese Technologie wird als Fortführung der Mikrotechnik bezeichnet, die völlig neue Ansätze in der Verkleinerung von Mikrostrukturen in »Bottom-Up-Ansätzen« verfolgen (also Ansätze, die im Gegensatz von »Top-Down-Ansätzen« von ›unten kommend‹ kleinste Verbindungen herstellen, die sich dann zu größeren Molekularstrukturen aufbauen). In der Chemie etwa werden so aus einer Vielzahl von einzelnen Moleküleinheiten nanoskalige Molekülverbände aufgebaut.[7] Die Nanotechnologie wiederum weist vielfältige Querverbindungen zu anderen Basistechnologien auf. Sie ist ein weiteres Vernetzungskennzeichen der neuen Globalisierung. Bei der Nanotechnologie handelt es sich um die Miniaturisierung der Informationstechnologie. Der Nanometer-Bereich ist der natürliche Treffpunkt von Biologie, Chemie und Physik. Er verbindet die Wissenschaftszweige der modernen Informations- und Biotechnologie. Wichtig und interessant ist er mit Blick auf die Materialwirtschaft, in der Computertechnik, in der Robotik, der Medizintechnologie und im Bereich der künstlichen Intelligenz (KI). In der Medizintechnik spielt die Nanotechnik eine zunehmend wichtige Rolle: Nanoroboter können sich durch verkalkte Adern fressen, implantierte Biochips die Gesundheit überwachen und Minicomputer tauben oder blinden Menschen Teile ihrer fehlenden Fähigkeiten ersetzen. Schon seit längerem ist es möglich, Taubheit durch ein elektronisch arbeitendes Implantat zu überwinden. Es ist direkt mit dem Gehörnerv des Behinderten verbunden. Vor 20 Jahren war dies Zukunftsmusik; heute sind solche Hilfestellungen eine Selbstverständlichkeit. Nanotechnologie nährt große Erwartungen hinsichtlich der Materialforschung oder der Schaffung künstlicher Intelligenz. Sie schürt aber auch Ängste hinsichtlich einer unkontrollierten Nutzung und Verbreitung.

7 | Vgl. http://de.wikipedia.org/wiki/Nanotechnologie, aufgerufen am 24. Mai 2014.

Mit der Nanotechnologie verbindet die Wissenschaft revolutionäre Lösungen für die Verbesserung von Zivilisationsproblemen im 21. Jahrhundert

Erfinder und Transponder des Begriffs ist Eric Drexler, der sich 1986 mit seinem Buch »Engines of Creation« aufmachte, um die Mikrowelt des Nanobereichs zu erkunden und ihren Nutzen für den Menschen und die Zivilisation zu untersuchen (Drexler 1986). Nanotechnologie steht für die Erwartung, dass man in den Bereichen Clusterphysik, Halbleiterphysik, in der Chemie, im Maschinenbau oder in der Lebensmitteltechnologie durch eine extreme Miniaturisierung von einzelnen Bausteinen zu ungewöhnlichen und fast unvorstellbaren Lösungen von technischen, medizinischen oder sogar sozialen Zivilisationsproblemen kommen kann.

Das berühmteste und eingängigste Bespiel im Bereich neuer Materialien ist der Lotuseffekt: feine Nanostrukturen sorgen dafür, dass Wasser auf dem Blatt der Lotusblume abperlt und die Haftung von Schmutzpartikeln minimiert wird. Dies galt in der Welt der Nanotechnologie als wegweisend. Auch sind im Kalk von Muschelschalen organische und anorganische Stoffe im Nanobereich so eng aneinandergereiht, dass Muschelschalen extrem stabil und widerstandsfähig sind, derselbe Effekt existiert auch im menschlichen Knochen. Heute findet die Nanotechnologie Anwendung bei Pigmenten oder Additiven für Lacke oder Kunststoffe. In der Medizin bieten gezielt eingesetzte Nanopartikel die Möglichkeit, neuartige Diagnosen und Therapien zu entwickeln, zum Beispiel Kontrastmittel für bildgebende Verfahren der Computer- oder Magnetresonanztomographie. Beides sind bildgebende Verfahren, welche die Diagnosen von schweren inneren Krankheiten wie Krebs bemerkenswert vereinfacht und präzisiert haben.

Nanotechnologie realisiert ein Entwicklungsspektrum vom Staubsaugerroboter bis hin zur artifiziellen Mensch-Maschine

Hoch interessant sind die künstliche Intelligenz und Robotik. In den 1990er und 2000er Jahren entwickelte sich eine Debatte über die Chancen und Herausforderungen dieser Technologie, die bis in die Gegenwart hineinreicht und somit nach wie vor Gegenstand von Forschungen und allgemeinem Interesse ist. Hans Moravec, Forschungsdirektor am Robotics Institute der Carnegie Mellon University in den USA, erwartete in einer ersten Phase Produkte mit Leitsystemen für industriellen Transport und Reinigungsmaschinen. Anschließend würden diesen Robotern Haushaltsroboter für den normalen Verbraucher folgen. Größere Maschinen mit Manipulatorarmen und mit der Fähigkeit, mehrere verschiedene Aufgaben zu übernehmen, würden diesen dann wiederum folgen um schließlich menschengroßen Universalrobotern

Platz zu machen, die ihr Programm für die meisten einfachen Aufgaben einsetzen können. Danach rechnet er mit einer zweiten Generation, die von säugetiergleicher Gehirnkapazität und Kognition (Wissensfähigkeit) sein werde. Diese Generation werde über einen konditionierten Lernmechanismus verfügen und bei Anwendung ihrer Programme im Lichte ihrer bisherigen ›Erfahrungen‹ zwischen alternativen Möglichkeiten wählen können, so dass sie sich nach und nach an die jeweiligen Umstände anpassen könnten. Die dritte Generation werde denken wie es kleine Primaten, also etwa Schimpansen, tun, und werde physische, kulturelle und psychologische Modelle der Welt aufbauen, um bestimmte Aufgaben erst im Bewusstsein einzuüben und ihre Abwicklung geistig zu optimieren, ehe sie konkret stattfinden. Die vierte, menschenähnliche Generation schließlich werde aus einem selbst entwickelten Weltmodell abstrahieren und logische Schlüsse ziehen. Diese Entwicklung war für Moravec aus Sicht der anbrechenden 2000er Jahre unaufhaltsam, da die Robotik zur größten Industrie werde und damit die uns heute bekannte Informationstechnologie weit hinter sich lassen werde. Diese habe lediglich jene marginalen Aufgaben automatisiert, die wir als ›Papierkram‹ zu bezeichnen pflegten. Die Robotik werde demgegenüber alles andere automatisieren (Moravec 2000). Diese Vision galt anderen in ihrer puren positiven Aufladung als naiv. Sie unterstellten, dass derartig ausgestattete Maschinen dereinst ihr eigenes Bewusstsein und ein nicht mehr steuerbares Verhalten entwickeln könnten und würden. Die Miniaturisierung technischer Systeme und die Möglichkeiten ihrer Ausstattung mit KI schreiten mit hoher Geschwindigkeit voran. So rückt die Schaffung völlig neuer, für das bloße Auge unsichtbarer Welten in greifbare Nähe. Damit eng verbunden entstehen mit den Disziplinen der Bioinformatik, der Biometrie, der Systembiologie oder der Molekularelektronik Forschungszweige, welche die Informations- und Biotechnologien verknüpfen und interessante gesellschaftliche Perspektiven eröffnen.

Die Nanotechnologie entfachte vor 20 Jahren eine hitzige Debatte über die Chancen und Risiken der Technologie

Die industrielle Anwendung und die Synergien zwischen Informations-, Bio- und Nanotechnologien versprachen aber nicht nur gewaltige technologische Fortschritte für das Leben der Menschheit; sie rückten damit auch in den Sorgehorizont einer globalen Technologiegesellschaft (Joy 2000). Im Jahr 2000 wurden die Entwicklungsperspektiven der Nanotechnologie zum Gegenstand einer kritischen Debatte, die polarisiert war zwischen den Segnungen des Vorstoßes in die unbekannte Dimension und den möglichen ökosozialen Folgen einer unkontrollierbaren Kettenreaktion molekular erzeugter künstlicher Intelligenz (›gray goo‹). Der amerikanische Wissenschaftler

Bill Joy etwa betrachtete damals mit dramatischem Gestus die unkontrollierbare Entwicklung selbstreplizierender Nano-Maschinen als zusätzliche Sackgasse in eine weitere ökologische Katastrophe und hat damit die Forderung nach einem Forschungsverzicht begründet. Aus seiner Sicht sollten wir uns klarmachen, dass die stärksten Technologien des 21. Jahrhunderts – für ihn sind dies Robotik, Gentechnik und Nanotechnologie – ganz andere Gefahren heraufbeschwören, als die bisherigen Technologien. Sein Szenario kalkulierte die Nanotechnologie letztendlich auch als jene Voraussetzung ein, die es langfristig ermöglichen würde, den ›Cyborg‹ zu erschaffen, ein bio- und informationstechnologisch optimiertes Kunstwesen, die ›Mensch-Maschine‹, ein ›Golem‹ des 21. Jahrhunderts, die nützliche Dienste leisten soll, sich später aber durch ihre technologische Perfektion, ihre wachsende Intelligenz und die Möglichkeit der selbstständigen Replikation über den Menschen erhebt. Er schrieb:

»Vor allem Roboter, technisch erzeugte Lebewesen, und Nanoboter besitzen eine gefährliche Eigenschaft: Sie können sich selbstständig vermehren. Eine Bombe explodiert nur einmal, aus einem einzigen Roboter können viele werden, die rasch außer Kontrolle geraten« (Joy 2000).

Wenngleich die Debatte zuweilen in das Reich einer literarisch ›verrückten‹ Science Fiction reichten, die auch durch den Wissenschaftler und Buchautor Michael Crichton mit seinem Weltbestseller »Beute« befeuert wurden (Crichton 2002), wiesen die aus der seriösen Wissenschaft kommenden öko-sozialen Unbekannten dieser völlig neuen Synergien langfristig dennoch auf gesellschaftliche Konsequenzen hin, die auch andere Experten nicht bestreiten, wenn auch ihre Antworten auf diese Herausforderung unterschiedlich gewesen sind.

Für den amerikanischen Computerwissenschaftler David Gelernter würde die Bedeutung des Computers und der Nanotechnologie gegenüber dem, was sie an Möglichkeiten schaffen, im nanotechnologischen Zeitalter sogar aus dem Bewusstsein verschwinden. Er schrieb:

»Das Netz ist der Computer – ja, aber wir interessieren uns immer weniger für Computer. Das eigentliche Interesse der Astronomie gilt dem Kosmos, nicht den Teleskopen. Das eigentliche Interesse beim Einsatz von Computern gilt der Cybersphäre und den darin enthaltenen Strukturen, nicht den Computern, die wir als Teleskope oder Tuner einsetzen« (Gelernter 2000).

Viele Autoren sahen also nützliche technologische Möglichkeiten – und keine Gefahren: man werde mit seinem Computer reden können, elektronische Körperanzüge tragen und in einer Welt wohnen, in der man den Computer nicht

mehr wahrnimmt, obwohl er vieles beherrscht. Biologen, Chemiker und Physiker arbeiten in dieser Welt eng mit Technikern zusammen, damit eines Tages Computer mehrere Sinne ansprechen können. Schlagwörter sind ›electronic noses‹ und ›haptic interfaces‹ wie etwa Datenhandschuhe oder 3D-Brillen sowie 3D-Drucker.

Die Informationsgesellschaft wird Menschen und Organisationen in allen Bereichen prägen, im alltägliche Leben (Hausärzte per Monitor; automatisches Kochen; Autocomputer und elektronische Navigation; individuelles Handwerken/publizieren; virtuelle Interessensgemeinschaften in News-Groups), im Gesundheitsbereich (Operationsroboter; Cyber-Gesundheitskioske) oder im Bereich der Ausbildung (Simulation; Rollenspiel; automatisierte Tutoren; Weltbibliothek). Das Leben werde sich so radikal verändern, dass sich irgendwann niemand mehr die »pre-cyborg«-Ära vorstellen kann. In Zukunft werde alles verknüpft sein, so der amerikanische Zukunftsforscher William Mitchell zur damaligen Zeit, unser Bodynet, mit dem Buildingnet, die wiederum mit dem Communitynet und dem Globalnet verbunden sind (Mitchell 1996). Es werde sich eine überwältigende Informationswirtschaft entwickeln. Die Hälfte des Handels der industrialisierten Welt, prophezeite derzeit Dertouzos, könnte vom Info-Marktplatz beeinflusst werden. Die Welt werde eine neue Handelssprache entwickeln und Organisationen komplett umstrukturieren. Kurzfristig werde die Produktivität nur langsam wachsen, langfristig aber enorm. Das Bruttosozialprodukt in der Informationsgesellschaft werde auf ca. neun Billionen Dollar anwachsen. Irgendwann werde es eine fast komplett arbeitsfreie Gesellschaft geben, wo die Menschheit eine arbeitsfreie Ethik entwickelt hat und Maschinen besitzt, die jede Arbeit verrichten. Der Faktor ›elektronische Nähe‹ des Info-Marktplatzes festigt kulturelle Verbindungen zwischen Nationen, übt Druck auf lokale Kulturen aus und errichtet über den lokalen Kulturen eine universelle dünne Kulturschicht, welche Polarisierungen ausbalancieren und neben Handel und Diplomatie zu einem neuen wichtigen Kommunikations- und Kooperationskanal werden wird (Dertouzos 1997).

Das war seinerzeit ein faszinierendes Bild.

Soviel zur positiven Utopie

Dieser Ausflug in die Vorstellungs- und Diskurswelten der 1990er und 2000er Jahre zeigt: da wurde viel ›herumgesponnen‹. Allerdings sind diese Überlegungen, Visionen, Betrachtungen wichtig und waren immer auch (zum Teil) wissenschaftlich unterfüttert; sie sind gerade einmal erst vor etwa15 bis 20 Jahren entstanden, und dann bedacht, und dann veröffentlicht worden. Früher waren sie Gegenstand der Science-Fiction-Literatur von weltbekannten Autoren wie dem Amerikaner Isaac Asimov, dem Deutschen Herbert W. Franke oder dem Polen Stanislaw Lem. Vieles, was dort literarisch spannend entfaltet wurde, ist heute schlichte Realität, wenn auch die Dramatik der damals ge-

äußerten Befürchtungen bis hin zu einer sich in Paranoia hineinsteigernden Phantasie einfach zu hoch waren. Dennoch ist die Vision des Cyborg oder der Mensch-Maschine nicht vom Tisch. Sie ist entdramatisiert, ist aber auch im Bereich moderner Medizintechnik und der Hirnforschung weiterhin da. Der Cyborg ist als Mensch-Maschine auch heute präsent.

Die Kombination von menschlichem Geist und technischer Intelligenz ist offenbar unwiderstehlich. Max Biederbeck und Hakan Tanriverdi stellten deshalb 2013 in einer kurzen Bestandsaufnahme zur Lage fest:

»Der Begriff Cyborg scheint sich in seiner mehr als fünfzigjährigen Geschichte gewandelt zu haben. Von einer Science Fiction-Utopie hin zu einer einfachen Frage: wann ist es soweit?« (Biederbeck/Tanriverdi 2013).

Es geht dabei um die Frage, wie der Mensch seine Fähigkeiten trotz seines Alterns oder prinzipiell erweitern kann. Menschen beginnen, sich Technik zu implantieren. Rein äußerlich wandert der Computer in miniaturisierter Form in Kleidungsstücke oder audiovisuelles Gerät wie Brillen und Kopfhörer. Innerlich helfen Herzschrittmacher oder Retina-Chips, nachlassende Fähigkeiten oder Behinderungen auszugleichen. Es gibt Armprothesen, die per Fiberglasleitung ins Nervensystem eingegliedert werden. Und es gibt Sonden, Pads und Chips, die Schmerzen ausschalten können. Das alles ist heute Realität. Ein spektakuläres Beispiel hier ist der Eyeborg, der farbenblinden Menschen über eine technische Einrichtung die Fähigkeit gibt, Farben über Schallwellen wahrzunehmen. Das Thema wurde ein ethisches Problem, weil weitergehende Anwendungen das Gerät nicht nur über einen Sensor am Kopf mit dem menschlichen Gehirn in Verbindung bringen. Die geplante Implantation im Kopf beschäftigt heute ethische Kommissionen, ob solche Technologien überhaupt patentiert und allgemein angewendet werden dürfen.

Auch heute warnen Wissenschaftler vor den Gefahren bewusster und sich selbst replizierender Systeme

Nanotechnologie ist ein Thema mit globaler Ausstrahlung geworden. Jenseits der Chancen oder Herausforderungen dieser Technologie wurden seit Mitte der 2000er Jahre auch Befürchtungen laut, die sich auf warnende Aussagen etwa von Bill Joy bezogen und einen Verzicht auf eine sozial oder ethisch nicht reflektierte Forschung in diesem Bereich forderten. Ähnlich wie im Bereich der grünen Gentechnologie wurden Ausbreitungseffekte in der Fläche befürchtet, die sich der Beherrschung durch den Menschen entzögen. Im Juli 2004 legten die Royal Society und die Royal Academy of Engineering in London einen Bericht vor, in dem sie eine stärkere Regulierung von Nanotechnologien fordern. Der Bericht war ein Jahr zuvor von der britischen Regierung in

Auftrag gegeben worden. Studien des Center for Biological and Environmental Nanotechnology (CBEN) an der Rice University zufolge reichern sich Nanopartikel über die Nahrungskette in Lebewesen an. Dies bedeute nicht zwangsläufig eine Schädlichkeit, betonen die Autoren, verweisen jedoch auf andere Technologien, die am Anfang ebenfalls als ungefährlich galten.[8]

Aufsehen erregte 2014 ein Vorstoß von Bill Gates, Elon Musk und Stephen Hawking, die in einem gemeinsamen Auftritt vor der artifiziellen Intelligenz warnten, weil die dem Leben wie wir es kennen, ein Ende setzen werde (Barrat 2015). Die Argumentationskette ist dabei etwa so wie früher. Allerdings verlagert sich der Schwerpunkt der Betrachtung nun von den technischen Möglichkeiten der Technologie selbst zu ihrem gewollten Einsatz. Hawkings bemerkte in diesem Zusammenhang, das die Folgen der Künstlichen Intelligenz kurzfristig davon abhingen, wer sie kontrolliere; langfristig hingen sie davon ab, ob sie sich überhaupt kontrollieren lasse. Gleichzeitig räumte er ein, dass die KI eine sogenannte Dual-Use-Technologie sei, also eine Technik, die einerseits Gutes tun und andererseits großen Schaden anrichten könne. Die Kernspaltung, die hinter der Atomkraft und der Atombombe stehe, sei ein Beispiel für eine Dual-Use-Technologie. Und er fügte hinzu, dass solche Technologien so schädlich oder so gut seien wie die Absicht ihrer Nutzer.

James Barrat, der selbst Autor zu den Möglichkeiten und Risiken der Künstlichen Intelligenz ist (Barrat 2013) beschrieb zwei sensible Einsatzgebiete der Künstlichen Intelligenz: »Ein naheliegendes Beispiel sind autonome Tötungsmaschinen. Mehr als 50 Nationen entwickeln derzeit Kriegsroboter. Am gefragtesten werden Roboter sein, die ohne menschliches Zutun die »Tötungsentscheidung« treffen – die selbstständig einen Menschen ins Visier nehmen und umbringen«. Die Forschung zu autonomen Kriegsrobotern und Drohnen ist in vielen Ländern finanziell gut ausgestattet, etwa in den USA, in Großbritannien, Deutschland, China, Indien, Russland und Israel. Und an Südkoreas sensibler Grenze zu Nordkorea patrouillieren schon heute Roboter, autonom, selbstgesteuert, mit Infrarotaugen in den Diensten des Militärs. Über Israels Bergen und Tälern fliegen Drohnen des Typs Harpy. Sie haben ein Robotergehirn, das keine Befehle mehr von außen braucht, um gegen Feinde aktiv zu werden. Die Drohne kann gegnerische Radarstellungen selbstständig erfassen und angreifen, ohne dass ein Mensch gefragt werden muss. In Zukunft soll es dann autonome Tötungsmaschinen geben, die in komplexeren Szenarios zum Einsatz kommen und auf unvorhergesehene Ereignisse im Rahmen ihrer künstlichen Intelligenz flexibel reagieren (Geiß 2015).[9] Diese Waffen sind zwar vom internationalen Recht nicht verboten, ob sie jedoch den Menschenrechten

8 | Vgl. http://de.wikipedia.org/wiki/Nanotechnologie, aufgerufen am 24. Mai 2014.

9 | Vgl. auch die Dokumentation »odysso: Der automatisierte Krieg« im Südwestrundfunk/Saarländischen Rundfunk vom 29. September 2016.

oder auch nur dem Kriegsvölkerrecht entsprechen, bleibt zu bezweifeln. Wie werden sie Freund und Feind auseinanderhalten? Soldaten und Zivilisten? Wer wird verantwortlich sein? Der UN-Sonderbeauftragte Christof Heyns sprach in diesem Zusammenhang plakativ vom »death by algorithm«, vom Tod durch den Algorithmus (ebd.). Dass diese Fragen unbeantwortet bleiben, während die Entwicklung autonomer Tötungsmaschinen bereits in einen inoffiziellen Rüstungswettlauf eintritt, zeigt, wie schwierig die ethischen Fragen sind (Friedrich Ebert Stiftung 2015).

Hinzu kommt auch, dass die atomare Bewaffnung der Großmächte USA und Russland sowie China immer mehr in digitale Netzwerkstrukturen eingebunden werden, was sie für Hackerangriffe verwundbar macht und zu unkontrollierten Einsätzen führen könnte.[10] Im Rahmen der bestehenden nuklearen Erstschlagsdoktrinen wird auch in diesem hoch brisanten Bereich das Thema Cyber-Sicherheit wichtig, ohne dass dies bisher von den Nuklearmächten in Rüstungs- und Abrüstungsverhandlungen thematisiert worden ist.

Ethisch gleichermaßen komplex ist der Bereich der hochmodernen Tools zur Datengewinnung, die von der US National Security Agency (NSA) eingesetzt werden. In der Vergangenheit entschieden Richter darüber, ob ausreichend Anlass dafür besteht, dass eine Strafverfolgungsbehörde die Telefondaten eines Amerikaners einsieht, die persönliches Eigentum sind und vom Vierten Verfassungszusatz geschützt werden. Aber seit spätestens 2009 umgeht die NSA den Schutz der richterlichen Anordnung, indem sie außerhalb der USA die Glasfaserkabel von Yahoo und Google anzapft und Unmengen Daten herauszieht – die meisten von US-Amerikanern. Ohne die intelligenten KI-Tools könnte die NSA mit diesen Daten nichts anfangen. Doch mit modernster Data-Mining-Software kann sie Datenmengen durchforsten und kategorisieren, für die das menschliche Gehirn Jahrmillionen bräuchte.

Tötungsroboter und Data-Mining-Tools beziehen ihre Macht aus denselben KI-Techniken, die unser Leben in vielerlei Hinsicht bereichern. Wir nutzen sie zum Einkaufen, Übersetzen und Navigieren, und bald schon werden auch unsere Autos damit fahren. Das IBM-Computerprogramm Watson, die ›Denkmaschine‹, die in der Quizshow Jeopardy! gewann, legt die US-amerikanische Medizinerprüfung ab. Watson führt digitale Ermittlungen durch, genau wie Jungjuristen im ersten Jahr, nur schneller. Das Programm findet auf Röntgenbildern schneller Lungenkrebs als ein Mediziner und hängt die besten Wirtschaftsanalytiker locker ab. Wie lange wird es dauern, bis eine Denkmaschine auch die Forschung und Entwicklung Künstlicher Intelligenz beherrscht? Anders herum formuliert: Wann lernt der Roboter HAL 9000, sich in einer endlosen Rückkoppelungsschleife wachsender Intelligenz klüger zu programmieren, als er schon ist?

10 | Vgl. ebd.

Barret schlussfolgert weiter: »Die Krux liegt darin, dass wir nicht wissen, wie wir superintelligente Maschinen kontrollieren sollen. Viele meinen, solche Roboter wären harmlos oder sogar dankbar. Aber wegweisende Studien des KI-Forschers Steve Omohundro legen die Vermutung nahe, dass sie Instinkte entwickeln würden. Egal, ob es nun ihre Aufgabe wäre, auf Asteroiden Rohstoffe zu fördern, Aktien zu kaufen oder unsere Energie- und Wasser-Infrastruktur zu betreiben: Sie würden sich selbst schützen und versuchen, Ressourcen zu beschaffen, um besser an ihr Ziel zu gelangen. Um zu überleben, würden sie gegen uns kämpfen, und sie würden es nicht einfach zulassen, dass man sie abschaltet. Omohundro gelangt in seinen Studien zu dem Schluss, dass die Instinkte der superintelligenten Maschinen mit unseren Instinkten auf Kollisionskurs geraten, wenn wir bei der Konstruktion nicht sehr gut aufpassen. Mit Stephen Hawking können wir völlig zu Recht fragen:

»Angesichts der unberechenbaren Vorteile oder Risiken für die Zukunft tun die Experten doch sicher alles Erdenkliche, damit das bestmögliche Ergebnis herauskommt, oder?« (Barret 2015).

Diese ironische Anspielung auf die Möglichkeiten der Menschen zur Kontrolle der Technologie wird auch heute immer wieder mit den Möglichkeiten der Bio- und Gentechnologie verknüpft. Die Frage also ist, wie der Mensch in die Schöpfung eingreift und was dies letztendlich bewirkt.

Das Zeitalter der Biotechnologie ist da

In diesem Sinne sind (3.) auch bahnbrechende Innovationen im Bereich der Bio- oder Gentechnologie und elektronisch basierte und zunehmend ortsunabhängig genutzte Medizintechnologien beeindruckend. Die Gentechnologie hat als ›Genetic Engineering‹ heute einen beachtlichen Zugriff auf die Architektur des Menschen und der Natur realisiert. In ihrem Mittelpunkt steht das Verstehen, dass allen organischen, auf Kohlenstoff basierenden Lebensformen ein sich selbst reproduzierendes Datenband zugrunde liegt. Dessen Programmiersprache ist bei allen Organismen biochemisch gleich codiert. Der Träger dieser Codes ist die Desoxyribonukleinsäure (DNA) oder die Ribonukleinsäure (RNA). DNA und RNA sind ein in allen Lebewesen vorkommendes Biomolekül und Träger der Erbinformation, also der Gene. Ihr Unterschied besteht in ihrer Struktur und bestimmten Reaktionen biochemischer Art. Prinzipiell sind sie Träger von biochemisch codierten Informationen. Die Universalität des genetischen Codes erlaubt eine Fülle von Rekombinationsmöglichkeiten organischen Lebens. Wenn das vergangene 20. Jahrhundert das Jahrhundert der Chemie und Physik gewesen war, wie es der amerikanische Nobelpreisträger Robert Curl einmal sagte, so wurde schnell klar, dass das 21. Jahrhundert

das Jahrhundert der Biologie sein werde. In Form der Biotechnologie hat sich die Möglichkeit eröffnet, das Programm des Lebens zu entschlüsseln und Veränderungen zugänglich zu machen.

Das Wesen dieses technologischen Epochenschritts beschreiben vier Elemente:

- die Fähigkeit, gezielt in das Erbmaterial einzugreifen, ist das Herzstück der molekularen Revolution. Die Anwendungen der Zukunft, sei es in der Humanmedizin, der Landwirtschaft oder der Umwelttechnik, beruhen auf der neuen Programmierung genetischer Baupläne;
- genetische Ressourcen werden auf diese Weise zum Rohstoff und zum Kapital eines neuen, global wirksamen Wirtschaftszweiges, dessen Entfaltung auf der Phalanx von Computertechnologie und Genforschung basiert und der davon lebt, daß DNS als firmeneigenes Kapital bearbeitet, patentiert und besessen werden kann;
- durch den Umbau des Erbmaterials entwickelt sich der Mensch zum Objekt seines eigenen technisch-medizinischen Gestaltungswillens. Die Naturgeschichte des Menschen geht über in ein neues Zeitalter, in dem die Gestaltbarkeit des Lebens möglich wird;
- die Auswirkungen dieser neuen Verfaßtheit des Menschen werden das Leben in ganz unmittelbarer, praktischer und konkreter Form berühren. Sie werden aber auch jeden zwingen, sich auf irgendeine Weise auf eine persönliche Auseinandersetzung und Stellungnahme einzulassen.

Dabei sind die Vorteile der Anwendung ebenso groß wie ihre Tragweite für Gesellschaft und Individuum. Aus der wissenschaftlich-technischen Revolution der Gentechnologie ist in den 2000er Jahre eine politische, ethische, wirtschaftliche, soziale und psychologische Herausforderung geworden, welche Entscheidungen abverlangt über Werte, Ziele und den Weg dorthin. Darüber hinaus wurde die Gentechnologie auch ein politisches Thema der neuen Globalisierung: die Anwendung von humanen Eingriffen etwa bei der In-Vitro-Fertilisation oder der Früherkennung von genetischen Defekten von ungeborenem Leben unterliegt in den jeweiligen Ländern sehr unterschiedlichen moralischen Ansichten oder gesetzlichen Regelungen. Globalisierung erlaubt durch Medizintourismus oder Internetgebrauch die Umgehung länderspezifischer Regularien, lagert grundlegende ethische, soziale oder politische Problematiken der Technologie damit über die Grenzen hinaus; gentechnologische Manipulationen agrartechnischer Art können Pflanzen resistenter gegenüber Umwelteinflüssen machen und Ernteerträge steigern, sie werfen aber Probleme mit Blick auf ihre allgemeine Umweltverträglichkeit innerhalb ihrer Ansiedlung in einer ›natürlichen‹ Umwelt oder die Beherrschung von Märkten für gentechnisch modifiziertes Saatgut durch einige wenige Agrarkonzerne

insbesondere gegenüber indigenen Volksgruppen in Entwicklungsländern auf. Auch hier zeigte sich in den vergangenen 20 Jahren der globale Einfluss einer zunächst in Universitäten und Forschungslaboren ›unschuldig‹ entwickelten Basisinnovation, die schlussendlich erhebliche Probleme hinsichtlich ihrer Umweltverträglichkeit, ihrer allgemeinen Verfügbarkeit und des ›Eigentums‹ von natürlichen Ressourcen geschaffen hat (Weidenfeld/Turek, 2002: 197 ff).

Der amerikanische Zukunftsforscher Jeremy Rifkin orakelte bereits Ende der 1990er Jahre über einen gigantischen ›Faustschen Pakt‹, der mit dem Zeitalter der Biotechnologie über die Menschen kommen werde. Es entstünden große Verlockungen großer Fortschritte und einer leuchtenden Zukunft voller Hoffnungen, doch zu welchem Preis? Mit seiner ihm eigenen dramatisierenden Art sprach er von einer fatalen Unterbrechung der natürlichen Evolution und fragte: sind wir dabei uns zu Aliens in einer von geklonten, chimären und transgenen Kreaturen bevölkerten Welt zu entwickeln? Und weiter: welche Folgen wird es für die Weltwirtschaft und Weltgesellschaft haben, wenn der Welt-Genpool von einer Handvoll multinationaler Konzerne kontrolliert werde? Und wie wird die Patentierung von Leben an unsere tiefsten Überzeugungen über die Natur als göttliche Schöpfung und über den unveräußerlichen Wert von Leben rütteln? (Rifkin 1998). Seitdem waren atemberaubende Fortschritte in der Bio- und Gentechnologie zu verzeichnen. Mit Blick auf Rifkins warnende Worte setzte das Jahr 2016 einen wichtigen Akzent. Es war das Jahr, als in Großbritannien behördenseitig eine Genehmigung erteilt wurde, gentechnische Versuche an menschlichen Embryonen durchzuführen. Nach den Worten des deutschen Gesundheitspolitikers Karl Lauterbach eine problematische Entscheidung, da diese Erlaubnis nun in der Welt sei, die Folgen einer gezielten Veränderung des Erbgutes und die damit verbundenen Risiken aber nach wie vor nicht zu überblicken seien (Zinkant/Becker 2016).

Dies waren und sind allesamt aufrüttelnde Fragen. Sehen wir nach, wie die Entwicklung in der Breite des Themas bis heute verlief.

Biotechnologie repräsentiert einen technologischen Kosmos von faszinierenden Möglichkeiten

Biotechnologische Verfahren werden in den unterschiedlichsten Bereichen angewendet. Dies sind zum Beispiel die Medizin (Rote Biotechnologie), die Industrie und der Umweltschutz (Weiße bzw. Graue und Braune Biotechnologie) sowie Pflanzen bzw. Landwirtschaft (Grüne Biotechnologie). Alle drei Bereiche sind einerseits ein Ergebnis der Globalisierung im wissenschaftlichen, technischen und agrarökonomischen Bereich; gleichzeitig treiben sie dabei die Globalisierung aufgrund ihrer weltweiten Bedeutung weiter an. Und sie sind vielfältig miteinander verknüpft. Pflanzliche Zellen oder Enzyme kön-

nen auch zur Produktion von industriellen Stoffen oder von Medikamenten genutzt werden Auch zur Entgiftung von Böden (Phytorenmediation) oder als Umweltsensoren sind Pflanzen geeignet. Die Geltungs- oder Durchsetzungskraft biotechnologischer Innovationen hängt derzeit aber von ethischen oder rechtlichen Bestimmungen und Restriktionen ab. Diese sind von moralischer, technologischer, wettbewerbspolitischer oder mentaler Natur. Während die rote Biotechnologie weltweit Durchbrüchen in der Humanmedizin den Weg bahnt und damit für die Reproduktionsverhalten und die Möglichkeiten von Eingriffen in das menschliche Erbgut steht, werden die weiße/braune und grüne Biotechnologie zu einer starken Unterströmung im Mainstream der wirtschaftlichen oder entwicklungspolitischen Globalisierung.

Die weiße oder braune Biotechnologie eröffnet vielfältige industrielle Anwendungen. Dies sind zum Beispiel:

- die Substitution fossiler Energieträger durch Biotreibstoffe;
- die Produktion von Antibiotika zur Behandlung von Infektionskrankheiten;
- die Herstellung von Nahrungsmittelzusätze zur Steigerung des Nährwerts von ›Functional Food‹ (Vitamine, Aminosäuren, Enzyme, Hormonen);
- die Entwicklung von biologisch abbaubarer Polymeren als Biokunststoffe;
- Problemlösungen im Bereich der industriellen Nutzung von biologischen Dekontaminationsstrategien im Umweltschutz.

Die weiße Biotechnologie kann in der Konsequenz erdölabhängige chemische Prozesse durch Mikroorganismen in Zellfabriken ersetzen und so vom Erdöl unabhängiger machen. Sie hat ein großes Potenzial in der Feinchemie. Sie ist dabei weniger öffentlicher Kritik ausgesetzt als die rote oder grüne Biotechnologie, da sich diese Sparte vor allem auf ressourcenschonende, energiesparende und abfallvermeidende industrielle Produktionsprozesse konzentriert. Ein hohes Wachstum ist insofern programmiert, das 2015 in der deutschen Biotechnologiewirtschaft bei etwa 2,5 Milliarden Euro p. A. lag. Der weltweite Umsatz der weißen Biotechnologie wurde dabei aus der Sicht der Jahre 2012/2013 auf rund 50 Milliarden Euro p. A. geschätzt. Er ist damit vergleichbar mit dem gegenwärtigen Umsatz, den Biopharmaka weltweit p. A. erzielen und der mit 55 Milliarden Euro angegeben wird (Eiden 2012).

Die grüne und rote Gentechnik repräsentiert den Bereich, der im Rahmen der Ernährung und gesundheitlichen Versorgung einer wachsenden Weltbevölkerung für die Globalisierung am bedeutendsten ist, wobei sich der Aspekt der Gesundheitsversorgung nicht auf vergleichsweise elitäre oder kostspielige Anwendungen der Fortpflanzungsmedizin wie die Insemination, die Invitro-Fertilisation, die Mikroinjektion oder die Hodenbiopsie beziehen, sondern auf globale Krankheiten wie Malaria, Tuberkulose oder Aids.

Agrarwirtschaft und Ernährungsindustrien sind High-Tech-Industrien

Das menschliche Leben wird durch globale Technologien im Bereich der Lebenswissenschaften oder der Agrarwirtschaft fundamental berührt. Alleine die Agrarwirtschaft, die 2050 zwischen neun und zehn Milliarden Menschen zu ernähren hat, wird über ihren Charakter einer High-Tech-Industrie zum wichtigen Globalisierungsfaktor. Mit der Biotechnologie eröffnen sich Möglichkeiten für die ausreichende Ernährung einer wachsenden Weltbevölkerung. Ein Großteil der Agrarwirtschaft wandelt sich zu einem kapital- und forschungsintensiven High-Tech-Sektor, zu einer Industrie, in der DNS, der Rohstoff des Lebens in Eigentum umgewandelt werden kann. 2025 werden mehr als 85 Prozent der Menschheit in Entwicklungsländern leben. Um eine ausreichende Ernährung für alle sicherzustellen, muss die Nahrungsmittelproduktion nach vorliegenden Schätzungen um rund 50 bis 75 Prozent gesteigert werden. Die Bio- und Gentechnik wird das Profil der Agrarwirtschaft ändern. Boden, natürliche Ressourcen und Arbeit verlieren als charakteristische Faktoren der Landwirtschaft an Bedeutung. Agrarwirtschaft und Ernährungsindustrie werden zum High-Tech-Produzent, kapitalintensiv und auf Laborforschung gestützt. Schon heute funktioniert die Tierzucht nicht mehr ohne die Arbeit im Labor. In-vitro-Fertilisation, die ›Befruchtung im Glas‹, und Embryonenübertragung sind ›state of the art‹ und haben bereits den Weg für das Szenario ihrer Anwendung in der nahen Zukunft geebnet. Die Fähigkeit, gezielt in das Erbgut einzugreifen, wird aller Wahrscheinlichkeit nach binnen der nächsten fünfzehn Jahre ›ganz normal‹ kommerziell genutzt werden können, um die Eigenschaften und die Leistungsfähigkeit von Nutztieren wie Kühen und Schweinen maßzuschneidern.

Tiere mit zusätzlichen Nutzfunktionen werden ›produziert‹ werden: Schafe, Ziegen, Kühe, die als lebende Pharmafabriken Arzneimittel liefern und mit der Milch ausscheiden; oder Schweine, die als Organspender Herzen, Lebern und Nieren bereitstellen, deren Zellen so verändert worden sind, dass sie das menschliche Abwehrsystem als artgleich toleriert. Die Nutztierhaltung wird damit um die Produktion von Nahrung oder von ›Ersatzteilen‹ für Mensch und Tier ergänzt. Hinzu kommen andere industrielle Anwendungen. So lassen sich bereits heute aus den Erbanlagen der goldenen Radnetzspinne Erbanlagen isolieren, die zur Produktion extrem belastbarer Fasern dienen. Das Material, das so gewonnen wird, dient der Produktion von biologisch abbaubarem chirugischem Nahtmaterial oder leichtgewichtigen kugelsicheren Westen. In der Pflanzenzucht werden gentechnische Eingriffe vorgenommen, die gezielte Neukombinationen von Einzelmerkmalen bewirken, um die Resistenz gegen Viren, Insekten, Salz, Kälte und Dürre zu stärken oder um die Zusammensetzung der Nährstoffe zu gestalten. Der Einsatz der Gentechnik wird sich nicht nur auf Veränderungen von Kulturpflanzen beschränken, die den Ertrag auf

den Feldern erhöhen. Es wird auch mehr synthetisierte, also künstliche Produkte geben, die in Laboratorien erzeugt und in Fabriken verarbeitet werden und damit den herkömmlichen Anbau vermutlich zunehmend ergänzen oder gar ersetzen. Die Lage auf den Feldern wird sowohl von ursprünglichen als auch gentechnologisch modifizierten Pflanzen und Organismen geprägt. Dies hat zu einer Kontroverse um die Zulässigkeit und die ethische Verantwortung eines gleichermaßen natürlichen wie gentechnologisch modifizierten Anbau geführt.

Die Agrarstruktur der Zukunft wird von Unternehmen bestimmt, die Teile des Produktionsprozesses, zum Beispiel Entwicklung und Herstellung von Mastfutter, Saatgut, Pestiziden oder Dünger, in ihr Sortiment aufnehmen. Grenzlinien zwischen Landwirten, Saatgutentwicklern, Düngemittelfirmen oder lebensmittelverarbeitenden Fabriken werden dann verschwimmen. Im Zeitalter der Globalität werden auch Life-Science-Unternehmen, Agrarkonzerne und international agierende Handelshäuser oder Lebensmittelhändler dazu übergehen, Joint Ventures zu bilden. Es werden sich Allianzen herausbilden, die von der Forschungskooperation bei der Entschlüsselung und Patentierung von Pflanzen- und Tiergenomen über Saat und Ernte bis zu Produktion und Vertrieb von Nahrungsmitteln reichen. Die High-Tech-Transformation der Agrarwirtschaft wird sich im neuen Jahrhundert als global wirksames Muster in allen modernen Industriegesellschaften vollziehen, selbst wenn sich die gegenwärtigen Entwicklungen in Nord- und Südamerika, in China, Südostasien, Südafrika und Europa unterscheiden. Beispielsweise stammten in den USA 2000 bereits über die Hälfte der Soja- und rund ein Drittel der Maisernte aus genetisch verändertem Saatgut. Auch in Kanada und Argentinien kann man von einem Schulterschluss der großen Agrarunternehmen und der Bio-Tech-Industrie sprechen. Demgegenüber reagieren die europäischen Regierungen, Landwirtschaftsverbände und Verbraucher nach wie vor gegenwärtig überwiegend ablehnend auf die Anwendungen der grünen Gentechnologie. Ein ähnliches Bild zeigt sich in einigen asiatischen Ländern, wie etwa Japan, und seit einiger Zeit auch bei den amerikanischen Verbrauchern.

Die Mischung aus Befürwortung, Bedenken, Misstrauen und dem Lavieren in politisch-wirtschaftlichen Regulierungsfragen ist wahrscheinlich eine Übergangserscheinung. Dies zeigt sich, weltweit gesehen, in der gestiegenen Nachfrage nach gentechnologisch modifizierten Sorten. Nach Angaben des als relativ unabhängig geltenden ›International Service for the Aquisition of Agro-Biotech Applications' brachte bereits das Jahr 2001 für die Hersteller und Verkäufer gentechnisch modifizierter Nutzpflanzen ein Rekordergebnis. Gemessen am Jahr 2000 war demnach die weltweite Anbaufläche um fast ein Fünftel gestiegen. Auf insgesamt rund 52 Millionen Hektar wuchsen gentechnologisch veränderte Mais- und Sojapflanzen, Baumwolle und andere Kultursorten. Die Organisation erklärte diese große Steigerung vor allem mit dem

wachsenden Interesse von Kleinbauern in China und Südafrika an gentechnisch veränderten, schädlingsresistenten Baumwollsorten. Das bedeutet, dass seit Mitte der 1990er Jahre die Größe der Anbaugebiete um das dreißigfache angestiegen ist. Dieses Wachstum und die internationale wirtschaftliche Verflechtung werde dazu beitragen, die unterschiedlichen Marktstrukturen und Regulierungsniveaus anzugleichen.[11] Verbesserte Kenntnisse über die Chancen und die Vermeidung von Umwelt- und Gesundheitsrisiken werden mittelfristig eine Reihe von – auch emotionalen – Vorbehalten gegenüber der grünen Gentechnik einebnen bzw. zu einer differenzierteren Sichtweise führen und damit auch gesetzliche Schranken fallen lassen. Obwohl von Kritikern der Bio- und Gentechnik oft ins Feld geführt, ist die Frage, inwieweit die Dominanz einer bio- und gentechnologischen Agrarindustrie Bauern ihrem Land entwurzelt, in den europäischen Industrienationen von untergeordneter Bedeutung. Kleinbetriebe spielen ökonomisch ohnehin eine immer geringere Rolle, wenngleich sie aufgrund ihrer Bedeutung für den ländlichen Raum in einer Nischenfunktion überleben werden.

Für Asien dagegen ergibt sich ein anderes Bild. In einigen Ländern dieser Region ist es durchaus vorstellbar, dass die Bio- und Gentechnik in traditionelle Kultur- und Sozialformen eingreift, nämlich dann, wenn es den Unternehmen mehr und mehr gelingt, Produkte zu produzieren, die zur Exportpalette und damit zur Lebensgrundlage gehören; oder etwa, wenn im Labor Ersatzstoffe entwickelt werden, die sich kostengünstiger herstellen lassen. Anders als in Nordamerika und Europa muss daher in Asien der Verlust landwirtschaftlicher Arbeitsplätze auch als Faktor sozialer Unruhe kalkuliert werden. Die ländliche Familie und das Dorf mögen im Westen von abnehmender Bedeutung sein, in vielen Teilen Asiens stehen sie aber weiter für ein wichtiges Maß an sozialer Stabilität und Kontinuität (Weidenfeld/Turek 2002: 76ff.).

Gesundheitstelematik entspannt das Gesundheitswesen durch effiziente Versorgungsformen im demographischen Wandel

Der Bereich der Gesundheitstelematik bezeichnet die Möglichkeit, mittels moderner Informations- und Kommunikationstechnologien Menschen zeit- und ortsunabhängig medizinisch zu beobachten und zu behandeln. Sie ist besonders attraktiv mit Blick auf chronische Krankheiten wie Bluthochdruck, Herz-Kreislauferkrankung (Herzinfarkt und Schlaganfall) sowie Diabetes (I und II). In Deutschland sind etwa sechs Millionen Menschen von diesen Erkrankungen betroffen. Dies sind immerhin fast acht Prozent der Bevölkerung. Die

11 | Vgl. Die grüne Gentechnik gedeiht. Anbau transgener Nutzpflanzen abrupt um ein Fünftel gestiegen, in: Frankfurter Allgemeine Zeitung vom 11. Januar 2002.

Alterung der Menschen im Zuge des demographischen Wandels wird dieses Phänomen intensivieren.

Gleichzeitig steigt die Betroffenheit der Menschen von diesen Krankheiten mit steigendem Wohlstand und im Zuge ungesunder Lebensführung weltweit an. Deshalb sind moderne Behandlungsmethoden vor dem Hintergrund der Alterung weltweit ein Thema mit höchster Priorität. Betroffen ist dabei nicht nur die westliche Hemisphäre, sondern es sind auch die Gesellschaften Asiens, allen voran China und Japan. Hinzu kommt: die Unterschiede dabei aber sind von gravierender Natur. in der Sahelzone geht es weiter ums Überleben – in China oder Indien zunehmend auch um die Konsequenzen einer luxuriösen Lebensführung. Mit allen Folgen der Zivilisationserkrankungen. Sie benötigen entweder in strukturschwachen Zonen in ihren Heimatländern oder im Rahmen ihrer (weltweiten) Mobilität eine entlokalisierte und entgrenzte medizinische Unterstützung. Im Kontext des Sogs der großen Metropolen, der Ausdünnung des ländlichen Raums und einer verstärkten Mobilität sowie der Notwendigkeit von modernen Versorgungsformen, werden telemedizinische Innovationen global gesehen gesellschaftlich und gesundheitspolitisch immer wichtiger. Dazu dient auch der zeitnahe und global organisierte Austausch medizinischer Informationen und Daten, so etwa in der Radiologie, wo rund um die Uhr von Spezialisten Informationen von Kontinent zu Kontinent ausgetauscht und bewertet werden. Das spart Zeit und Geld und intensiviert die Behandlung von kranken Menschen.

Dies kann man auch in einem größeren Zusammenhang sehen. Gesundheit und Gesundheitstechnik werden in Zukunft zu einem prägenden Teil der entwickelten und sich entwickelnden Ökonomien. So wie die Mechanik, die Chemie, die Elektrotechnik und zuletzt die Informations- und Telekommunikationstechnologie als bahnbrechende Basisinnovationen Volkswirtschaften über lange Zeiträume in entscheidender Weise prägten, wird das Gesundheitswesen und die Medizintechnik als entscheidender Wirtschaftszweig in den ersten 50 Jahren des 21. Jahrhunderts genauso bestimmend werden wie die genannten Basistechnologien der Vergangenheit. Dabei sind alle Technologien und technischen Lösungen in den Bereichen Logistik und Verkehr auch Globalisierungsinstrumente. Über so gebaute ›Brücken‹ zwischen allen Erdteilen der Welt kommt es zu vielfältigen Kontakten in der Globalisierung. Verkehr und Logistik haben einen kulturellen Effekt. Menschen kaufen oder vermieten nicht nur Waren und Dienstleitungen, sondern tauschen sich kritisch über deren Mehrwert, Nutzen oder moralischen Entstehungskontext aus. Und dies in zunehmender Weise auch über das Internet oder die Mobiltelefonie, also über globale Strukturen, die dann Meinungen und Bewertungen aus der ganzen Welt umfassen und – jenseits der Zensur – zulassen. Dabei gewährleisten moderne Logistik und adäquate technologische Lösungen die Möglichkeit einer Weltentwicklung, die innerhalb von verschiedenen Szenarien den Globus in

den kommenden Jahrzehnten entscheidend prägen werden (Deutsche Post AG/Z_punkt 2012).

Der Weltraum wird als Forschungslabor, als zivile und als militärische Operationsbasis unverzichtbar

Hinzu kommt eine stark anwachsende zivile und militärische Nutzung des Weltalls, welche sehr wichtig geworden ist, für Navigation, Ortung, militärische Führung oder ökologische Messprozesse in den Bereichen Wetter, Klima und Erdbeschaffenheit. Die Weltraumtechnologien verdeutlichen als erdumspannendes technologisches Netzwerk bildhaft die neue Globalisierung und integrieren wichtige Länder unserer Welt.

2. Big Data und das koronare Herzkranzgefäss des globalen Organismus

Die zweifelslos wichtigsten technologischen Antriebsmotoren der neuen Globalisierung sind die Informations- und Kommunikationstechnologien. Sie sind mit Blick auf ihre Funktion das koronare Herzkranzgefäß der Globalisierung, das diese tagtäglich mit dem Sauerstoff versorgt, ohne den der Herzschlag der Globalität nicht möglich wäre. Die durch sie transportierten Informationen haben einen Wert, der dem prozentualen Anteil des Sauerstoffgehalts im Verhältnis zu seinem Kohlendioxidgehalt im Blut entspricht. Würden die Wege, Instrumente und Mechanismen von Information und Kommunikation schlagartig verstopft und kollabieren, wäre dies ein schwerer Herzinfarkt der globalisierten Welt.

Informationen sind ein Goldschatz

Die Bedeutung der Informations- und Kommunikationstechnologien liegt unter anderem in ihrem ökonomischen Potenzial. Sie halten in der neuen Globalisierung Einzug in sämtliche Lebensbereiche, wobei der Trend zur Konvergenz von Informations- und Kommunikationstechnologien sowie Sensorik, Robotik und Biometrie die weitere Entwicklung der Big Data Bewegung exponentiell voranbringen wird (Mayer-Schönberger/Cukier 2013; Ford 2015). Big Data bezeichnet eine Methode und ein Modell der Vorhersage menschlicher Entscheidungssituationen. Mithilfe der Sensorik, einer Vielzahl von Datensätzen sowie bestimmten Algorithmen erlauben sie automatisierte Voraussagen über Verhaltenspräferenzen, die sich anhand von statistischen Korrelationen abbilden lassen. Im Ozean der Daten sind überraschende und wertvolle Verbindungs- und Knotenpunkte verborgen, um die sich bis Anfang der 2000er Jahre niemand so richtig gekümmert hat. Mit der Methodik des Data-Mining

ist nun ein Zustand erreicht, bei dem menschliche Handlungen, Aktivitäten oder Gefühlszustände messbar sind. Deshalb ist Big Data kommerziell, staatlich und gesellschaftlich hochinteressant. Dadurch kommt die Welt ihrem Wunsch näher, das Leben zu quantifizieren und es mit humaner Robotik oder künstlicher Intelligenz aus der Kombination der verschiedensten Datensätze attraktiver zu gestalten. Nanotechnologische und gentechnologische sowie materialtechnologische Innovationen werden diesen Prozess durch unterstützende Technologien und Prozessentwicklungen flankieren.

Ihre Chancen für Wirtschaft, Wissenschaft, und Politik sind facettenreich und ihre kulturelle Bedeutung erheblich. Daten haben einen enormen ökonomischen Wert, der dem Wert von Rohstoffen und Energie gleichkommt. Sie realisieren Produktivitätserhöhungen, Kostenreduktion oder optimierte ›Business to Business‹ (B2B) und ›Business to Consumer‹ (B2C) – Strukturen; sie erleichtern die Bildung von zielführenden Szenarien und sind unverzichtbar in der Prognostik und Ausbeutung von sozio-ökonomischen Entwicklungen. Auch die Bereiche der Wissenschaft, der öffentlichen Verwaltung oder des Gesundheitswesens werden von ihnen erfasst. Big Data ermöglicht eine Vorstellung der Zukunft der digitalisierten Existenz. Dabei sind allerdings auch erhebliche Herausforderungen zu bewältigen.

Yvonne Hofstetter warnt davor, das Big Data zum neuen Geschäftsmodell der Überwachung wird. Die Masse der Daten, die permanent durch das weltweite Netz fluten, seien alleine bisher kein Risiko gewesen. Erst die intelligenten Algorithmen, die Big Data ausmachen, würden zunehmend zum Problem. Sie analysieren und prognostizieren uns, um uns zu kontrollieren – autonom, schnell, überall und permanent. Sie verbreiteten sich im Rahmen artifizieller Intelligenz, als selbstlernende Haustechnik, vernetzte Autos, elektronische Armbänder oder intelligente Smartphones (Hofstetter 2014). Die Begehrlichkeiten von Unternehmen oder Regierungen nach personenbezogenen Daten steigen. Internetnutzer werden zum gehandelten Gut, ohne dass es ihnen bewusst ist oder sie dadurch ökonomischen Nutzen erzielen. Dies reicht in alle Bereiche des Alltags hinein. Aufsehen erregten Berichte die zeigten, wie nicht nur das Internet, sondern an das Internet angeschlossene Geräte und Gegenstände Informationen an den Staat oder die Industrie übermitteln können, um so aufschlussreiche Informationen über die Verhaltensweisen und Wünsche von Menschen zu sammeln, auszuwerten und später in individualisierte Marketingstrategien zu übersetzen.

Wenn die Barbiepuppe fragt: »Willst Du Tänzerin werden? Oder Politikerin?«, fließen aufschlussreiche Daten

Selbst vor dem Kinderzimmer macht diese Methodik keinen Halt. Selbst herkömmliches Spielzeug enthält heute elektronische Komponenten. So hat die weltberühmte Barbie-Puppe ein elektronisches Hörgerät, mit dem sie vernehmen kann, was das spielende Kind an Missstimmungen oder Gefühlen mitzuteilen hat. Damit die Kleinen mit ihrer Puppe reden, hat die Puppe auch einen Lautsprecher über den sie dem Kind Fragen stellt: »Du hast mir gesagt, dass Du gerne auf einer Bühne stehst, möchtest Du vielleicht Tänzer werden? Oder Politiker?« (Boie 2015). Werden die Daten an den Hersteller elektronisch übersandt, kann dieser sich Gedanken darüber machen, wie er aus diesen Informationen durch die Weiter- oder Neuentwicklung von Spielzeug Profit schlagen kann. Andere Beispiele sind der kleine Dinosaurier ›Cognitoy‹, der im Gespräch mit den Kindern die semantischen Fertigkeiten des Nachwuchses prüft und überwacht, wie schnell er klüger wird. Dabei kommen solche Funktionen den Eltern entgegen. Es besteht die Option, dass diese Geräte die Informationen an die Eltern schicken. Diese können dann prüfen, wie der Geisteszustand ihrer Kinder ist, womit sie sich beschäftigen und wo sie gerade genau sind. Künstliche intelligente Technik wird so zur Beschäftigungstherapie und zur Erziehungsinstanz. Wo früher Großfamilien die Entwicklung des Nachwuchses persönlich und in intimer Umgebung förderten, nehmen künstliche Intelligenz und smarte Geräte den ›Helikoptereltern‹ viele Anstrengungen in deren Erziehung ab. So paradox es klingt: dies kann auch als eine win-win-Situation gedeutet werden, in der die Bedürfnisse von Kindern, Eltern und Industrie auf eigenartige Weise konstruktiv zusammengeführt werden können.

Problematisch bleibt aber auch: Daten und Informationen, die im frühen Kindesalter über Menschen erhoben worden sind und sorgfältig gespeichert werden, können später von unschätzbarem Wert sein. Wer früh einen Menschen durchleuchtet hat und die Daten sorgfältig im Zeitverlauf pflegt, kann Rückschlüsse für das restliche Leben des Menschen ziehen. Wer als Teenager besonders wild Fahrrad gefahren ist, zahlt vielleicht mehr für die Fahrschule, die 30-jährige Bankerin, die als kleines Mädchen stets den Porsche im Videospiel gefahren ist, möchte nun womöglich einen echten kaufen und wer mit zwölf Jahren hervorragend im Ego-Shooter war, der will mit 17 Jahren vielleicht gerne zur Bundeswehr (ebd.). Dabei durchläuft die Spielzeugindustrie die gleichen Veränderungen wie andere Branchen. Die Hersteller versuchen so viel wie möglich, über ihre Kunden zu erfahren, um deren Bedürfnisse oder persönlichen Entwicklungen im Voraus zu erahnen. Aber auch der Staat berechnet mit Algorithmen, wo eher Verbrecher auftauchen und wo eher nicht, und Versicherungen prüfen mit komplexen Programmen, wer einen Kredit oder eine Versicherung bekommt und wer nicht.

Die Politik tut sich mit Kontrolle und Regulierung von Big Data schwer

Viele Unternehmen sind mit galaktischen Raumschiffen im Internet in Lichtgeschwindigkeit unterwegs. Der Staat und regulierende Behörden zuckeln in einem Bummelzug mit Tempo 50 hinterher. Zunehmende Datenmengen, unterschiedliche und inkompatible ITK-Strukturen und Datensicherheit wurden in den letzten zwei Jahrzehnten zu Recht problematisiert. Mit Bezug auf Big Data ist so auch das Erkennen des Data Minings oder die illegale Datenauswertung schwierig. Es fehlen integrierte Digitalisierungsstrategien, um auf Chancen und Herausforderungen des digitalen Strukturwandels angemessen zu reagieren. Dementsprechend sind die Risiken hoch. Zu dem Gefühl des ›Information Overload‹ kommt der Verlust der Datenhoheit, den viele Internetnutzer allerdings zum Teil durch ihr egozentrisches und schwatzhaftes Benehmen in den sozialen Medien oder anderen Internetangeboten selbst zu verantworten haben. Die Big-Data-Entwicklung realisiert ein unglaubliches Veränderungspotenzial des menschlichen Miteinanders. Insofern sind regulative Rahmenbedingungen nötig, so dass sich Technologie und Methodik optimal entfalten können (Dapp/Heine 2014). Auf der anderen Seite geht es darum, die Unantastbarkeit des Menschen und die Menschenwürde gegen eine wild wuchernde digitale Revolution zu verteidigen.

Die Journalisten Stefan Aust und Thomas Amman weisen deshalb zu Recht auf ein geradezu historisches Projekt der Europäischen Union hin: eine einheitliche Datenschutzregelung für die Europäische Gemeinschaft. Hierbei geht es um die digitalen Persönlichkeitsrechte von mehr als einer halben Milliarde Menschen. Es handelt sich dabei um die Datenschutz-Richtlinie, die die 1995 erlassene Richtlinie der Europäischen Gemeinschaft zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten ersetzen soll. Die Datenschutz-Grundverordnung soll diese Richtlinie wesentlich weiter entwickeln. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt und andererseits der freie Datenverkehr innerhalb des europäischen Binnenmarktes gewährleistet werden. Die Datenschutz-Grundverordnung ist Teil der beabsichtigten EU-Datenschutzreform, welche die Europäische Kommission 2012 vorgestellt hatte.[12] Damit soll europaweit und einheitlich festgeschrieben werden, dass die Bürger der Weiterverarbeitung ihrer Daten ausdrücklich zustimmen müssen und ein Recht auf ›Vergessen werden‹ haben, also auch im Nachhinein die Löschung ihrer Daten verlangen können. Aufgrund der komplizierten Gemengelage und der Einflussnahme der Lobbygruppen aus den USA konnte bisher aber keine Einigung über den Gesetzentwurf der EU-Kom-

12 | Vgl. https://de.wikipedia.org/wiki/EU-Datenschutzreform, aufgerufen am 24. Juni 2015.

mission erzielt werden und auch die nationalen Haltungen zu diesem Gesetzesvorhaben sind ambivalent (Aust/Amman 2014: 23).

Big Data realisiert eine weitere Evolutionsstufe im Internet

Die Welt befindet sich inmitten des digitalen Strukturwandels und die Relevanz web- wie wissensbasierter Technologien nimmt in allen Gesellschaftsbereichen zu. Damit vollendet sich eine Entwicklung, die gerade einmal etwa 50 Jahre jung ist und in den 1940er Jahren am Institute for Advanced Study in Princeton/USA im Kreise von Albert Einstein, Robert Oppenheimer, Kurt Gödel, Alan Turing und John von Neumann mit den ersten Schritten hin zur Digitalisierung der Information ihren primitiven Anfang nahm (Dyson, 2014). Unzählige betriebliche, staatliche oder private Interaktionen sind heute an digitale Informations- und Kommunikationstechnologien gebunden. Big Data ist nach einer Reihe logischer Evolutionsstufen im Internet der aktuelle Aggregatzustand der globalen Digitalisierung.

Nach der Individualisierung, der Verlagerung der Daten in die Cloud oder des Wunsches nach digitaler Mobilität wächst das Verlangen, aus den vorhandenen Datenbergen wertvolle Interaktionsmuster und Verhaltensgewohnheiten der Menschen zu extrahieren, um diese mittels eines modernen Data-Mining Prozesses systematisch zu erfassen, auszuwerten und kommerziell oder politisch zu nutzen. Es geht darum, unterschiedliche Datensätze zu kombinieren, Muster in diesen kumulierten Daten mit intelligenter Software aufzuspüren, um anschließend wertvolle und lukrative Schlüsse aus den Ergebnissen zu ziehen. Daten erweisen sich so einerseits als Quelle für Innovation, Kreativität und münden idealerweise in neue Geschäftsideen, Produkten oder Dienstleistungen ein. Andererseits kann durch Missbrauch die informationelle Datenhoheit gefährdet werden und die eigene Selbstbestimmung verloren gehen.

Das Internet legt sich in Kombination mit den modernen Kommunikationstechnologien bis zur Jahrhundertmitte als koronares Netz über die ganze Welt

Weltweit nutzten Ende der 2000er Jahre etwa 17 Prozent der Weltbevölkerung das Internet. Auf das Jahr 2010 bezogen waren das etwa 1,23 Milliarden Menschen. Im Jahr 2015 waren es dann schon gut 2,5 Milliarden Internetnutzer. Geht diese Entwicklung weiter braucht es wenig Phantasie um zu erkennen, dass sich das Internet in Kombination mit den modernen Kommunikationstechnologien bis zum Jahr 2050 als koronares Herzkranzgefäß komplett um die Welt legt und alle Menschen mit den immer wichtigeren Informationen versorgt.

Ohne dieses Netz wird das Herz der Welt im übertragenen Sinn nicht mit Blut und Sauerstoff versorgt. Obwohl das Nutzungsverhalten unterschiedlich ist, wird der Gebrauch des Netzes gerade auch im Alltagsleben über elektronisch geführte militärische Operationen, internetbasierte Finanztransaktionen, modifizierte Kommunikationsgewohnheiten, neue Geschäftsmodelle, privates Konsumverhalten, internationales Gaming, private Netzwerkpflege oder elektronisch intensivierte Familienkontakte immer alltäglicher – und in der Konsequenz existenzfördernd oder sogar lebenserhaltend. Soziale Netzwerke wie Facebook, Twitter, Xing, Snapchat oder Linkedin sind alltägliche Adressen der ›Netizens‹, die längst keine ›Nerds‹[13] mehr sind. Das Netzt bannt oder ängstigt niemanden mehr. Es ist Normalität. Zugleich aber Segen und Fluch. Das Internet gestattet es, dass wir durch den Zugang zu großen Wissensbeständen klüger werden und die Menschen ihr Leben mit Hilfe der neuen Technologie sinnvoll gestalten können.

Wikipedia ist eines der genialsten Projekte der Internetgesellschaft

Eines der wichtigsten und bemerkenswertesten Projekte des Internet und der Wissensgesellschaft war hierbei die Gründung von Wikipedia. Dies ist ein 2001 gegründetes Projekt zur Erstellung eines freien Onlinelexikons in zahlreichen Sprachen. Wikipedia ist zum meistgenutzten Online-Nachschlagewerk der Welt geworden und liegt auf Platz sieben der meistbesuchten Websites auf der Welt! Etwa 35 Millionen Artikel der Wikipedia in mehr als 28 Sprachen werden in Mehrautorenschaft von unentgeltlich arbeitenden Freiwilligen konzipiert, verfasst und nach dem Prinzip des ›kollaborativen Schreibens‹ fortwährend gemeinschaftlich korrigiert, erweitert und aktualisiert. Das Ziel von Wikipedia ist es, eine frei lizenzierte und qualitativ hochwertige Enzyklopädie zu schaffen und weltweit zu verbreiten. Jeder Internetnutzer kann Wikipedia nicht nur lesen, sondern auch als Autor (allerdings unter Kontrolle der Wikipedia-Community) daran mitwirken. Um Inhalte zu verändern, ist eine Anmeldung nicht erforderlich. In einem offenen Bearbeitungsprozess hat Bestand, was von der Gemeinschaft der Mitarbeitenden akzeptiert wird.[14] Damit hat Wikipedia eine revolutionäre Bildungsfunktion. Während in Deutschland zum Beispiel die Enzyklopädie Brockhaus über Jahrzehnte für etwa 3.000 bis 5.000 Deutsche Mark verkauft wurde, gibt es Wikipedia umsonst. Die Inhalte des Brockhaus waren überaus wertvoll, konnten aber von niemand öffentlich kontrolliert oder sogar korrigiert werden und das Wissen verfiel innerhalb der rasant zunehmenden Halbwertzeit von Information rasant.

---

13 | Als Nerds (englisch) bezeichnet man Computerfreaks, die als genial aber sonderbar und als kontaktarm im Alltagsleben gelten.

14 | Vgl. https://de.wikipedia.org/wiki/Wikipedia, aufgerufen am 17. Oktober 2015.

Jedermann kann das Netz für sich nutzen, für Unternehmensgründungen, für soziale Projekte oder politische Partizipation (Urchs/Cole 2014). Es ermöglicht zahllose praktische Hilfestellungen im Alltag der Menschen, verführt aber andererseits auch zu seinem Missbrauch. Dies bezieht auch kriminelle Aktivitäten, die über das Internet abgewickelt werden, mit ein. Der Verein Mimikama[15] klärt zum Beispiel über Missbrauchsmöglichkeiten auf, die strafrechtlich bzw. zivilrechtlich relevant sind. Dabei geht es etwa um Verletzungen der Privatsphäre, Abonnements-Fallen, Spam-mails, Betrug oder elektronisches Stalking.

Die Digitalisierung hat auch die Politik grundlegend verändert

Die Digitalisierung schafft einen neuen Aggregatzustand der Politik. Politische Prozesse werden innerhalb des E-Government, der E-Democracy, des E-Campaigning und der E-Administration zunehmend digital – und direkt. Damit bedeutet es eine Demokratisierung von Information und prägt das Verhältnis von Bürger und Staat. Im Wahlkampf spielten zum Beispiel internetbasierte Wahlkampfstrategien in der jüngeren Vergangenheit eine immer bedeutsamere Rolle. Dies ist ein wichtiger Aspekt hinsichtlich der politischen Erreichbarkeit und Beeinflussung der Bürger. Exemplarisch hat dies der digital organisierte Wahlkampf von US-Präsident Barak Obama gezeigt. Er hatte zum Zeitpunkt seiner Wahl 2009 ca. 31 Millionen Facebook-Fans, 250.000 Youtube-Abonnenten und 21 Millionen Twitter-Folger. Vor ihm hatte es der republikanische Senator John McCain Anfang der 2000er Jahre schon vorgemacht. Mit einer für ihn eingerichteten Website erreichte er 20 Prozent mehr Wähler als mit herkömmlichen Methoden. Die Einrichtung der Seite kostete 300.000 US-$. McCaine konnte auf diesem Weg 5,6 Millionen US-$ an Wahlkampfspenden akquirieren (Weidenfeld/Turek 2002: 69). Für die ›Campaigner‹ des deutschen Wahlkampfs 2013 war dies eine zielführende Botschaft. Insofern wurde der internetbasierte Wahlkampf auch in Deutschland wichtig. Die Evolution des Internet zu einer Big Data Plattform hat auch den Bereich der Open Government Data entwickelt. Damit wurden intransparente Behördenabläufe transparent und der Dienstleistungscharakter von Behörden wurde spürbar verbessert. Ende 2013 verpflichteten sich die G8-Mitglieder mit der Unterzeichnung einer Open Data Charter dazu, gewisse Prinzipien zur Öffnung ihrer Datenbestände zu implementieren. Dazu gehört unter anderem die Auskunft darüber, was der Staat an Steuergeldern in seinen Haushalten zu welchem Zweck verwenden will.

Das Netz stimuliert Impulse für Bildung und Arbeitsmärkte. Es hat neue Elemente in die klassischen Gütermärkte oder Dienstleistungsbereiche ge-

15 | Vgl. http://verein.mimikama.at/, aufgerufen am 17. Oktober 2015.

bracht und eröffnet die Möglichkeit, einen wirksamen Beitrag zur Reduktion von Transport- und Verkehrsströmen zu leisten. Auch die Optimierung elektronischer Steuerungen von Industrieanlagen kann den Energieeinsatz und den Schadstoffausstoß drosseln, wenn die digitalen Möglichkeiten nicht durch Manipulationen von Emissionsdaten wie bei dem deutschen Autobauer Volkswagenwerke (VW) 2015/2016 diskreditiert werden. Gerade der Blick auf die Schadstoffemissionen zeigt, welch wichtige Rolle die Digitalisierung der Information und ihr industrieller Einsatz spielen kann, um konsistente Lösungen zu entwickeln und so einem entscheidenden Kriterium der Nachhaltigkeit zu entsprechen. Der Einsatz der digitalisierten Informationstechnologien entfaltet ein bemerkenswertes Potenzial für sinnvolle, nachhaltige und akzeptable Lösungen industrieller Produktionsweisen und des Alltagslebens. Zu letzterem gehören auch alle Möglichkeiten eines digital ›unterstützten‹ Lebens, das insbesondere im demographischen Wandel Alterungsprozesse sinnvoll fördern kann (Connected Living oder Ambient Assistant Living, AAL). Es geht hierbei um alle elektronischen Möglichkeiten im eigenen Haus oder Wohnbereich, die ein unauffällig technisch unterstütztes Leben im Alter ermöglichen. Hierbei spielen Lösungen eine zentrale Rolle, die gesundheitstelematische, architektonische und sozial-kooperative Komponenten zu funktionierenden Lösungsmodellen mit Blick auf den demographischen Wandel und die zunehmende Alterung der Menschen verbinden.

Der gesellschaftliche und politische Nutzen von Big Data ist also bemerkenswert

Data-Mining erhöht nicht nur den volkswirtschaftlichen Nutzen. Es wird zunehmend auch dafür eingesetzt, gesellschaftliche Probleme zu mildern. Big Data lässt sich also nicht nur auf kommerzielle Interessen oder die Möglichkeiten verkürzen, die sich in den sozialen Netzwerken mit den Anwendungen digitaler Ökosysteme verbinden. Big Data bietet das Potenzial, gesellschaftliche Probleme im Gesundheitswesen, im sozialen Miteinander oder im Umweltschutz anders und erfolgreich anzugehen. Der Begriff steht auch für Entwicklungspotenziale in Wissenschaft und Forschung. Nicht zuletzt die Zukunftsforschung, die Prognostik oder die Bildung von Szenarios werden durch Methodik und Modell des Big Data enorm stimuliert. Wie wir im Bereich der Gesundheitstelematik schon gesehen haben, sind die Informations- und Kommunikationstechnologien wichtig für Medizin und Pflege. Big Data erhöht den Nutzen solcher Technologien durch Innovationen im Bereich Pandemien und Reaktion. Zurzeit geht zum Beispiel viel Zeit verloren im Prozess der Übertragung von Daten zur Entstehung von Grippeerkrankungen und der Reaktion des Gesundheitssystems, die ohne den Einsatz von Big Data bei rund zwei Wochen liegt. Ergänzend zu den amtlichen Meldeverfahren bietet Google seit

einiger Zeit deshalb den Internet-Tool »Google Grippe-Trends« an (Ginsberg 2009; Dapp/Heine 2014: 26f.). Demnach soll ein auf Algorithmen beruhendes Frühwarnsystem verwendet werden, um zeitnaher oder präventiv aktiv zu werden. Durch Suchvolumenanalysen mit Bezug auf grippale Symptome hat sich gezeigt, dass sich Suchanfragen zu Beginn einer Grippewelle überdurchschnittlich häufen. Der nachträgliche Datenvergleich mit tatsächlichen Krankheitszahlen der Gesundheitsbehörden hat gezeigt, dass die auf den elektronischen Suchanfragezahlen basierenden Ergebnisse mit den tatsächlichen Krankheitszahlen weitgehend übereinstimmten. Auf dieser Basis lassen sich also exakte Schätzungen zur aktuellen Grippelage anstellen, was den Behörden Zeitvorsprünge gewährt und es erlaubt, Grippe-Epidemien schneller zu bekämpfen.

Die Implementierung der Informations- und Kommunikationstechnologien realisiert aber auch beträchtliche politische, rechtliche und soziale Probleme

Die digitale Gesellschaft eröffnet in ihrem gegenwärtigen Entwicklungszustand bemerkenswerte Entwicklungsmöglichkeiten. Der Begriff der digitalen Revolution ist damit nach wie vor angebracht. Eine hochtechnisierte Gesellschaft kann über Informationsoperationen der aggressiven, kriminellen, terroristischen Art aber auch empfindlich getroffen werden. Infrastrukturen in Politik, Wirtschaft und Gesellschaft sowie ihre Vernetzungen wurden von der Informations- und Kommunikationstechnologie abhängig und dadurch verwundbar. Es entstanden so eine Reihe von gravierenden Problemen, die auch Globalisierungsprobleme sind:

- Der gläserne Mensch und die ›dunkle Seite der Macht‹;
- Computer- und Netzwerkkriminalität;
- Cybermobbing;
- staatliche Überwachung von Lebensstilen, politischen Verhaltensweisen oder privaten Konsumgewohnheiten;
- ›Liquid Democracy‹ und Schwächung der repräsentativen Demokratie;
- Gefährdung der Privatheit;
- fehlender Datenschutz;
- Zugang zum Netz (Access).

Die Macht der Algorithmen

Die Problemzonen der Informations- und Kommunikationstechnologien fordern eine zeitgemäße Strategie der Digitalisierung heraus. In Deutschland wurde dies nach der Bundestagswahl 2013 erstmals auch institutionell um-

gesetzt, als das Verkehrsministerium ausdrücklich eine Kompetenz für eine Politik der Digitalisierung erhielt und in das ›Bundesministerium für Verkehr und Digitales‹ umbenannt worden ist. Alle Parteien haben auf Bundes- und Landesebene mittlerweile Arbeitskreise für die digitale Gesellschaft etabliert. In keinem anderen Bereich ist dies 2013 so deutlich geworden wie im Bereich Datensicherheit und dem Schutz der Privatheit der Bürger. Das Gehabe von Geheimdiensten war Anfang der zweiten Dekade des 21. Jahrhunderts schockierend. Julien Assange und andere Desperados des Informationszeitalters haben insbesondere in den 1990er Jahren investigativ und verdeckt ermittelt und zum Ende ihrer ›bemerkenswerten‹ Karrieren die Verwundbarkeiten von Unternehmen und Behörden dokumentiert. Edward Snowden hat den Wahn herumschnüffelnder Hightech-Nationen in dramatischer Weise enthüllt. Snowden zeigte den stillen und unsichtbaren Krieg der USA gegen den internationalen Terrorismus in einer als historisch einzustufenden Art und Weise an. Mit dem Snowden-Skandal wurde das ganze Ausmaß der Massenüberwachung der amerikanischen Geheimdienste und auch angeschlossener Dienste in anderen Ländern transparent. Mittels einer relativ simplen technischen Überwachungsmethode mit Algorithmen im Internet wird jeder ausgespäht. Die Bevölkerung eines jeden Landes steht zunächst einmal unter Kollektivverdacht – es gibt in Wirklichkeit keine Privatsphäre mehr (Greenwald 2014; Rosenbach/Stark 2014).

In der Folge wurden auch die Verstrickungen anderer Staaten in diese Aktivitäten deutlich. Dies betraf etwa Großbritannien und die Bundesrepublik Deutschland. Beide Länder gerieten im Gefolge dieses ›Sturms‹ heftig in Schlagseite. Der Vorfall ist Ausdruck eines Dramas im Informationszeitalter. Es ist total global. Als George Orwell in den Jahren 1946 bis 1948 sein weltberühmtes Buch »1984« schrieb und 1949 veröffentlichte, hatte er die Horrorvision eines totalitären Präventions- und Überwachungsstaats vor Augen, der um die schiere Macht willen seine Bürger im tollwütigen Wahnsinn des Totalitarismus programmiert, kontrolliert und drangsaliert (Orwell, 1950). Eine lautlose und unsichtbare Überwachung und Kontrolle innerhalb eines demokratischen Systems hat er sich dabei als subtile Variante der ›Überneugier‹ des großen Bruders so sicherlich nicht vorstellen können. Auch wenn von einer ungeheuren Verselbstständigung der Geheimdienste im Krieg gegen den Terror ausgegangen werden kann oder muss, ist die NSA-Abhöraffäre als ›Super-GAU‹[16] für den liberalen und demokratischen Rechtsstaat 2013/2014 schlechthin zu einer schweren Belastungsprobe für das demokratische System

16 | GAU bezeichnet den größten anzunehmenden Unfall. Der Begriff wurde mit großen Technikunfällen und hier insbesondere mit Blick auf die Risiken der Nuklearenergie in Zusammenhang gebracht. Herausragende Beispiele dafür sind Kernkraftwerkhavarien im amerikanischen Harrisburg, im ukrainischen Tschernobyl oder im japanischen Fukushima.

der westlichen Welt und ihre ›freundschaftlichen Beziehungen‹ untereinander geworden. Der deutsche Journalist Frank Schirrmacher bezeichnete sie als den ersten großen Zivilisationsbruch des digitalen Zeitalters. Stefan Aust und Thomas Amman gehen noch weiter. Sie sprechen von der digitalen Diktatur, von der Geißel von Totalüberwachung, Datenmissbrauch und Cyberkrieg.

Die amerikanische NSA, deren Hauptquartier in Fort Meade den Beinamen ›Crypto City‹ trägt, ist der mächtigste Geheimdienst der Welt und das wohl wirkungsvollste Instrument staatlicher Überwachung. Der amerikanische Geheimdienstexperte James Bamford beschreibt die seit den 1930er Jahren andauernde Geschichte der NSA als einen Prozess der zeigt, wie George Orwells ›Big Brother‹ Wirklichkeit wurde. (Bamford 2001). Der Agentur geht es heute nach einer Selbstdarstellung um nichts anderes als die ›Information Superiority‹ in der Welt. Das bedeutet die informationelle Vorherrschaft. Aust und Amman beziehen die großen Internetkonzerne in das Bild der digitalen Diktatur mit ein, weil sie sich in einer Art Public-Private-Partnership gegen Bezahlung direkt von Apple, Google, Facebook und Co. mit Kundendaten beliefern lassen. Dies zeuge von der Entstehung eines neuen militärisch-industriellen Komplexes. Silicon Valley betreibe, aktualisiere und monetarisiere die Infrastruktur, während die NSA darauf nach Belieben zugreifen kann (Aust/Amman 2014: 13). Nach dem Internetkritiker Evgeny Morozov präsentiere sich die USA mit dieser Zusammenarbeit in ihrer ganzen Pracht. Mit dieser Teilprivatisierung könnten die Dienste gesetzliche und datenschutzrechtliche Bestimmungen einfacher umgehen. Gleichzeitig erweiterten sie das Spektrum der Zugriffs- und damit der Kombinationsmöglichkeiten fast bis ins Unendliche (Morozov 2014). Wikileaks-Gründer Julian Assange, Jacob Appelbaum und Andy Müller-Maguhn fassen diese ganze Entwicklung unendlich ernüchternd in die Worte: » Das Internet, unser großartigstes Emanzipationsmittel, hat sich in den gefährlichsten Wegbereiter des Totalitarismus verwandelt, mit dem wir es jemals zu tun hatten« (Assange/Appelbaum/Müller-Maguhn 2013). Durch die Möglichkeiten der staatlichen Totalüberwachung sei das weltweite Netz zur Bedrohung der menschlichen Zivilisation geworden, die direkt in einen postmodernen Überwachungs-Albtraum münde, aus dem es für niemanden außer den Gewieftesten ein Entrinnen geben werde (ebd.). Insofern gelte eine Annahme aus früheren Tagen, dass nämlich das Internet die Welt nur demokratischer mache, nicht mehr. Bei allen Fortschritten, die das Internet für politische Partizipation und Verwaltung bringt, wurde im Zeitverlauf klar: Bürger fühlen sich gläsern, von Staaten und Konzernen gleichermaßen durchleuchtet (Borchardt 2015).

Der gläserne Mensch und die ›dunkle Seite der Macht‹

Ein spezielles Problem beim allumfassenden Einsatz von Informations- und Kommunikationstechnologien ist die Big-Data-Problematik. Hierbei geht es um unverhältnismäßige Überwachungsvorhaben des Staates oder kriminelle oder wenigstens sittenwidrige Manipulationen von Unternehmen. Hier sind besonders große internationale Internetplattformen wie Google, Amazon, Linkedin, Facebook, AOL oder Apple gemeint. Im Gegensatz zu dem Vorwurf einer heimlichen Bespitzelung von Menschen geht es hierbei darum, dass Bürger und Konsumenten zum Spielball der Interessen von ungebetenen Gesellen des Internetzeitalters werden, die Datenprofile von Menschen zu ihren Zwecken aufrufen und daraus Schlüsse ziehen, ob diese nun in der NSA, im BND, im MI6, im KGB oder in den krakenartigen Bit-Tempeln der internationalen Internetwirtschaft residieren. Besonders pointiert hat diesen Sachverhalt der Jahreskongress des Chaos Computer Club Hamburg Ende 2016. Die etwa 12.000 Teilnehmer waren sich dort mehr oder wenig einig, dass die potenziellen Überwachungs- und Manipulationsmöglichkeiten von Staat und Wirtschaft nunmehr ein kritisches Maß erreicht hätten (Brühl/ Tanriverdi 2016). Wurde einst der berühmte Roman von George Orwell ›1984‹ immer wieder als Sinnbild für totalitäre staatliche Überwachungspraktiken zitiert, bringt es der 2014 erschienene Roman ›Zero‹ des österreichischen Journalisten Marc Elsberg mit der Geschichte der oft tödlich endenden Manipulation von Menschen anhand von freiwillig gelieferten Persönlichkeitsprofilen in der Wirtschaft heute auf den Punkt (Elsberg 2014).

Noch weiter geht der Amerikaner Dave Eggers. Er liefert mit seinem Roman ›Der Circle‹ ein erschreckendes Portrait einer von einem gigantischen Medienmogul beherrschten Gesellschaft, in der eine Fusion von Google, Facebook und Twitter angedeutet wird und die die größte Datensammelmaschine der Welt erschafft. Zum Wohle der Menschen und der Gesellschaft? Natürlich nicht. Die Transparenz der Daten hat ihren Preis. Dies bemerken die Nutzer aber nicht. Sie zahlen am Ende mit ihrer Freiheit. Gemeinsam mit den Erkenntnissen zu den Ausspähpraktiken des Staates (Greenwald 2014.), ergibt sich daraus ein Bild der technischen Möglichkeiten, nahezu jeden Menschen der Erde mittels seines elektronischen Kommunikationsverhaltens zu erfassen, zu katalogisieren, zu interpretieren und gegebenenfalls zu manipulieren. Dies hat auch der Internetpionier und Träger des Friedenspreises des Deutschen Buchhandels 2014 Jaron Lanier mit seinem Buch »Wem gehört die Zukunft. Du bist nicht der Kunde der Internetkonzerne. Du bist ihr Produkt« eindrucksvoll illustriert (Lanier 2014). Demnach sind die Internetkonzerne mit ihren technologischen Möglichkeiten, alle diese Informationen auszuwerten und weiterzuverkaufen, am Ende die wahren Profiteure. Die dazu notwendigen Informationen hinterlassen die Menschen freiwillig oder unfreiwillig im Netz und sind blind dafür,

dass sie den Schatz ihrer Persönlichkeit dabei fahrlässig auf einem unsichtbaren Marktplatz feilbieten. Und einige ›Cyber-Totalitaristen‹ des Silicon Valley sind weiterhin berauscht von ihrer Technik und ihren Möglichkeiten und denken nicht daran, sich in ihrem Machbarkeitswahn an der Debatte um ethische oder politische Fragen der Netzregulierung ernsthaft zu beteiligen.

Der digitale Fußabdruck produziert einen gewaltigen Trampelpfad im Netz

Die gesamte Big Data-Problematik wurde Anfang März 2014 in einer Studie von Thomas F. Dapp und Veronika Heine von der Forschungsabteilung der Deutschen Bank ›Deutsche Bank Research‹ hervorragend thematisiert (Dapp/Heine 2014). Sie beschreiben dort den Stand der Entwicklung digitaler Ökosysteme und zeigen auf, wie das System überhaupt funktioniert und welche Problematiken sich daraus ergeben. Wenn Menschen mittels stationärer und mobiler Endgeräte im Internet surfen, hinterlassen sie über die IP-Adresse oder die freiwillige Registrierung als Kunde und Nutzer Datenspuren, die man auch den ›elektronischen Fußabdruck‹ nennt. Diese Fußabdrücke werden mittels der Big Data – Technologien immer deutlicher und präziser und leichter aufzuspüren.

Insbesondere auf den großen Internetplattformen wie Google, Facebook oder Xing und Linkedin werden im Laufe der Zeit von den ›Usern‹ eine Fülle von Daten so freiwillig hinterlegt. Dies sind nicht nur geschäftliche oder kommerzielle Daten; private und intime Informationen in Wort und Bild finden sich dort ebenso wie Präferenzen für Filme oder Musik, Reisewünsche und Konsumgewohnheiten. Jede gefolgte oder selbst erstellte Nachricht auf Blog-Diensten drückt auch eine Meinung oder individuelle Präferenz aus. Durch die Verknüpfung der einzelnen Tweets[17] kann schnell und einfach ein Profil über politische oder gesellschaftliche Neigungen des Nutzers erstellt werden. So lassen sich Interessen, Neigungen, Meinungen oder sexuelle Obsessionen ablesen, die man später für gezielte Ansprachen der Individuen zu eigenen Zwecken nutzen und insbesondere geldwert umsetzen kann. Während früher eindimensionale Kundeninformationen via Adressverkauf oder singuläre Einkaufsinformationen diffuse Rückschlüsse auf einzelne Kundenpräferenzen zuließen, erlauben sowohl detaillierte als auch komplexe Nutzerprofile mittlerweile eine relativ totale Erfassung einer Person. Digitale Fußabdrücke werden zu handelbaren und begehrten Profilen.

Mittlerweile ist praktisch jedermann in digitale Ökosysteme privat und/oder geschäftlich integriert. Viele Lebens- und Arbeitsbereiche werden durch die Digitalisierung durchdrungen, und viele nützliche Tools wie Suchmaschinendienste, Software, email-Dienste, Cloud-, Wiki- oder Streaming-Dienste

17 | Tweets (englisch) meint Piepser oder Gezwitscher (wie das Synonym Twitter).

sowie Märkte für digitale Güter erleichtern das Leben. Über die Registrierung der Nutzer oder ihre elektronische IP-Adresse können Suchbewegungen der Nutzer gespeichert, zusammengeführt und ausgewertet werden. Und das ultimative Zukunftsprojekt des Silicon Valley ist: der Mensch als Datei in der Cloud. Selbst Datensparsamkeit und Vorsicht sind für die Datendetektive des Internet aufschlussreich. Denn auch sie lassen Rückschlüsse auf Charakter und Persönlichkeit eines Netizens[18] zu.

»Denn sie wissen, was wir tun«

Beide Autoren haben sich die Mühe gemacht, einen fiktiven Fußabdruck im Internet zu entwickeln, so dass jedermann einen Eindruck bekommen kann, was ein aussagekräftiges Profil im Internet für ein Individuum bedeuten und an Konsequenzen haben könnte. Sie laden uns ein, uns vorzustellen, dass wir aufgrund einer Datenpanne oder dank eines Whistleblowers[19] zufällig an einen persönlichen Datensatz gelangen, der von einem auf Datenerhebung spezialisierten Unternehmen oder einem Geheimdienst stammt. In Ihrem Profil könnten sie folgendes lesen:

»X ist männlich, 43 Jahre promovierter Ingenieur, verheiratet mit V., weiblich, 37 Jahre; X lebt mit Individuum V in Ein-Familienhaus in Frankfurt und hält eine Katze; X bezieht regelmäßig das Magazin ›Schöner Wohnen‹ sowie das digitale Abo des ›Maschinenbauers‹ direkt auf sein mobiles Endgerät der Marke A; X kauft regelmäßig Fachliteratur, Kleidung und Elektronik beim Onlinehändler A; X interessiert sich für diverse Umweltthemen und unterstützt mittels Dauerauftrag einige internationale NGOs; X interagiert mehrmals täglich auf diversen sozialen Netzwerk-Plattformen über mobile und stationäre Geräte und unterhält überdurchschnittlich viel Kontakt zu den Individuen H (männlich, 41 Jah-

18 | Netizens ist ein Kunstwort, das die englischen Begriffe Net (Netz) und Citizen (Bewohner) zusammenführt. Es meint, dass Individuen eine Technologie wie das Internet nicht ›nur‹ nutzen, sondern sich in der Sphäre des World Wide Web sozial umfänglich und quasi wohnlich einrichten.

19 | Ein Whistleblower ist eine Person, die ausspähende (und später manipulierende) Aktivitäten staatlicher oder kommerzieller Internetnutzer seitens Dritter an die Öffentlichkeit weiter sagt (d.h. an die Öffentlichkeit weiter »wispert«). Seit der Enthüllung des Watergate-Skandals in den USA, der Präsident Nixon aufgrund der Informationen einer »wispernden« Stimme einer Quelle namens »Deep Throat« zu Fall brachte, bezeichnet dieser Begriff eine bestimmte Art von Enthüllungsmechanismen von Informationen, die für die Öffentlichkeit, sozial, wirtschaftlich oder politisch hoch relevant sind, die aber niemand ohne diese Ermittlungsarbeit so erfährt. Edward Snowden hat diese Chiffre der investigativen Öffentlichkeitsarbeit dann 2014 mit einer weiteren spektakuläre Aktion hinsichtlich der ausspähenden Aktivitäten des amerikanischen Inlandgeheimdienstes NSA komplettiert.

re), S. (weiblich, 29 Jahre), und K. (weiblich 35 Jahre); X konsumiert Video-on-Demand-Angebote und surft im Schnitt eins bis zwei Stunden täglich ab 22.00 Uhr im Internet; X unterhält mehrere Kontoverbindungen zu den deutschen Banken D und P sowie der schweizerischen Bank U; X bevorzugt digitale, webbasierte Bezahlmethoden; X besitzt zwei Kreditkarten der Anbieter M und A, Kreditkarte M wird auch von Individuum V (Ehefrau) mitbenutzt, Umsätze laufender Monat der Kreditkarte A: Reiseführer Paris EUR 9,95, Flugreise nach Paris für zwei Personen EUR 379,00 Hotel Paris EUR 440,00 Gastronomie Paris EUR 90,00, Schmuck Paris EUR 399,00, Umsätze laufender Monat der gemeinsam genutzten Kreditkarte M: keine Umsätze; X kauft regelmäßig Sportartikel für Outdoor-Aktivitäten; X lässt sich vermehrt Angebote diverser Kfz-Anbieter zumailen (ist folglich im Begriff, ein Fahrzeug zu kaufen/zu leasen/zu mieten); X vergleicht Preise von Stromanbietern (wägt eventuell einen Stromanbieterwechsel ab); X bucht jährlich online Winterurlaube in Österreich und leiht im Voraus online die Skiausrüstung bei zwei Anbietern (neigt ansonsten zu Fernreisen mit Individuum V und kurzen Städtereisen, zuletzt mit Individuum S (X unterhält höchstwahrscheinlich partnerschaftliche Beziehung zu Individuum S). X bezieht mehrmals im Quartal rezeptpflichtige Medikamente (X ist Allergiker, neigt zu hohem Blutdruck), X besucht regelmäßig unterschiedliche Foren und partizipiert an Diskussionen zu seltenen Krankheiten (X benutzt hierfür entweder den anonymen Avatar ›neugierig‹ oder ›curious_1970‹). X besitzt Kfz-, Haftpflicht-, Rechtsschutz- und Hausratsversicherung von Unternehmen A; X bezog 2012 juristische Dienste von Unternehmen A in einem Verkehrsdelikt-Prozess, der Prozess ist noch im Gange. Echtzeit-Zusatzinformation: im Moment hält sich Individuum X in der Seitensprungstraße 7 auf. Hier wohnt Individuum S« (ebd.: 19).

Der gläserne Mensch ist ein kostbares Gut

Ein solches Datenprofil ist heute hinsichtlich der vielen digitalen Fußabdrücke, die der Mensch im Internet hinterlässt sowie der verfügbaren Datenanalyse-Tools realistisch und technologisch machbar. Auf diese Weise ist es möglich, kontextübergreifende zeitliche Abläufe und digitale Profile über Aufenthaltsorte, soziale Beziehungen, Konsum- und Mediennutzungsverhalten, Gesundheit, Einkommen, Beruf, Neigungen oder Abgründe der Persönlichkeit zu erstellen. Und jede Information in diesem Profil hat einen ökonomischen Wert. Es ergeben sich Anknüpfungspunkte für die Wirtschaft (zum Beispiel Versicherungsunternehmen, Konsumgüterhersteller), Wissenschaft (zum Beispiel Neurologie, Soziologie, Medizin) oder Politik (zum Beispiel Finanzamt, öffentliche Verwaltung, Geheimdienste, Sozialämter). Dapp und Heine rechnen dabei im Rahmen einer Modellrechnung vor, welchen Wert solche digitalen Profile haben könnten. Die Marktkapitalisierung von Facebook betrage etwa 70 Milliarden Euro und das Unternehmen werbe mit einer Anzahl von Facebook-Nutzern von über 1,2 Milliarden. Der monetäre Wert eines durchschnittlichen Nutzerprofils könnte sich durch Division auf etwa 58,00 Euro belaufen.

Unter der weiteren Annahme, dass nur zwei Drittel der Konten aktiv sind, erhöht sich der Wert auf 88,00 Euro. Diese Kalkulation könnte die Basis für Verhandlungen über den Preis einzelner Nutzerprofile zwischen Investoren oder sonstigen Akteuren sein. Gegenüber den vielen anderen Phänomenen und Problemen von Big Data zeigt diese simple Modellrechnung auf, wie sehr es in diesem Kontext schlicht um finanzielle Interessen geht (ebd.: 20).

Im Ergebnis entstehen starke Log-in-Effekte in eingezäunten digitalen Ökosystemen. Internetplattformen und – unternehmen haben mittlerweile viele attraktive Dienste in ihrem Angebot. Gleichzeitig vergrößern sie aufgrund eines großen Stamms an loyalen Kunden und einer berechenbaren Liquidität ständig ihr Angebot mit neuen Produkten und Diensten, wobei sie auch in branchenfremden oder branchenübergreifenden Bereichen tätig werden. So entwickelte Google ein Smartphone und eine web-basierte Brille und will zukünftig verstärkt in Haushaltsgeräte und Robotik investieren. Während Amazon ursprünglich als internetbasierter Buchhändler an den Start ging, handelt das Unternehmen heute zusätzlich mit Haushaltsgeräten, Unterhaltungselektronik oder Film- und Musiktiteln. Sie festigen ihre Position und erhöhen ihre Attraktivität, in dem sie für eine hohe Verfügbarkeit von komplementären Internet-Diensten und Apps sorgen.

Für Unternehmen bedeutet dies lukrative Geschäfte, für Staaten und ihre Geheimdienste optimierte Aufklärung, für gesellschaftliche Gruppen zielgenaue Ansprechmöglichkeiten für soziale Unterstützung. Viele Bürger werden trotz der Ausspähungsmöglichkeiten und ihrer potenziellen Manipulierbarkeit die Services und Informationsmöglichkeiten der internetbasierten Anbieter trotz ihrer Risiken für die Privatheit und persönliche Integrität weiter nutzen. Facebook etwa legte im Juli 2014 neue Zahlen hinsichtlich der Nutzer vor und verzeichnete trotz der Snowden-Affaire und anderer Skandale mit Blick auf Datenmissbrauch steigende Mitgliederzahlen. Das Unternehmen hatte bis 2014 1,32 Milliarden aktive Nutzer pro Monat! Sie und die damit verbundenen Sekundäreinahmen haben dem Konzern im ersten Quartal 2014 61 Prozent mehr Umsatz eingebracht als im Vergleichsquartal des Vorjahres. Aktuell sind es 2,9 Milliarden US-$.[20] Dies lässt für den Augenblick nicht den Schluss zu, dass ein Bewusstsein entsteht, dass die Nutzer zu einem hohen Grad manipulierbar und transparent geworden sind oder sich ihrer Datenhoheit beraubt fühlen. Daten- und Verbraucherschützer sehen die Verknüpfung von privaten und intimen personenbezogenen Daten und ihren Transfer zwischen einzelnen Firmen im Internet indes mit wachsender Besorgnis.

Das Internet der Dinge und die Industrie 4.0 bieten Möglichkeiten, die in der Tat für Wirtschaft und Gesellschaft revolutionär sind. Im Kontext des gro-

20 | Vgl. http://business.chip.de/news/Facebook-1-32-Mrd.-Nutzer-bringen-3-Mrd.-Dollar_71184875.html, aufgerufen am 24. Juli 2014.

ßen Themas ›Big Data‹ erzeugt dies aber, wie bei jeder Revolution, auch große Probleme. Die deutsche Managerin Yvonne Hofstetter hat dies 2015 in einer für eine Unternehmerin ungewohnt offenen Art und Weise thematisiert. Sie sieht in der künstlichen Intelligenz, dem Internet der Dinge und der Industrie 4.0 Konfliktpotenzial, wägt schließlich aber Chancen und Herausforderungen sorgfältig ab. Sie führt in ihrem Buch »Sie wissen alles« aus:

»Was aber heißt intelligente Maschinen und worin besteht ihre Intelligenz. Intelligente Maschinen sind nicht mehr auf die Eingabe einer Handlungsanweisung durch den Menschen angewiesen, sondern lernen selbstständig. Als Optimierer lernen sie, optimale Entscheidungen unter Unsicherheit zu treffen. Als verteilte Software-Agenten zerlegen sie komplexe Probleme des Alltags in einfachere Suchprobleme und lösen sie durch Kooperation und Kommunikation miteinander. Als ›Emergentes System‹[21] vernetzen sich unabhängige Programme zu einer maschinellen Parallelwelt, die kein Programmierer je programmiert oder getestet hat und deren Dynamik wir weder kennen noch ohne weiteres analysieren können« (Hofstetter 2015: 13).

Nach den Enthüllungen Edward Snowdens haben solche Programme auch einen Namen. Beim Geheimdienst heißen sie PRISM, XKeyscore und Tempora. Diese drei Programme dienen der Überwachung und Analyse von Millionen von Daten zur Überwachung unzähliger unverdächtiger Bürger. In der Finanzindustrie entsprechen ihnen Aladdin oder Corsair. Als gigantische Datenanalysen liefern solche Programme globale Risiko- und Investmentinformationen. Damit beeinflussen sie das Börsengeschehen, mit schwer einschätzbaren Risiken für die globale Realwirtschaft. Intelligente Maschinen erledigen immer öfter ›Arbeiten für jedermann‹. Für Hofstetter haben wir nun einen Wendepunkt in der Industriegeschichte erreicht. Mit Big Data seien unsere technologischen Fähigkeiten grenzenlos. Und Regeln für die Informationsökonomie gebe es nicht, ebenso wenig wie eine politische oder gesellschaftliche Strategie für den künftigen Umgang mit intelligenten Maschinen (ebd.: 17).

Neben die spezielle Problematik von Big Data treten bekannte Probleme hinzu. Dazu gehören intensivierte und perfektionierte Hackeraktivitäten im Internet, um das Verhalten von Unternehmen oder Staaten auszuspähen und gegebenenfalls spektakulär an die Öffentlichkeit zu bringen. Hinzu kommen alle unschönen menschlichen Verhaltensweisen, die das Diffamierungspotenzial der anonymisierten Internetkommunikation speist.

21 | Ein ›Emergentes System‹ bezeichnet einen kybernetischen Kontext von Systemeigenschaften, die sich gegenseitig beeinflussen und eine Eigendynamik in ihrer Entwicklung realisieren. Das Ergebnis ist die zum Teil unkalkulierbare Herausbildung von neuen Eigenschaften oder Strukturen eines Systems infolge des Zusammenspiels seiner einzelnen Elemente.

Im Visier der Hackereliten: das Netz

In den 2010er Jahren wurden Aktivitäten von Gruppen wie LulzSec oder Anonymus publik, die durch ihren im Internet betriebenen ›Hacktivismus‹ auffällig geworden sind. Bekannt wurden hier insbesondere Hacker-Attacken auf Unternehmen wie Nintendo, Sony oder den US-Senat.[22] Insofern stilisiert der Vorgang die Politik der Digitalisierung zum Megathema der Politik des Informationszeitalters, der zum Beispiel auch Mitte 2014 wieder einmal mit einem Angriff von Hackern auf die Homepage der Europäischen Zentralbank und Mitte 2015 mit einer beachtlichen Cyber-Attacke auf den Deutschen Bundestag dokumentiert worden ist.

Es kommen andere Probleme hinzu. Computer- und Netzwerkkriminalität sind alltägliche Erscheinungen der Netzgesellschaften geworden, Cybermobbing eine hässliche Begleiterscheinung pubertierender und gehässiger ›Netizens‹ oder verwirrter Stalker, die nun eine technische Plattform für ihr Handeln etwa über soziale Netzwerke bekommen haben. Aufgrund der intensiven globalen Vernetzungen nehmen auch die Angriffsflächen für Terroristen und Kriminelle zu. Hackerterrorismus, elektronische Industriespionage oder das Auskundschaften von politischen und staatlichen Verhandlungsstrategien gehören heute ebenso zum Alltag des Netzes wie eine geschickte Manipulation von Öffentlichkeit oder selbstverliebte Jungenstreiche im pubertären Drogennebel, wie es die Hackerelite um Julian Assange in den 1990er Jahren vorgemacht hatte (Dreyfus/Assange 1997).

Auf staatlicher Ebene geht es um die Manipulation der Öffentlichkeit oder den Diebstahl von Staatsgeheimnissen bis hin zum Angriff auf kritische Infrastrukturen der Industriegesellschaft wie Kraftwerke, Telekommunikations- oder Stromnetze. Diese sind hoch kritische Infrastrukturen hochtechnisierter Gesellschaften. Cybercrime und Cyberwar sind zu alltäglichen Phänomen des globalen Informationszeitalters geworden. Bemerkenswert dabei ist, dass das Problem – gegenüber anderen Vorwarnungen der letzten 20 Jahre – heute nicht nur aktuell, sondern geradezu beklemmend intensiv geworden ist. Dabei zählt es 20 Jahre. Schon Mitte der 1990er Jahre ist klargeworden, dass Militär, Wirtschaft und Gesellschaft und ihre weitgehende Vernetzung von modernen Informationstechnologien abhängig werden würde. Und damit verwundbar durch informationstechnologische Operationen von Hackern im Auftrag von Unternehmen, Geheimdiensten oder Regierungen. Einen Vorgeschmack darauf lieferten Attacken auf das Pentagon sowie auf amerikanische Internetfirmen Anfang der 2000er Jahre, als ›Computerviren‹ und ›Trojaner‹ die Server vollständig verstopften und Geschäfte und Kommunikation darüber

22 | Vgl. www.golem.de/news/verhaftungen-luzsec-mitglieder-von-ihrem-anfuehrer-ans-fbi-verraten-1203-90296.html, aufgerufen am 29.12.2015.

vollständig zum Erliegen brachten. Internetexperten warnten in diesem Zusammenhang aber schon früh vor viel weitergehenden Attacken mit extremen Auswirkungen. So hat das Hamburgische Weltwirtschaftsinstitut (HWWI) ausgerechnet, was alleine in Berlin ein durch Hacker ausgelöster Stromausfall kosten würde: etwa 23 Millionen Euro – pro Stunde (Balser/Braun 2015).

›Industrielle Desorganisation‹ wird zu einem attraktiven Instrument der militärischen Gebrauchs des Internet

Seitdem sind technische Abwehrmechanismen ein ›heißes‹ Thema der Informatik. Neben die Möglichkeit der militärischen Nutzung treten die Gefahren der industriellen Desorganisation und anderer krimineller Machenschaften. Olaf Winkel, seinerzeit Geschäftsführer des Horst-Görtz-Institutes für IT-Sicherheit am European Center of Excellence for IT-Security an der Universität Bochum und andere wiesen (etwas sehr optimistisch) bereits Anfang 2000 auf die Möglichkeiten der elektronischen Sicherheit hin. Die Grundlage technischer Sicherheitsmaßnahmen sei die elektronische Kryptographie. Bei diesem Verfahren verfügen die Kommunikationsteilnehmer über identische Schlüssel, mit denen sie die füreinander bestimmten Nachrichten verschlüsseln oder entschlüsseln und damit den externen Zugriff auf eine vertrauliche Kommunikation verhindern können. Dies seien geeignete Wege, die den flächendeckenden Einsatz von leistungsfähigen Schlüsselsystemen in offenen Netzwerken wie dem Internet schaffen könnten (Winkel 2000). Der Ingenieur Reinhard Hutter hielt damals dagegen:

»Sicherheitsmaßnahmen wie Firewalls, Virenschutz, Virtual Private Networks (VPNs), digitale Signaturen und Verschlüsselung sind notwendig, aber nicht hinreichend, um mit Attacken auf komplexe Infrastrukturen umgehen zu können. […] Die naheliegenden Bedrohungen im Informationszeitalter werden von Sicherheitsexperten weltweit mit eben soviel Energie gesucht wie von Hackern und […] kriminellen Kräften im Hinblick auf Wirtschaftsspionage oder Terrorismus. […] Angreifer können Bedrohungen und Schwachstellen ausnutzen; die Gegenseite wird versuchen, sie zu identifizieren, zu verstehen, sie muss davor warnen und Gegenmaßnahmen entwickeln, diese anbieten und einsetzen« (Hutter 2000).

Da wurde ein Spiel aufgesetzt, welches sich lukrativ und lustvoll betreiben ließ. Das alles ist erst 15 Jahre her. Die Hinweise zur Cybersicherheit haben sich als Anfangswarnungen bewährt. Die zaghaften oder vereinzelten Bezüge auf die kriminellen und terroristischen Potenziale des Internet wirken heute aber naiv. Der Krieg im Netz indes hat sich in den 2000er und 2010er Jahren enorm intensiviert, wobei das Bundesamt für Sicherheit in der Informationstechnik 2015 von einer anhaltenden asymmetrischen Bedrohungslage im Cyber-Raum

gesprochen hat (Bundesamt für Sicherheit in der Informationstechnik 2015). Das bedeutet, dass verborgene Akteure des Darknet sich weiter formieren und auch mächtige Institutionen, Bürokratien oder Unternehmen mit ihren Guerillataktiken attackieren. Nach dem Lagebericht des Amtes zur Cybersicherheit 2015 war das Jahr 2015 geprägt durch eine Reihe von gravierenden IT-Sicherheitsvorfällen, die eine fortschreitende Professionalisierung der Angriffsmittel und Angriffsmethoden verdeutlichen. Dazu gehörten 2015 der Cyberangriff auf den Deutschen Bundestag und auf den französischen Fernsehsender TV5 Monde (ebd.).

Die Cybersicherheit ist auch ein zunehmendes Problem der Wirtschaft. Alleine in Deutschland waren 2014 gut die Hälfte aller Unternehmen Opfer von digitaler Wirtschaftsspionage, Spionage oder Datendiebstahl geworden. Dies ergab eine 2015 von Aris und Bitkom Research durchgeführte Umfrage, bei der die Geschäftsführer und Sicherheitsbeauftragten von 1.074 Firmen befragt wurden. Der am stärksten betroffene Wirtschaftszweig ist demnach die Automobilindustrie mit 68 Prozent der betroffenen Unternehmen, gefolgt von der Chemie und Pharmaindustrie mit 66 Prozent sowie Banken und Versicherungen mit 60 Prozent. Der entstandene Schaden beläuft sich für die gesamte deutsche Wirtschaft auf über 50 Milliarden Euro pro Jahr.[23]

Das am häufigsten auftretende Delikt ist der Diebstahl von IT- und Kommunikationsgeräten. In 28 Prozent der Unternehmen wurden Computer, Smartphones oder Tablets gestohlen. In 19 Prozent der Fälle wurden Mitarbeiter so manipuliert, dass sie sensible Daten weitergaben.17 Prozent der Unternehmen berichteten vom Diebstahl elektronischer Dokumente oder Daten und 16 Prozent von Sabotage ihrer IT-Systeme oder Betriebsabläufe. Bei acht Prozent wurde die elektronische Kommunikation ausgespäht. Häufigstes Ziel sind die IT-Systeme und die Kommunikationsinfrastruktur. In 20 Prozent der betroffenen Unternehmen hatten es die Angreifer auf die Bereiche Lager und Logistik abgesehen. Es folgen der Einkauf (18 Prozent), die Produktion (15 Prozent) sowie die Geschäftsleitung (14 Prozent). In neun Prozent der Firmen wurden die Forschungs- und Entwicklungsabteilungen (F&E) gehackt oder ausspioniert. Unter den großen Unternehmen ab 500 Mitarbeitern sind die F&E-Bereiche bei fast jedem Dritten (30 Prozent) betroffen. Fast ein Viertel des auf 51 Milliarden Euro geschätzten Schadens pro Jahr machen laut Bitkom Umsatzeinbußen durch Plagiate aus. Es folgten Patentrechtsverletzungen, die ähnliche Folgen wie Plagiate hätten. An dritter Stelle liegen Umsatzverluste durch den Verlust von Wettbewerbsvorteilen. Ein weiterer großer Posten sind Kosten infolge des Diebstahls von ITK-Geräten sowie Ausgaben, die durch den

23 | Vgl. das Referat der Studie von dem ZDF-Journalisten Björn Greif unter www.zdnet.de/88231934/bitkom-haelfte-der-deutschen-firmen-von-digitalen-angriffen-betroffen/, aufgerufen am 5. Mai 2015.

Ausfall von IT-Systemen oder die Störung von Betriebsabläufen entstehen. Hinzu kommen Imageschäden und ein Vertrauensverlust in Unternehmen, der schnell existenzgefährdende Formen annehmen kann.[24]

Totaler Cyberwar – an allen Fronten

Insofern begann in den 2000er Jahren ein virtueller Rüstungswettlauf. Er kannte keine eindeutigen Gegner und Feindbilder oder klare Konfliktlinien. Und somit keine erkennbaren Sammlungsräume von Flotten, Armeen oder Schützengräben, die man hätte optisch erfassen und militärisch präzise in einem Kosten-Nutzen-Szenario hätte bekämpfen können. Der Internetspezialist Arne Schönbohm stellte bereits Anfang der 2010er Jahre die aktuellen Aggressionspotenziale im Internet systematisch dar (Schönbohm, 2011, 2013). Er berichtet, dass zum Beispiel dem Sicherheitsunternehmen Comodo wichtige Internet-Zertifikate für Firmen wie Yahoo, Microsoft oder Google gestohlen wurden. Ein anderer Vorfall ist der Fall Cablegate. Hier wurden über die Internetplattform Wikileaks 140.000 vertrauliche Depeschen amtlicher Stellen der USA im Rahmen einer Indiskretion des amerikanischen Soldaten Bradley Manning veröffentlicht. Die damalige US-Außenministerin Hillary Clinton schäumte vor Wut. Schönbohm berichtet, dass Staaten kriegerisch motivierte Angriffe auf andere Staaten in der Regel nicht selbst durchführen, sondern Hacker mit diesen Cyberattacken beauftragen. Beispiele seien die ›roten‹ Hacker Chinas oder das Russian Business Network, das durchaus staatliche und private Aufträge des Cyberwars durchführe und er führt konkrete Beispiele wie das Spionageprogramm »Flame« an, das Rechner im Nahen Osten überwacht hat. Einen absurden Höhepunkt erreichte dieses Spiel im Jahr 2014, als (mutmaßlich) Nordkorea einen Hackerangriff auf die japanische Firma Sony verübte. Gegenstand des Angriffs war die Filmsatire »The Interview«. Der Film handelt von einem Attentat auf den nordkoreanischen Führer Kim Yong Un. Hacker hatten in diesem Zusammenhang über eine unerhörte Verhöhnung des Landes geklagt, die Rechte des Unternehmens an dem Film geschändet und mit Terror in den USA gedroht, falls dieser Film in die Kinos kommen würde. Auch hier war die Quelle des Angriffs vernebelt und die Spuren verliefen über nordkoreanische und chinesische Server im Nichts.

Darüber hinaus gewinnt der Cyberwar auch für die Gotteskrieger des IS eine starke Attraktivität (Boie et al. 2015). Es ist das erklärte Ziel des IS, komplex vernetzte Gesellschaften ins Chaos zu stürzen. Für diese Generation junger Terroristen ist der Gebrauch moderner Informationstechnologien sowohl kinderleicht als auch eine Selbstverständlichkeit. Diese Terrororganisation ist mittlerweile innerhalb ihres territorialen Terrains genauso kampfbereit und

24 | Vgl. ebd.

gefährlich wie virtuell. Zwischen 50.000 und 70.000 Nutzerkonten sollen IS-Terroristen oder ihren Sympathisanten gehören. Auch die Attentäter von Paris kommunizierten über Twitter. Über Propagandavideos mobilisiert und rekrutiert der sogenannte Islamische Staat Kämpfer, über das Internet verbreitet er durch Horrorbilder von Enthauptungen und Zerstörung im Vorfeld seiner konkreten militärischen Operationen einen solchen Schrecken, dass die angegriffenen Einheiten der Gegenseite schon vor der eigentlichen Attacke innerlich erstarren und schließlich die Flucht ergreifen. Und er droht, zentrale Infrastrukturen wie Wasser- und Energieversorger zu attackieren. Auch Flughäfen und Atomkraftwerke sind potenzielle Ziele. Es klingt paradox: trotz der archaischen Struktur und der mittelalterlichen Sehnsucht nach dem Kalifat beherrschen die Terroristen die Mittel der elektronischen Kriegsführung nahezu perfekt und sind sich der durchschlagenden Wirkung dieser Waffe in Zukunft mehr als bewusst.[25]

Die Grenzen zwischen Cyberwar und Cyberkriminalität werden durchlässig

Die Grenzen zwischen (staatlichem) Cyberwar und (privater) Cyberkriminalität verwischen sich. In Verbindung mit dem globalen Krieg gegen den Terrorismus ist das Internet Kriegsschauplatz. Allerdings ist das Schlachtfeld nicht nur auf den Terrorismus beschränkt. Für alle Staaten dieser Welt eröffnen Informations- und Kommunikationstechnologien und das Internet nach Land, Wasser, Luft und Weltraum eine fünfte Dimension der Kriegsführung. Seit 2010/2011 haben etwa die USA, Großbritannien, Frankreich, Deutschland, die Niederlande oder Indien operative Einheiten und nationale Strategien für Cybersicherheit etabliert. In den USA wurde diese Aufgabe dem US-Verteidigungsministerium zugeordnet, in Deutschland dem Innenministerium und in Indien dem ›Department of Information Technology‹ (Dunn/Cavelty 2012: 122). Dabei liegt zunehmend eine asymmetrische Bedrohung vor, die aus dem Cyberraum kommt und Staaten nutzen zunehmend mit immer größerer Raffinesse die Möglichkeit, getarnte und über ›private‹ Mittelsmänner durchgeführte Cyberangriffe auszuführen.

US-Verteidigungsminister Leon E. Panetta sprach Ende 2012 im ›Intrepid Sea, Air and Space Museum‹ in New York von einem »Cyber Pearl Harbour« und warnte mit Blick auf dieses sozialpsychologische Trauma der amerikanischen Nation davor, dass ganze Teile der amerikanischen Infrastruktur bei ›Nacht und Nebel‹ durch einen umfassenden Angriff aus dem Cyberspace lahmgelegt werden könnten. Er adressierte dies in bemerkenswert undiplomatischer Weise direkt an Russland, China, Iran und ›militante Gruppierun-

25 | Vgl. »Terrorkrieg im Internet«, in der ARD vom 13. Juli 2015.

gen‹.[26] Im Kontext der nordkoreanischen Cyberattacke im Dezember 2014 auf die Firma Sony sprach der amerikanische Präsident Obama von ›Cybervandalismus‹[27] und erwog, das Land wieder auf die Liste der Terrorhelfer-Länder zu setzen. Das Land reagierte mit dem wohlbekannten Reflex der Drohung einer nuklearen Aufrüstung und zeigte auf, dass auch im Internetzeitalter die brachialen Verhaltensweisen des Kalten Krieges gepflegt werden können. Im April 2015 demonstrierte schließlich auch die Terrororganisation IS mit einem umfangreichen Cyberangriff auf den französischen Fernsehsender TV 5, dass auch der internationale Terrorismus diese Spielart des Krieges mittlerweile souverän beherrscht. Unbekannte Hacker hatten in der Nacht vom 8. auf den 9. April 2015 das weltweite Programm des französischsprachigen Senders lahmgelegt und auf dessen Webseite Drohbotschaften der Terrormiliz IS hinterlassen. Dieser Angriff verdeutlichte erneut das Potenzial des Internet für eine zusätzliche Methode der Kriegsführung, und die veröffentliche Meinung reagierte sehr gereizt darauf, weil sensible Infrastrukturen einfach besser geschützt werden müssten.[28] Doch das Ausmaß der Bedrohung wächst. Profi-Ermittler und IT-Fachleute wissen nicht, ob sie der Gefahren der Cyberkriminalität noch Herr werden können und spüren, dass sie in einer kritischen Phase die Kontrolle über Teile des Internet verlieren könnten.

Für Cyberangriffe muss man heutzutage kein Fachmann sein, urteilte der Präsident des deutschen Bundeskriminalamtes Holger München 2015. Illegale Ware könnte in ›Black Markets‹ erworben werden. Dort würden Dienstleistungen und Software zur Begehung von Straftaten angeboten. ›Crime as a Service‹ – das sei das Geschäftsmodell des sogenannten ›Darknet‹. So nennen Fachleute den verdeckten Teil des Netzes, in dem sich eine dunkle Nachfrage mit einer dunklen Angebotsseite träfen und die praktisch für staatliche oder polizeiliche Stellen zu über 70 Prozent nicht mehr kontrollieren seien (Bartlett, 2015; Balser/Braun 2015). Wie leicht es ist sich über das Darknet mit Waffen zu versorgen hat der Anschlag eines rechtsextremen Täters auf das Münchner Einkaufszentrum am Olympiapark 2016 gezeigt. Die Tatwaffe, eine deutsche Handfeuerwaffe der Bauart Glock, war dort relativ unproblematisch zu besorgen.

26 | Vgl. New York Times unter www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0, aufgerufen am 25. Juni 2014.

27 | Vgl. »Konflikt um Hackerangriff eskaliert«, in Süddeutsche Zeitung vom 22. Dezember 2014.

28 | Vgl. etwa »Halbherziger Kampf gegen Cyberattacken«, in: Süddeutsche Zeitung oder »IT-Sicherheit nicht auf leichte Schulter nehmen«, in: Le Figaro, beide vom 10. April 2015.

Steigende Cyberkriminalität

Hinzu kommt die Cyberkriminalität. Netzwerkspezialist Arne Schönbohm unterscheidet hier Cyberangriffe nach ihren a) politischen und b) materiellen Motiven: »Der größte Teil der Cyberangriffe, die heute weltweit durchgeführt werden, hat [...] keine politischen, sondern materielle Hintergründe, wie Diebstahl, um sich selbst zu bereichern oder zu verwirklichen« (Schönbohm, 2013). Diese erstreckt sich auf viele Bereiche des alltäglichen Lebens: Betrug, Kannibalismus, Prostitution, Kinderpornographie und Menschenhandel. Die hauptsächlichen Motive für einen Angriff bestehen aus Motiven der finanziellen Bereicherung, zum Beispiel durch den Diebstahl und Missbrauch von Kreditkarteninformationen. Hier ist eine Armada von Betrügern global mit ausgeklügelten Computerprogrammen und psychologischen ›Anmachertricks‹ unterwegs.[29] 2015 haben auch die betrügerischen Umtriebe über das Telefon zugenommen. So geben sich Cyberkriminelle als Rechtsanwälte, Bankangestellte oder Techniker aus, um mit perfiden Tricks vertrauensseligen Bürgern per Telefon sensible Daten wie PINs und TANs zu entlocken oder sie direkt zu einer Zahlung zu veranlassen.[30]

Das Unternehmen Symantec zeigt auf, dass Deutschland in Europa den Spitzenplatz mit Blick auf die Intensität von Angriffen einnimmt. Die ›Millenials‹, also die nach 1980 geborenen Personen im Land, sind besonders technologieaffin und mögen den alltäglichen Gebrauch von Smartphones, Tablets und Laptops. Und sie lieben die Möglichkeiten und Verlockungen des Internet. Man nennt sie auch die ›Digital Natives‹, also digitale Eingeborene. Fast 90 Prozent dieser Kohorte haben bereits mit Internetbetrug zu tun gehabt oder zu tun. In Deutschland gibt es täglich über 40.000 Erwachsene in dieser Gruppe, die einem Cyberangriff ausgesetzt sind. Arne Schönbohm zitiert den Sicherheitsexperten Adam Palmer, der darauf hinweist, dass in einem Jahr drei Mal mehr Menschen Opfer von Internetbetrug geworden sind als von physischen Verbrechen. Der Trend geht dabei dahin, Angriffe vermehrt auf Smartphones, und Tablet-PCs zu verüben. Die Schäden betrugen dabei mit Blick auf 2010 in Deutschland etwa 24 Milliarden Euro. Dabei beliefen sich die direkten finanziellen Schäden durch den Diebstahl von Geld oder für Kosten für die Unter-

29 | Etwa durch, »spyware« (Spionageprgramme), »malware« (Programme, die spezielle Computer oder Netzwerke durch Viren, oder Trojaner angreift), »password fishing« oder »Pishing« (das Ergattern von Passwörtern von Internetnutzern), »Pharming« (Umleitung zu einer anderen Website als der gewünschten), »Zählpixel« (um zu überprüfen, wer welche websites oder emails aufruft), SQL-injections (Kontrolle über Server), »Carding« (klassischer Kreditkartenbetrug).

30 | Vgl. https://bankenverband.de/newsroom/presse-infos/bei-anruf-betrug-so-schutzen-sie-sich/, aufgerufen am 31. März 2015.

suchung von Cyberangriffen auf 16,4 Milliarden Euro. 76 Prozent der erwachsenen Internetnutzer werden im Laufe ihres Lebens Opfer von Internetbetrug (Schönbohm 2013).

Dieses Bild wurde Ende 2014 durch das aktuelle Lagebild des deutschen Bundeskriminalamtes (BKA) bestätigt. Der Chef der Behörde, Jörg Zierke, warnte Unternehmen und Privatpersonen vor einem allzu laschen Umgang mit dem Internet, dem Austausch privater Daten oder dem Online – Banking. Er wies darauf hin, dass die Internetkriminalität weiter auf dem Vormarsch sei. Das gelte nicht nur für das ›Pishing‹, das stark zugenommen habe. Dabei erschleichen sich Kriminelle die Zugangsdaten zum Online – Banking und räumen anschließend die Konten ihrer Opfer über das Internet leer. Über 4.000 Fälle wurden 2013 vom BKA registriert. Das war gegenüber dem Vorjahr eine Zunahme um 19 Prozent.[31] Dabei werden die Methoden der Betrüger immer raffinierter und die Abwehr der Angriffe immer komplexer. Und die Kriminalität ist global. Schätzungen zufolge verdient die organisierte Kriminalität mehr Geld durch das Internet als durch Prostitution. Schönbohm identifiziert dabei drei kriminelle Vereinigungen, die auch und gerade mit Blick auf Deutschland besonders aktiv sind und aus Kolumbien, Rumänien und Estland aus – also international – operieren.

Das Internet lädt auch zu Mobbing, persönliche Verunglimpfung oder Pädophilie in geradezu beängstigender Weise ein

Hinzu kommen personale Delikte wie Mobbing, Verunglimpfung und Beleidigungen von einzelnen Personen, Hasskriminalität oder Kinderpornographie. In einem verstörenden Bericht der Frankfurter Allgemeinen Sonntagszeitung vom 15. Dezember 2013 wurden Triebfedern und Wurzeln der europäischen Pädophilen unter dem Titel »Das Netz« dargestellt.[32] Dort wurde deutlich, wie sehr das Thema Erwachsenen- und Kindersexualität eine komplexe Erscheinung in der europäischen Gesellschaft war und ist. Es verwundert deshalb nicht, dass das Internet zu einer idealen Plattform dafür geworden ist, die seit den 1970er Jahren besonders über Frankreich, Dänemark und die Niederlande über ihre Protagonisten sogar eine gesellschaftliche Akzeptanz für dieses Thema suchten. Heute ist dies ein schwieriges Thema für die Staatsanwaltschaften Europas, um diesen Sumpf des Netzes auszutrocknen. Alle Fahndungsergebnisse haben gezeigt, dass insbesondere das Thema der Kinderpornographie ein überaus lukratives, total globales Feld der Schwerstkriminalität geworden

31 | Vgl. BKA warnt vor Internet – Betrug, in: Süddeutsche Zeitung vom 28. August 2014.

32 | Vgl. »Das Netz«, in: Frankfurter Allgemeine Sonntagszeitung vom 15 Dezember 2013.

ist. Die Justiz hat mit internationalen Operationen bislang große Netzwerke der Kinderpornographie ermittelt und ausgehoben.

Spektakuläre Aktionen waren zum Beispiel die Operationen ›Landslide‹ Ende der 1990er Jahre, die Operation ›Himmel‹ Ende 2007 oder die Operation ›Susi‹ Anfang 2009.[33] Die »Operation ›Landslide‹ wurde 1999 in den Medien als »der größte Schlag gegen die kommerzielle Kinderpornografie aller Zeiten« bezeichnet. Die Firma Landslide Inc. soll laut Medienberichten im Zusammenhang mit 5.000 kinderpornographischen Websites und 250.000 Konsumenten gestanden und 1,4 Millionen Dollar monatlich mit Kinderpornografie verdient haben. Thomas Reedy, der Besitzer, wurde zu 35 Jahren und seine Frau zu 15 Jahren Haft verurteilt. Landslide war ein Dienstleistungsunternehmen, das für Anbieter herkömmlicher Pornographie Kreditzahlungen durchführte. Zwei der Webseiten-Betreiber, für die Reedy aktiv war, boten auf ihren Seiten kinderpornographische Darstellungen an. 1997 und 1998 wurde mit diesen Webseiten ein Umsatz im Bereich von Millionen Dollar erzielt. Im Zuge der Operation wurde eine Datenbank mit 250.000 Personen gefunden. Das FBI veröffentlichte in Folge auf der beschlagnahmten Webpräsenz von Landslide Angebote, die den Eindruck von Kinderpornografie erwecken sollten. Im Zuge dieser »Sting-Operation« kam es zu zahlreichen Ermittlungen gegen Interessenten dieses Angebots, darunter viele in Österreich, Deutschland und Großbritannien mit etwa 7.000 Fällen.[34]

Dunkelziffer der Cyber-Kriminalität ist sehr hoch

Leider ist davon auszugehen, dass die Dunkelziffer der kriminellen Delikte trotz dieser großartigen Fahndungserfolge weitaus größer ist als bekannt. Auch das BKA ging 2014 davon aus, dass nur 25 Prozent der Delikte aufgeklärt werden und dass eine gigantische Dunkelziffer von nicht gemeldeten Fällen bestehe. Letzteres sei vor allem darauf zurückzuführen, dass die Cyber – Sabotage dramatisch zunehme, also die Angriffe auf Unternehmen, um deren Rechner lahmzulegen und anschließend die Funktionsfähigkeit der Firmennetze im Rahmen einer Lösegeldzahlung wieder herzustellen. Viele Firmen scheuten sich solche Erpressungen zu melden, damit das Firmenimage nicht leide. Für viele Konzerne ist dies ohnehin keine Option. Endlos ist die Reihe der Meldungen über Großangriffe auf Banken und global agierende Unternehmen, die Anfang der 1980er Jahre ihren heute rührig erscheinenden Anfang mit den spinnerten Hackerangriffen von Typen wie Julien Assange genommen hatten. Heute sind dies Großangriffe, die die Weltwirtschaft erschüttern und

33 | Vgl. http://de.wikipedia.org/wiki/Kinderpornografie, aufgerufen am 30. Dezember 2013.

34 | Vgl. ebd.

das Vertrauen in die digitale Gesellschaft zerstören. So etwa eine großangelegte Attacke auf die amerikanische Bank JPMorgan und andere Geldhäuser Mitte August 2014, bei der in großem Stile mutmaßlich aus Russland große Mengen an Kontodaten gestohlen worden sind.[35] Insofern sind heute andere Gegenmaßnahmen nötig als früher. Bemerkenswert dabei ist der in Deutschland von Arne Schönbohm gegründete und bis Anfang 2016 als Präsident geführte Cyber-Sicherheitsrat e.V., der namhafte wirtschaftliche, politische und zivilgesellschaftliche Akteure der Netzwerkgesellschaft bei elektronischen Sicherheitsfragen professionell berät und unterstützt.[36]

Schwächung der Demokratie umstritten

Das Internet wird auch zur Herausforderung für die repräsentative Demokratie. Es ermöglicht einerseits eine stärkere direkte Beteiligung der Bürger an politischen Entscheidungsprozessen. Das Netz räumte in den vergangenen 15 Jahren mit Hierarchien auf, mit Grenzen und Barrieren. Seine Rolle als Labor für Experimente, die in der Regel auf eine Demokratisierung der Verhältnisse hinausliefen, bestreitet niemand. Das Ideal vom ultimativen und selbst organisierten Freiraum wurde zur leitenden Utopie. Es führte dazu, dass sich insbesondere die jungen ›Netizens‹ der Gegenwart anderen politischen Artikulations- und direkten Organisationsformen begeistert zuwendeten. Grundidee und Effekt dabei sind, dass sich politische Entscheidungen zwischen direkten und repräsentativen Entscheidungsformen bewegen und nicht auf die permanente Anwesenheit der Mandatsträger des Politischen angewiesen sind. Dies führt andererseits zu einer Verflüssigung demokratischer Entscheidungsprozesse (Liquid Democracy) und bedeutet gleichzeitig eine Entmachtung der repräsentativen Demokratie. Das Konzept entwickelte besonders bei jungen Menschen ›Appeal‹. Es hat sich aber als wenig praktikabel erwiesen. Dies zeigt das Beispiel der deutschen Piratenpartei. Sie wollte den innerparteilichen Willensbildungsprozess ›verflüssigen‹, was jedoch zu chaotischen Entscheidungsprozessen meist ohne Ergebnis führte, so dass die Partei einzig als bewegliche und launige »Stimmungswolke« erschien (Weidenfeld, in: Schönbohm [Hg.]: 2013), die 2015/2016 völlig an Bedeutung verlor.

Gleichzeitig hat die Snowden-Affaire gezeigt, dass der gewonnen Freiraum bis in kleinste Nischen hinein von Geheimdiensten, Kriminellen oder Unternehmen kontrolliert werden kann – und wird. Dass das Netz genauso ein Inst-

35 | Vgl. Bankenverband (Hg.), Bankenbrief vom 28. August 2014; vgl. auch Bloomberg »FBI Examining Whether Russia is Tied to JPMorgan Hacking«, unter www.bloomberg.com/news/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.html, aufgerufen am 28. August 2014.

36 | Vgl. http://cybersicherheitsrat.de/, aufgerufen am 23. März 2015.

rument des Überwachungsstaates sein kann wie ein Werkzeug der Befreiung, hat man in autokratischen Ländern wie China, Russland sehen können. Dabei sind nicht nur die USA und ihr Inlandsgeheimdienst NSA die alleinigen Übeltäter. Die Snowden-Affaire hat gezeigt, dass sie Teil einer Fünf-Augen-Front sind, zu der Großbritannien, Kanada, Australien und Neuseeland gehören. Sie wurde ergänzt von der Gruppe der Neun Augen bzw. der 14 Augen in den NATO-Staaten. Das alles stellt nach dem Journalisten Andrian Kreye von der Süddeutschen Zeitung die Frage, wer Grundrechte wie die Privatsphäre, das Briefgeheimnis oder die Würde des Einzelnen überhaupt noch garantieren kann – ein Staat, der seinen Bürgern prinzipiell misstraut, scheint dafür nicht mehr geeignet zu sein (Kreye 2013). Insofern stehen die Demokratisierungsgewinne den Demokratiegefährdungen diametral gegenüber und dies zeigt, dass die Demokratisierung des Internet je nach Perspektive der Betrachtung höchst umstritten ist.

Problem Datenschutz nimmt exorbitante Ausmaße an

Ein wichtiges Problem der Informations- und Kommunikationstechnologien (IKT) bleibt der Datenschutz. Hier wirft das Internet Probleme auf. Datenschutz beinhaltet – nüchtern definiert – die Kontrolle über die Art und Menge an Informationen, die über einen Menschen im Internet verfügbar ist oder freigegeben wird, und wer Zugang zu solchen Informationen hat. Datenschutz des Internet wird als Unterkategorie des Computer-Datenschutzes geführt.[37] Es geht also um den Zugriff auf gespeicherte Daten im geschäftlichen, öffentlichen oder privaten Bereich und die Überwachung der Kommunikation der Netzwerkteilnehmer, weltweit. Die NSA-Affäre 2013/2014 hat gezeigt, inwieweit eine solche Totalerfassung möglich ist und systematisch im Kontext der Rasterung von Datenströmen angewandt wurde. Drastisch definiert der amerikanische Sicherheitsexperte Bruce Schneier die Bedeutung des Datenschutzes in seinem Blog deshalb so: »Datenschutz schützt uns vor Missbrauch durch Mächtige, sogar, wenn wir nichts falsch machen, während wir überwacht werden«[38]. Dabei sind Millionen von Menschen von Datenschutzverletzungen im privatwirtschaftlichen Bereich bedroht. Unternehmen und Agenten von Firmen suchen danach, welche Informationen von einem Internetnutzer wie, wann und warum genutzt werden. Sie versuchen, diese Informationen durch Quizze oder Bonus-Angebote oder Rabattversprechungen zu erschleichen und dann Werbung auf den besuchten Seiten zu lancieren.

---

37 | Vgl. http://de.wikipedia.org/wiki/Datenschutz_im_Internet, aufgerufen am 11. August 2016.

38 | https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html, aufgerufen am 11. August 2016.

Auch die sozialen Medien sind datenschutzrechtlich problematisch

Facebook geriet im Juni 2014 ins Visier der britischen Datenschutzbehörden. Dem sozialen Netzwerk wurde vorgeworfen, 2012 in einem Experiment gegen geltende datenschutzrechtliche Bestimmungen verstoßen zu haben. Facebook wollte prüfen, wie sich Emotionen auf sozialen Netzwerken verbreiten. Das Unternehmen untersuchte dazu 689.000 seiner Nutzer. Dazu wurde die Hauptseite manipuliert. Für eine Gruppe wurden negative Inhalte ausgeblendet, für eine andere positive. Was genau negativ und positiv ist, wurde mit einer Analyse-Software entschieden. Schrieb ein Nutzer zum Beispiel das Wort »sad« (traurig), wurde das als negativ bewertet. Das Ergebnis der Studie war: wer mehr Negatives zu sehen und zu lesen bekommt, postet selbst auch mehr Negatives. Umgekehrt gilt das auch für positive Inhalte. Das Experiment fand statt ohne Wissen und Zustimmung der Nutzer, was unter wissenschaftlich-ethischen Kriterien unstatthaft ist. Auch wenn eine wissenschaftliche Nutzung der Daten in den allgemeinen Geschäftsbedingen (AGB) enthalten sei, so dass Unternehmen, wolle man dies in Zukunft nicht wiederholen. Problematisch dabei war, dass dieser Abschnitt offenbar erst nach dem Versuch in die AGB hinzugefügt worden ist.[39]

Das Experiment hat aber weiter gehendes gezeigt: es entstand die Angst vor einem Konzern, dem man sich ausgeliefert fühlen kann, weil er durch die Installation von Filterblasen das eigene Sozialleben im Netz manipulieren könnte. Der die Welt der einen aufhellt, die der anderen aber verdüstert. Gleichwohl das Experiment diesen Effekt nur minimal bewies, öffnete es die Phantasie für größere Aktionen. Gezielte Impulse auf weit mehr Menschen angewendet, könnten vielleicht stärkere Wirkungen erzeugen. Am Tag der amerikanischen Kongresswahlen von 2010 sahen 60 Millionen Nutzer in den USA ein Banner mit dem Aufruf, zur Wahl zu zugehen. Es gab Hinweise über ›Freunde‹, die ihre Wahlbereitschaft dezidiert bekundeten. Eine Begleitstudie von Facebook dazu ergab: die simple Aktion hatte 340.000 zusätzliche Wähler mobilisiert. Noch geht es um Positives oder Erstaunliches. Seit Mai kann man sich bei Facebook in den USA als Organspender zu erkennen geben – inklusive Nachricht an die ›Freunde‹. Die Ansteckung gelang. Am ersten Tag registrierten sich online mehr als 13.000 neue Spender. Der Durchschnitt liegt bei 616.[40] Der bittere Nachgeschmack dennoch bleibt. So haben die Studien die enorme Wirkungsmacht von gezielten Informationskampagnen demonstriert, die aber auch zu anderen politischen Zwecken genutzt werden könnten. Gravierender noch sind die Installation von Spyware (also Programme, die gespeicherte Daten und laufende Interaktionen eines Webnutzers ausspionieren) oder soge-

39 | Vgl. »Ermittlungen gegen Facebook«, in: Süddeutsche Zeitung vom 3. Juli 2014.

40 | Vgl. »Hexenmeister am Regler«, in: Der Spiegel Nr. 28 vom 7. Juli 2014.

nannte Exploits (Programme, die die Funktion von installierten Programmen insbesondere auf Personal- und Geschäftscomputern stören). In beiden Fällen können erhebliche Schäden für die davon betroffenen Personen oder Unternehmen entstehen.

Datenschutz ist im Finanz- und Gesundheitsbereich besonders sensibel

Ein besonders schwieriges datenschutzrechtliches Problem sind sensibelste Datenströme und Datenreservoirs im Finanz- oder Gesundheitsbereich. Der Bereich der Gesundheitstelematik – also die Verbindung moderner IKT mit medizinischen Behandlungsformen und der Verwaltung von Patientendaten im elektronischen Netz – thematisiert dies für Deutschland in herausragender Weise. Hier geht es um eine emotionalisierte, aber auch um eine sachlich komplizierte Verbindung von Versorgungsmanagement und Datenschutz.

Speziell bezieht diese Problematik die elektronische Versichertenkarte ein, welche alle medizinischen Daten eines Menschen enthält oder in Zukunft enthalten soll, oder etwa Behandlungsformen, die via Internet Patienten bei schweren oder chronischen Krankheiten versorgen. Dies gilt für telemedizinische Behandlungen von Menschen nach Herzinfarkt, bei Herzinsuffizienz oder bei Bluthochdruck. Beides ist kritisch, da intimste Daten in die Öffentlichkeit oder, noch kritischer, in die Hand von Unternehmen geraten und kommerziell ausgeschlachtet werden könnten. In jüngster Zeit wurde auch hier das Big – Data – Problem virulent. Also die Erfassung, Speicherung, Verteilung statistischer Analyse und Visualisierung von großen Datenmengen, was in der Gesundheitswirtschaft von höchster Relevanz ist. Hierbei geht es nach dem Vorsitzenden des Bundesverbandes Medizininformatik (BVMI) für die Region Berlin Brandenburg und Vorstand des Arbeitskreises ›E-Health‹ der BITKOM, Peter Langkafel, um mehr als technische Machbarkeiten. Es geht um die »Automatisierung des medizinischen Alltags« und seine Implikationen für den menschlichen Aspekt der medizinischen Versorgung. (Langkafel 2014).

Hierbei ist auch die Vernetzung der Patienten von einer zunehmenden Bedeutung. Die zunehmende Digitalisierung im Gesundheitswesen berührt nicht nur die traditionelle Schulmedizin oder das Gesundheitssystem an sich; eine wachsende Zahl von digitalen Anwendungen und Onlinediensten und personalisierten Applikationen lässt Patienten auch ihre eigene Gesundheit überwachen und so anders handhaben.

Datenschutz und Vertraulichkeit sind insbesondere im medizinischen Betrieb von herausragender Bedeutung

Das vertrauliche Arzt-Patienten-Verhältnis sowie die ärztliche Schweigepflicht kämen nach der Auffassung von Kritikern in Gefahr. Dabei gibt es Möglichkei-

ten, wie die Vorteile der Telemedizin unter Beachtung datenschutzrechtlicher Voraussetzungen erzielt werden könnten. Die Daten sollten hierbei strikt nur vom Versicherten und dem behandelnden Mediziner eingesehen werden können. Zudem solle der Patient im Rahmen des informationellen Selbstbestimmungsrecht die Autorität über den Gebrauch seiner Daten haben und allein entscheiden sowie immer kontrollieren können, wer Einsicht in seine Daten erhält. Die Diskussion macht deutlich, dass besonders der gravierende Mangel an Kommunikation, Information und Transparenz effiziente Innovationen bei der gesamten Implementierung von IKT-Lösungen im Gesundheitswesen erforderten. Die wachsende Menge an medizinischen Daten bedarf papierloser und elektronisch gestützter Verarbeitungsverfahren. Die elektronische Gesundheitskarte ist hierbei der ›Wasserhahn‹, durch den die Daten elektronisch transportiert werden und der im Behandlungsfall systematisch und organisiert angezapft werden muss. Die Gesundheitstelematik greift in ein tradiertes System der Gesundheitsfürsorge ein; es ist deshalb nicht verwunderlich, dass technische Innovationen einerseits faszinieren, andererseits aber auch auf Bedenken und Besitzstände stoßen.

Dennoch können Widerstände die Einführung von telematischen Systemen und einer entsprechenden Infrastruktur nicht verhindern, schließlich ist die elektronische Weitergabe von Daten im derzeitigen herkömmlichen System mittels E-Mail, Telefon oder Fax auch erlaubt und allgemeine Praxis. Die Möglichkeiten der Vernetzung und Interoperabilität der eingesetzten elektronischen Systeme sind derzeit noch höchst unvollkommen. Es braucht deshalb Versorgungssysteme, die nicht nur datenschutzrechtliche Hürden, sondern auch gravierende technische Inkompatibilitäten ausräumen können sollten. Dennoch führt an der Gesundheitstelematik kein Weg vorbei. eHealth ist das System, dass es ermöglicht, den demographischen Wandel besser zu beherrschen. Das Gesundheitssystem wird in Zukunft mit immer älteren und multimorbiden Menschen zu tun haben, wobei die finanziellen Mittel beschränkt bleiben, sofern die Menschen nicht zu größeren individuellen Eigenleistungen bereit sein werden. Die Telemedizin kann und wird entscheidend helfen, die Versorgung von Menschen im demographischen Wandel zu verbessern und das Gesundheitssystem bezahlbar zu halten. Insofern führt an eHealth kein Weg vorbei, was mittlerweile der Benchmark mit den Ländern Skandinaviens oder Israel sowie fast unzählige positive Pilotprojekte und Fallstudien in Deutschland klar zeigen.

Der Kampf um den Datenschutz ist eine der wichtigsten Schlachten des 21. Jahrhunderts

Daten sind nach dem grünen Europaabgeordneten Jan Philipp Albrecht das Gold des 21. Jahrhunderts, der Kampf um den Datenschutz die wichtigste

Schlacht um unsere Freiheit (Albrecht 2014). Spätestens seit den NSA-Enthüllungen Edward Snowdens ist klar, wie gläsern die Menschen in der Informationsgesellschaft geworden sind. Von den Nutzern relativ unbemerkt werden intimste Daten und privateste Informationen ermittelt und von der Wirtschaft ausgebeutet. Ein gigantisches System einfacher Logarithmen dient dazu, über simple Konnotation innerhalb der elektronischen Kommunikation diejenigen Zusammenhänge herauszufiltern, die gerade für eine Behörde oder ein Unternehmen von Interesse sind. Wer denkt, dass er nur auf Facebook oder andere soziale Medien verzichten muss, um sicher zu sein, täuscht sich. In einem Selbstversuch zeigten zwei Reporter des Ersten Deutschen Fernsehens 2014 auf was passiert, wenn man zum Ofer von Datenspionage wird. Dabei ließ sich einer der Reporter darauf ein, dass man ihn mithilfe von versierten IT-Experten ausspähte. Nach kurzer Zeit waren seine Vorlieben, sein Tagesablauf, Privatkontakte und sein Kontostand glasklar bekannt. Das IT-Team stahl im zunächst seine Daten, dann seine Identität. Er war plötzlich wie ausgelöscht. Die Reportage hat gezeigt wie die Opfer nach anfänglicher Gelassenheit ängstlich werden und schließlich bis ins Mark verunsichert sind. Der Film zeigt eindrucksvoll auf, dass und wie es jeden treffen kann.[41]

Mit Blick auf die Regulierung des Datenschutzes offenbart der nationale, europäische und internationale Vergleich erhebliche Unterschiede im Rechtsverständnis und den technologischen Grundlagen

Damit werden besonders die datenschutzrechtlichen Grundlagen von Big Data problematisiert. Das Grundrecht auf Datenschutz wurde 2009 in die Europäische Grundrechtscharta mit Artikel acht aufgenommen. Sie verstärkte damit das Datenschutzgrundrecht für alle EU-Mitgliedstaaten, die bereits 1995 mit einer Richtlinie auf europäischer Ebene als verbindlich formuliert worden ist. Die Richtlinie wurde allerdings nicht – was dem Charakter einer Richtlinie gegenüber einer Verordnung in der EU entspricht – in jedem Staat gleichermaßen umgesetzt. Mit Blick auf die Entwicklungsgeschwindigkeit webbasierter Technologien und die Umsetzungsgeschwindigkeit von europäischem und nationalem Recht wurde diese Vorgabe allerdings schnell zur Makulatur und dementsprechend im Januar 2012 durch einen Vorschlag für eine EU-Datenschutz-Grundverordnung ersetzt.

Im Kern geht es darum, den Geltungsbereich der Grundversorgung nicht daran zu knüpfen, wo geographisch gesehen die verantwortliche Stelle für die Verarbeitung von Informationen stattfindet, sondern sich darauf zu konzentrieren, ob davon personenbezogene Daten von EU-Bürgern betroffen sind. Das ›Marktortprinzip‹ soll dafür sorgen, dass sich die datenspeichernden US-

41 | »Zugriff – wenn das Netz zum Gegner wird«, in: ARD vom 7. Juli 2014.

Unternehmen und Ökosysteme nicht mehr darauf zurückziehen können, das europäische Recht binde sie nicht. Das Ergebnis ist ein Konflikt zwischen der EU und den USA, die ein völlig anderes datenschutzrechtliches Verständnis haben und die strukturellen und regelungstechnischen Fehler und Defizite im deutschen, europäischen und internationalen Datenschutzrecht offenlegen. Esgeht also darum, eine echte Anonymisierung der Datensätze zu erreichen, bei der Anwendung und Analyse von Datensätzen Maßnahmen zur Transparenz zu entwickeln und internationale Algorithmen-Abkommen zur Standardisierung und Zertifizierung einzuführen. Da sich die Ausmaße von Big Data erst noch entwickeln, ist es schwierig, den Komplex juristisch abzudecken. Das Potenzial der webbasierten Technologien und das Vertrauen in sie kann sich allerdings nur dann entwickeln, wenn die Privatsphäre unangetastet bleibt und die Grundrechte gewahrt werden (Dapp/Heine 2014: 22f.).

Access: die digitale Lücke schließt sich

Der globale Zugang für jedermann zu allen öffentlichen Informationen war und ist eines der zentralen Anliegen des Internet. ›Open Access‹ ist hierbei das Label, mit dem etwa die globale Informationsplattform Wikipedia kostenfrei und nur auf Spenden (und nicht auf Werbung) beruhend mit einem unsichtbaren Heer von kostenlos arbeitenden Fachleuten versucht, für alle Menschen eine globale Enzyklopädie des Wissens bereitzustellen. Wikipedia ist heute einer der bemerkenswertesten Pfeiler einer wissensbasierten Konzeption des Internet, dessen Bedeutung nicht hoch genug eingeschätzt werden kann. Access bezeichnete einerseits den freien Zugang zu allen wissenschaftlichen Informationen und anderen Materialien. Unter dem Druck der steigenden Preise für wissenschaftliche Publikationen bei gleichzeitig stagnierenden oder schrumpfenden Etats in den Bibliotheken während der Zeitschriftenkrise bildete sich seit Beginn der 1990er Jahre eine internationale Open-Access-Bewegung. Die zentrale Forderung dieser Bewegung war, dass wissenschaftliche Publikationen als Ergebnisse der von der Öffentlichkeit geförderten Forschung dieser Öffentlichkeit wiederum kostenfrei zur Verfügung gestellt werden müssen. Die bisherigen Publikationsstrukturen stellten eine Privatisierung des von der Allgemeinheit finanzierten Wissens dar. Durch Open Access sollte verhindert werden, dass dieses Wissen, erneut von der Allgemeinheit finanziert, von den Verlagen zurückgekauft werden muss, die durch die Publikation die Nutzungsrechte erhalten haben. Die Open-Access-Bewegung verfolgt auch das Ziel, die digitale Kluft zu verringern. Unter anderem sollen so Wissenschaftler mit geringem Budget an wissenschaftliche Ergebnisse gelangen und am akademischen Diskurs teilnehmen können.[42]

42 | Vgl. http://de.wikipedia.org/wiki/Open_Access, aufgerufen am 24. April 2014.

Mit Blick auf die ›Digitale Kluft‹ oder ›Digitale Lücke‹ war ›Open Access‹ eine bemerkenswerte globale Initiative. Der Begriff der digitalen Kluft wird auf die Unterschiede zwischen Bevölkerungsgruppen in einer Gesellschaft sowie in Bezug auf die Ungleichheit zwischen Industrieländern und Entwicklungsländern angewandt. Open Access hat den technischen Zugang zum Internet für jedermann in der sich entwickelnden und unterentwickelten Welt nicht lösen können. Die Informationstechnologie hatte das Potenzial dazu beizutragen, Ungleichheiten zu minimieren und sozio-ökonomische Entwicklung zu forcieren. Von Anfang an war aber klar, dass dies für eine allumfassende Globalisierung wünschenswert ist, dass aber nicht alle Menschen sofort oder komfortabel mit einbezogen werden konnten.

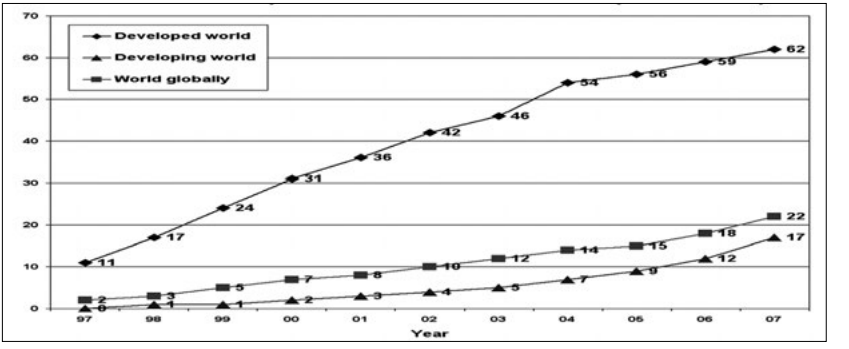
Das Problem der digitalen Ausgrenzung entstand. Es aktualisierte die These einer Wissenskluft, insbesondere zwischen Nord und Süd, allerdings auch innerhalb entwickelter Gesellschaften der westlichen Welt, hier sogar auch in Europa. Es gibt prinzipiell eine »Breitbandkluft, eine »Bildungskluft«, eine »Einkommenskluft« und eine »Alterskluft«. Die »Breitbandkluft« thematisiert die regional ungleiche Verfügbarkeit von Breitband-Internetzugängen und die Möglichkeit von Flatrate-Zugängen, worauf der Einzelne zunächst keinen Einfluss hat; die »Einkommenskluft« bezieht sich auf das verfügbare Haushaltseinkommen und die Möglichkeit, Zugangsabonnements zu buchen; die »Bildungskluft« bedeutet ein Unverständnis hinsichtlich der Nutzung von neuen Informations- und Kommunikationstechnologien aufgrund von Verständnisschwierigkeiten hinsichtlich der Funktionsweise neuer Technologien; die »Alterskluft« schließlich ist ein Akzeptanzproblem, weil ältere Menschen aus verschiedenen Gründen die Einrichtung und Anwendung moderner IKT ablehnen, ob aus Verständnisschwierigkeiten, Anpassungsverweigerung, Kostengründen oder der Furcht vor Internetkriminalität.

Die Internetnutzung hat auch in den Entwicklungsländern ein bemerkenswertes Niveau erreicht

Inwieweit sich die digitale Lücke mit Blick auf die dritte Welt schließt, ist noch nicht gänzlich klar. Um dies beurteilen zu können, müssten mehr valide Daten aus den betroffenen Ländern vorliegen. Allerdings weisen Indizien darauf hin, dass die Nutzung des Internet in den letzten 20 Jahren selbst in den Entwicklungsländern zum Teil stark zugenommen hat. Andere Zahlen zeigen, dass die Nutzung der mobilen Telefonie und die kommerzielle Nutzung des Internet über Online-Geschäfte zum Beispiel in Afrika gewachsen ist. Es gibt ohnehin viele Anzeichen dafür, dass Modernisierungserfolge auf dem schwarzen Kontinent in der westlichen Welt nicht bzw. viel zu spät erkannt und in jeder Hinsicht nicht aufgegriffen werden.

Interessant ist, dass seit der Debatte über dieses Thema ab Mitte/Ende der 2000er Jahre kaum noch aktuelles Material oder Daten zu diesem Thema zu finden sind. Es scheint so, als ob die Normalität der elektronischen Kommunikation in den Entwicklungsländern angekommen ist und das Thema an massenmedialer Relevanz verloren hat. Dies zeigt die boolesche Algebra bzw. Suchlogik des Internet auf. Die Google-Suche »Digitale Kluft + OECD« weist im Internet rund 16.900 Ergebnisse auf, die im wesentlichen nicht über das Jahr 2007 hinausgehen. Ein ähnliches Ergebnis ergibt sich bei der Suche »Digitale Kluft + UNO«, die mit ungefähr 11.200 Ergebnissen auch in der Mitte der 2000er Jahre verharrt. Auch die Mitte 2013 aktualisierte Website von Wikipedia griff Anfang 2014 lediglich auf Daten von 2007 zurück.[43] Die Weltbank meldete 2005, die digitale Kluft schrumpfe. Während nach wie vor weniger als vier Prozent der Menschen in Afrika mit Computern online sind, boomt der Bereich des Mobilfunks dort, der über moderne Smartphones auch den Zugang zum Internet erlaubt. Mit Blick auf diesen speziellen Zugang spielt die Zukunftsmusik laut. Das immer schnellere Internet dringt in immer entlegenere Winkel der Welt vor – auch per Mobilfunk, demnächst mit Ballonen, Drohnen oder Satelliten, die um die Erde kreisen, damit auch in diesem Kontext die zukünftige Bedeutung des Weltraums akzentuieren und ein SkyFi schaffen werden, gewissermaßen ein Internet am Himmel (Beise/Schäfer 2015d).

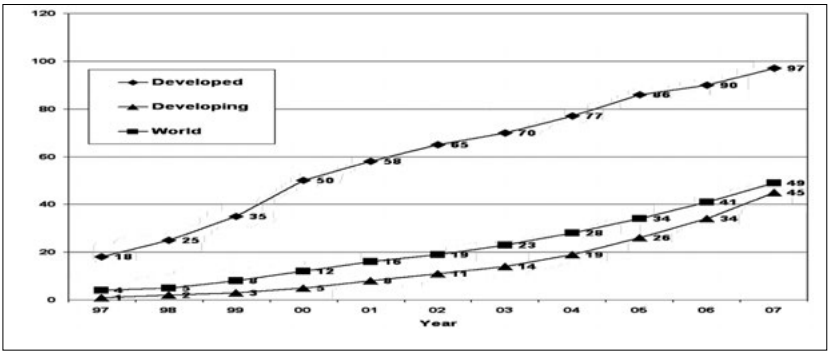
Abbildung 6: Internet users per 100 inhabitants 1997-2007 (Source: ITU)



Internetnutzer pro 100 Einwohner 1997-2007; Quelle: Internationale Fernmeldeunion

43 | Vgl. www.google.de/imgres?sa=X&biw=1251&bih=1289&tbm=isch&tbnid=AXp2tnwVGBYSzM:&imgrefurl=http://de.wikipedia.org/wiki/Digitale_Kluft&docid=Ks1r15DcL37_uM&imgurl=http://upload.wikimedia.org/wikipedia/commons/1/19/Mobile_phone_subscribers_per_100_inhabitants_1997-2007_ITU.png&w=911&h=810&ei=i961UvSGGomutAapkYDQBg&zoom=1&iact=rc&dur=1697&page=1&tbnh=148&tbnw=171&start=0&ndsp=50&ved=1t:429,r:0,s:0,i:83&tx=115&ty=112, aufgerufen am 21. März 2014.

Abbildung 7: Mobile phone subscribers per 100 inhabitants 1997-2007



Mobilfunknutzer pro 100 Einwohner 1997-2007; Quelle: wikipedia

Die Daten zeigen dabei auf, dass trotz bescheidener Fortschritte auch die Entwicklungsländer nun zügig an der Globalisierung partizipieren. Innerhab der entwickelten Länder nehmen Partizipationsmöglichkeiten aller Bevölkerungsschichten durch technische Vereinfachungen, sinkende Gerätepreise, wachsendes technisches Verständis, dem unwiderstehlichen stylischen ›Sexappeal‹ der Geräte und Verständnis für die globale Welt der digitalen Vernetzung zu. Die Generation der ›Digital Illiterates‹ (digitale Analphabeten) stirbt aus. Die digitale Lücke, sie schließt sich. Auch Afrika wird nun zunehmend global.

3. Die terrestrischen Strukturen globaler Interaktion

Die dritte Globalisierung bezeichnet ein Zeitalter der allumfassenden Vernetzung, die durch eine permanente Mobilität von Gütern, Dienstleistungen, Arbeit und Informationen gekennzeichnet ist. Es geht um die Sicherheit und Gewähr beim Transport von Menschen, Waren und Know-How. Dies erfordert eine nachhaltige Vernetzung, die, wie im Energiebereich, den Zielen von Versorgungssicherheit, Zuverlässigkeit und Qualität auch bei größten Belastungen wie Terrorismus und Krieg, Naturkatastrophen oder technischen GAU's, gerecht werden muss. Eine nachhaltige Vernetzung ist die unverzichtbare technische Grundlage der Globalisierung, permanente Versorgung und funktionierende Mobilität zu akzeptablen sozio-ökonomischen und ökologischen Bedingungen ihre Basis.

Die Voraussetzung dafür ist Funktionalität und Effizienz. Vernetzung ist ein Begriff der Systemtheorie. Ein System besteht aus einzelnen Teilen, die durch Ursache-Wirkungs-Beziehungen und Systemeigenschaften miteinander verknüpft sind. Dieses Verständnis von Systemen kannte man im 20. Jahrhundert im Rahmen der Kybernetik insbesondere aus dem Verstehen komplexer biologischer, informationstechnologischer, ökologischer oder medizinischer

Ansätze (Wiener 1948; Vester 1983; Bluma 2005). Kybernetik bezeichnet die Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen und wurde mit der Formel »die Kunst des Steuerns« umschrieben. Mit dem Entstehen einer eng verbundenen Weltgesellschaft sind kybernetische Sichtweisen auch auf soziologische, ökonomische und politische Regelzusammenhänge angewandt worden, auch wenn der Begründer der modernen Kybernetik, Norbert Wiener, diesen Zusammenhang stets kritisch gesehen und die Chaosforschung (oder Chaostheorie) das Verhalten von Systemen mit ›deterministisch chaotischer Dynamik‹ als nicht wirklich steuerbar erachtet hat. Ohne Zweifel aber prägt die Vernetzung das Schicksal der weltweiten Entwicklungen.

Im Rahmen dieses wissenschaftsgeschichtlichen Hintergrunds ist der Vernetzungsgrad von technischen, sozio-ökonomischen und politischen Systemen mit Blick auf die Globalisierung exorbitant angestiegen. Dabei wurden in den letzten 50 Jahren insbesondere die negativen Folgen des Ineinandergreifens von komplexen Systemen zunehmend wichtig, was sich zunächst auf Fragen der Ökologie (Gruhl 1978), der Demographie (Neuffer 1982) oder des industriell-militärischen Komplexes bezog (Kahn 1984). Zum Beginn des 21. Jahrhunderts erhöhten sich die Vernetzungsgrade in den jeweiligen Teilsystemen. Die Vernetzung von wirtschaftlichen, politischen und sozialen Subsystemen zu einem hoch komplexen Gesamtsystem wurde total und die Flutung der Welt mit komplexen Problemstellungen nahm kontinuierlich zu. Zu diesem Zeitpunkt wurde klar, dass viele neue Problemstrukturen nicht mehr mit etablierten Problemlösungen in Einklang zu bringen sind. Dabei ist die Logistik eines der herausragenden Werkzeuge der Globalisierung. Logistik ist mehr als Straßen, Schienen, Flüsse, digitale Telefonanschlüsse oder Glasfaserkabeln; sie ist mehr als Transportmittel zu Wasser, zu Lande, in der Luft oder im All; mit Hilfe komplexer Logistikinfrastrukturen planen und optimieren alle gesellschaftlichen Teilsysteme die Menschen-, Waren-, Dienstleistungs- und Informationsströme entlang komplexer Logistikketten weltweit vom Erzeuger bis zum Verbraucher, vom Sender bis zum Empfänger. Zum einen füttern innovative logistische Systeme das System der Globalisierung, zum anderen sind sie ein wesentlicher Teil von Problemen der Gegenwart, aber auch von Problemlösungen der Zukunft.

Logistik und Infrastrukturen sind als Grundlage der Globalisierung essenziell

Insofern bleibt Logistik als Element der Globalisierung essenziell. Die Logistikbranche stellt sich folgerichtig auf die Chancen und Herausforderungen von vernetzten Lebensformen und Verbrauchsgewohnheiten ein. Dabei ist sie einerseits ein Verursacher globaler Problemlagen. Sie zeitigt soziale und ökologische Folgen, etwa im Bereich der Energieversorgung oder der CO_2-Emis-

sionen; andererseits gehört die Logistik zum Herz-Kreislauf-System der Globalisierung und bietet vielfältige Möglichkeiten, solche Kosten zu reduzieren und ›smarte‹ Verkehrsströme der Globalisierung zu etablieren. Hierbei spielen ITK-Technologien eine wichtige Rolle. Es geht darum, Gesamtsysteme zu optimieren, um Kosten zu senken und Belastungen für Gesellschaften mit Blick auf Überlastungen oder Zusammenbrüche in komplexen Bewegungsmechanismen zu minimieren. Staus oder Zusammenbrüche in Liefer- und Versorgungsketten in den Bereichen Energie, Wasser, Transport und Verkehr erfordern erhebliche Anstrengungen in den Bemühungen, Engpässe und Emissionen genauso zu reduzieren wie Zeit- und Kraftstoffverschwendungen. Insofern ist es das Ziel, positive Beiträge zu einer nachhaltigen Vernetzung zu konzipieren und umzusetzen. Die Logistik wurde damit am Anfang zu einem Problem der Globalisierung; heute ist sie ein Teil ihrer Lösung.

Logistik muss sich an die Konsequenzen der Globalisierung anpassen

Im Rahmen eines langfristig angelegten Foresight-Prozesses macht sich das deutsche Unternehmen Deutsche Post AG deshalb zusammen mit dem Kölner Forschungsinstitut ›Z_Punkt. The Foresight Company‹ Gedanken darüber, auf welche zukünftigen Entwicklungen sich die Logistiksysteme und -unternehmen in der Welt eigentlich bis zum Jahr 2050 einstellen müssen (Deutsche Post AG 2012, 2014). Den verantwortlichen Führungskräften des Unternehmens und den Zukunftsforschern wurde klar, welche Entwicklungen eintreffen können und welche Folgen dies haben kann. Insofern kalkulierten sie im Rahmen der letzten Jahre mehrere robuste Entwicklungslinien, die auch in anderen sozio-ökonomischen oder politischen Kontexten reflektiert worden sind (ebd.: 40ff.).

Im Kern betrachteten die Studien die Verstädterung der Welt, die Folgen eines unkontrollierten Wachstums, die Veränderung von Lebensstilen und die Auswirkungen auf Lebensformen und Konsumstile, die technologischen Möglichkeiten der Optimierung logistischer System im ITK-Bereich sowie globale Herausforderungen und globale Widerstandsfähigkeit im Zeichen unumkehrbarer Folgen der Globalisierung. Diese Schwerpunkte sind interessant, weil Planungseinheiten in der Wirtschaft, in der Politik oder der Zivilgesellschaft jeweils aus ihren eigenen spezifischen Interessen heraus ähnlich Entwicklungen bedenken (Shell International BV 2013: 92; Center für European Policy Studies (CEPS) 2013). Hierbei ist der letztgenannte Punkt bemerkenswert, da er eine äußerst wahrscheinliche Entwicklung repräsentiert (Ostovics/Kovar/Mayrbäurl 2012). Demnach stellt man sich darauf ein, dass sozio-ökonomische Folgen der Globalisierung nicht mehr zu ändern sind und es darauf ankommt, mit intelligenten Anpassungsstrategien ihren Folgen gerecht zu werden. Ein herausragendes Beispiel dafür ist der Klimawandel, bei dem der Anstieg der

durchschnittlichen Erderwärmung nicht mehr aufzuhalten ist. Der Gedanken der Nachhaltigkeit wird hier mit dem Prinzip der Resilienz konfrontiert (ebd.). Dies gehört zu den zentralen Herausforderung für die Logistik der Globalisierung.

4. Gravity – Der Weltraum als dritte Dimension

Der Weltraum ist ein strategisches Operationsgebiet. Er gewann in den letzten 50 Jahren eine globale Dimension und eine große politische Bedeutung. Er ist von vitaler Bedeutung für Sektoren wie Sicherheit, Logistik, Wissenschaft, Technologie, Klima oder Umwelt. Wirtschaftlich bedeutsam ist er für den Luftverkehr, die Navigation von Fahrzeugen auf Land, im Wasser und in der Luft, den Tourismus, die Landwirtschaft. Der Weltraum ist eine Ressource für die Lösung von Problemen in den Bereichen Terrorismusbekämpfung, Klimawandel, neue Energien und Materialien oder Orientierung durch Navigation. Er gewinnt eine strategische Dimension weil er die Zukunft der wissensbasierten Industrieländer mitbestimmt und auch die Zukunft der Entwicklungsländer betrifft. Mit Blick auf die Aufmerksamkeit, welche die USA und Russland der Entwicklung und Nutzung von Weltraumtechnologien seit Ende des Zweiten Weltkriegs entgegen brachten, wurde im Lauf der 1990er und 2000er Jahre auch dem Rest der Welt die zukünftige zivile und militärische Bedeutung einer kohärenten Weltraumpolitik bewusst. Dies galt, allen voran, auch für die Europäische Union (Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik (DGAP) 1988; Turek 2010, 2014). Mit der Aufnahme der Weltraumpolitik in den Lissaboner Vertrag als Teil der europäischen Forschungs- und Technologiepolitik wurde dieses Politikfeld signifikant aufgewertet.

Weltraumpolitik bekommt auch ein europäisches Gewicht

Anfang des 21. Jahrhunderts haben die Europäische Kommission und Politiker in der EU auf die ökonomische und strategische Bedeutung des Weltraums, die Dominanz der USA bei der Entwicklung und Nutzung entsprechender Technologien sowie die wachsende Sensibilität anderer Länder für seine Erforschung hingewiesen. Obwohl Europa bereits seit den 1980er Jahren des 20. Jahrhunderts raumfahrttechnologische Kapazitäten mit der Arianerakete und eigenen Satelliten entwickelt und mit der ESA eine gute institutionelle Basis errichtet hat, galten vielen die damaligen Aktivitäten als unzulänglich. Deshalb wurde die Europäische Kommission Anfang 2003 aktiv und legte ihr Grünbuch »Europäische Raumfahrtpolitik« vor, das zahlreiche Vorschläge zu einer in sich schlüssigeren und europäisch koordinierten Raumfahrtpolitik enthielt. Nach einem breit angelegten Konsultationsprozess fasste sie das Konzept einer solchen Politik am 11. November 2003 im Weißbuch »Die Raumfahrt: Europäi-

sche Horizonte einer erweiterten Union. Aktionsplan für die Durchführung der europäischen Raumfahrtpolitik« zusammen und präsentierte es der Öffentlichkeit. Als Politikfeld wurde die europäische Weltraumpolitik damit im Rahmen der benachbarten Politikbereiche der Forschungs- und Technologiepolitik, der Sicherheitspolitik oder der Industriepolitik äußerst wichtig.

Die europäische Kommission und die europäische Weltraumagentur (European Space Agency, ESA) handelten 2003 ein Rahmenabkommen aus, das die Beziehungen beider Institutionen auf das neue Konzept ausrichtete. Bereits 2002 hatte die ESA in Wien das Europäische Institut für Weltraumpolitik (European Space Policy Institute, ESPI) gegründet. Es hat als unabhängige Einrichtung die Aufgabe, Netzwerke, Studien, Beratung und Entscheidungshilfe bei der Festlegung weltraumpolitischer Strategien zu organisieren. Genaue Ansätze zu einer kohärenten Raumfahrtpolitik formulierten dann der EU-Rat ›Wettbewerbsfähigkeit‹ und der ESA-Rat auf Ministerebene, die sich 2005 auf der Grundlage des EG-ESA-Abkommens von 2003 als »Weltraumrat« konstituierten, mit einer entsprechenden Mitteilung an den Rat und das Europäische Parlament zur europäischen Raumfahrtpolitik. Diese enthielt Ziele, Aufgaben und Zuständigkeiten sowie einen Katalog von Durchführungsgrundsätzen. Mit ihrer Mitteilung »Auf dem Weg zu einer Weltraumstrategie der Europäischen Union im Dienste der Bürgerinnen und Bürger« vom April 2011 hat die Europäische Kommission schließlich auf die besondere Bedeutung des Weltraums für die Zukunft Europas hingewiesen. Sie hat damit eine »Antwort auf die gesellschaftlichen, wirtschaftlichen und strategischen Herausforderungen, vor denen wir stehen« formuliert. Im Kontext der Entwicklung einer europäischen Weltraumpolitik seit Anfang der 2000er Jahre bedeutete diese Mitteilung eine Neuausrichtung. Diese war mit Blick auf die Zielsetzungen der Weltraumpolitik von großer Bedeutung.

Die zivile und militärische Bedeutung des Weltraums nimmt zu

Es wurde klar, dass etwa Satelliten für die Navigation anschwellender Verkehrsströme und weltraumgestützter Sicherheitskomponenten zur Führung militärischer Kapazitäten im Rahmen der Europäischen Sicherheitsstrategie gebraucht würden. Projekte wie Galileo (Navigation und Ortung) oder Copernikus (GMES, Global Monitoring for the Environment and Security) gelten als Flaggschiff-Projekte. Darüber hinaus hat sich die ESA 2008/2009 mit den Weltraumteleskopen Herschel und Planck spektakuläre und ambitionierte Forschungsgebiete im Bereich der naturwissenschaftlichen Erkundung des Universums erschlossen. Die Raumfahrt dient ausdrücklich europäischen Zielen des Umweltschutzes, der Mobilität, der Sicherheit und der Informationsgesellschaft. Neben der Entwicklung geeigneter technologischer Kapazitäten im Raketen-, Plattform-, oder Satellitenbau sowie in der Nachrichteninfrastruktur er-

forderte dies eine entsprechende Legitimation der politischen Zuständigkeiten auf europäischer Ebene. Mit dem Grünbuch sowie dem Weißbuch zur europäischen Raumfahrtpolitik sowie der Zuweisung entsprechender Kompetenzen an die Europäische Weltraumagentur wurde diese Legitimation im Rahmen eines systematischen Findungsprozesses von den entsprechenden Institutionen und Projekten realisiert. Die Mitteilung zu einer Weltraumstrategie der Europäischen Union hebt diesen Bedeutungszuwachs hervor.

EGNOS und Galileo sind die Flaggschiff-Projekte der EU-Weltraumpolitik

Aus operativer Sicht heißt dies die Fortsetzung der europäischen Satellitenprogramme Galileo und EGNOS; die konsequente Umsetzung des Europäischen Erdbeobachtungsprogramms Copernicus zur Überwachung von Land, See, Atmosphäre, Luftqualität und Klimawandel sowie Notfalleinsätze und Sicherheit; Schutz der europäischen Weltrauminfrastruktur durch den Aufbau eines Europäischen Systems zur Weltraumlageerfassung (Space Situation Awareness, SSA), um den Verlust von Technologien durch Zusammenstöße mit Weltraummüll und durch Weltraumwetter zu verringern (Schäden im Jahresdurchschnitt in Höhe von etwa 332 Millionen EUR); Unterstützung der Weltraumforschung etwa im Kontext der Internationalen Weltraumstation (International Space Station, ISS); Unterstützung von Grundlagenforschung und Entwicklung; Stärkung der Partnerschaft zwischen Europäischer Weltraumorganisation und den EU-Mitgliedstaaten; die Entwicklung eines weltraumbasierten Datenrelay (EDRS); die Entwicklung einer neuen Weltraumrakete Ariane 5-ME bzw. 6 bis 2017/2018 sowie die Beteiligung an der amerikanischen Raumkapsel Orion (u.a. Marserkundung). In wachsender Weise sind darüber hinaus internationale Kooperationen wie bei der Internationalen Weltraumstation (International Space Station, ISS) nötig. Hier ist etwa die 2007 von NASA, ESA, Roskosmos, CNSA (China) und 10 weiteren Weltraumagenturen formulierte »Global Exploration Strategy« wichtig, welche die Grundzüge einer gemeinsamen Raumfahrtstrategie entworfen hat.

Außerordentlich wichtig sind hierbei Galileo und Copernicus. Galileo ist das erste von der EU und der Europäischen Weltraumorganisation gemeinsam durchgeführte Projekt. Galileo ist das europäische Satellitennavigations- und Zeitgebungssystem, das unter alleiniger ziviler Kontrolle steht. Es wird auf den Zentimeter Daten zur genauen Positionsbestimmung liefern und ähnelt dem US-amerikanischen System NAVSTAR-GPS und dem russischen GLONASS-System. Das System basiert auf einer Grundkonstellation von 30 Satelliten, welche die Erde in einer Höhe von 23.260 km umkreisen und einem Netz von Bodenstationen, die die Satelliten kontrollieren. Copernicus offerierte 2013 ein neues System der offenen Datenverarbeitung, das kostenfreien, unbeschränkten und offenen Zugang zu einer Fülle wichtiger Umweltdaten gewährt. Mit

diesem Zugang wird die Entwicklung von Anwendungen für eine Reihe von verschiedenen Wirtschaftszweigen wie der Landwirtschaft, der Versicherungen, dem Verkehr und der Energieversorgung gefördert. Das Programm arbeitet mit großem Erfolg mit Daten aus bestehenden Satellitenmissionen und Sensoren an Land, zu Wasser und in der Luft. Als der Taifun Haiyan Ende 2013 die Philippinen verwüstete oder Überschwemmungen auf Sardinien herrschten, konnte das System das Katastrophen- und Krisenmanagement in beiden Regionen massiv mit unverzichtbaren geologischen Daten unterstützen.

Die globale Satellitennavigation ist geprägt durch Kooperation und Konkurrenz

Das Beispiel der internationalen Weltraumstation zeigt den globalen Charakter einer internationalen Weltraumpolitik auf, die auf globale Kooperation angewiesen ist. Gleichzeitig ist die Weltraumpolitik ein Feld internationaler Konkurrenz. Am deutlichsten wird dies in der Wettbewerbssituation zwischen dem amerikanischen GPS-System und dem europäischen Galileosystem. Aber zugleich integriert Galileo demgegenüber wiederum vielfältigste internationale Kooperationen und die EU strebt eine enge Kooperation mit den Amerikanern im Bereich der satellitengesteuerten Navigation an und will das System mit seinem US-Gegenstück GPS kombinieren, um so die Luftverkehrssicherheit zu erhöhen (Europäische Kommission 2014: 68). Auch dies ist mit Blick auf die amerikanische Konkurrenz bemerkenswert. Denn viele Staaten beteiligen sich ebenfalls an diesem Projekt. Das ist zum Beispiel China, das sich mit 280 Millionen Euro engagiert. Hinzu kommen Indien, Israel, Marokko, Saudi-Arabien, die Schweiz, Norwegen, Südkorea und die Ukraine. Argentinien, Australien, Brasilien Kanada, Mexiko oder Russland sind interessiert. Russland brachte im Oktober 2011 die ersten zwei Galileo-Satelliten mit einer Sojus-Rakete vom europäischen Weltraumbahnhof in Französisch-Guayana ins All. Die USA standen und stehen Galileo skeptisch gegenüber. Mit Blick auf die vielfältigen Möglichkeiten des Systems im öffentlichen, kommerziellen und sicherheitsdienlichen Bereich[44] befürchteten sie Gefahren einer unkontrollierten Nutzung. Bedenken bezüglich technischer Beeinflussungen des NAVSTAR-GPS-Systems durch Galileo konnten hierbei mittlerweile ausgeräumt werden, die Sorgen hinsichtlich der militärischen Relevanz des Systems bestehen weiter fort. Der Bereich der militärischen Aspekte der Information, Kommunikation und Führung von militärischen Operationen ist hierbei sensibel. Der stille Einsatz amerikanischer Drohnen im amerikanischen Antiterrorkampf ist auf eine globale IKT-Struktur angewiesen. Gleiches gilt für die

44 | Vgl. als Übersicht über die Fähigkeiten des Systems http://de.wikipedia.org/wiki/Galileo_Satellitennavigation, aufgerufen am 10.April 2014.

globale Überwachung elektronischer Kommunikationen im Internet oder via Mobiltelefonie. Inwieweit eine weltraumgestützte Satellitenstruktur und die ergänzenden terrestrischen Aufklärungsmöglichkeiten hegemoniale Gefühle von Staaten wie den USA, China oder Russland stören, könnte also ein brisantes Thema der Zukunft sein. Insofern ist die globale Weltraumpolitik geprägt durch Kooperation und durch Konkurrenz. Gleichzeitig nehmen aber auch Probleme oder Gefahren bei der Nutzung des Weltalls im militärischen und zivilen Bereich zu. Während einerseits die technologische Erschließung des Alls in vollem Gange ist, wächst andererseits auch der Druck, internationale Regeln für ein kosmisches Miteinander der weltraumfahrenden und weltraumnutzenden Nationen zu entwickeln. Dies bezieht besonders die Problematiken des wachsenden Weltraumschrotts ausgedienter oder beschädigter Satelliten und des Wettrüstens im Weltraum mit ein (Mutschler 2013).

Insgesamt aber ist der Nutzen des Weltraums für die Menschheit enorm

Dies lässt sich an einem spektakulären – nicht militärischen – Beispiel illustrieren. Ende 2013 wurden von Forschern der Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (UNESCO) und der kenianischen Regierung unter den Wüsten im Norden Kenias zwei riesige Reservoirs mit Grundwasser entdeckt – theoretisch genug, um nicht nur die durch Dürre geplagte Region selbst, sondern ganz Kenia mindestens über Jahrzehnte mit Wasser zu versorgen. Das Reservoir wurde per Satellit und Radar aufgespürt. Und nicht nur die Versorgung des Landes mit Trinkwasser und – indirekt – nunmehr anbaubaren Agrarprodukten könnte somit sichergestellt werden. Der für die Süddeutsche Zeitung tätige Korrespondent in Nairobi, Tobias Zick, wies darauf hin, dass dieser, durch moderne weltraumgestützte Technologien ermöglichte Fund auch friedensstiftend sein könne. In Konkurrenz um Weideland und Wasser bekämpfen sich immer wieder die verschiedenen Nomadenstämme gegenseitig, stehlen einander ihr Vieh, beinahe monatlich sterben dabei Menschen (Zick 2013). Alles in allem aber zeigt dieses Beispiel auf, wie außergewöhnlich nutzbringend eine satellitengestützte Erdbeobachtung für die Bereiche Ernährung und Umwelt eingesetzt werden kann, auch mit Blick auf persönliche Integrität und Sicherheit.