

Die Zukunft der Einbildung. Information, Informationssicherheit und globale Entwicklung

Durch die technologischen Revolutionen kehrt Information heute zu ihrem Ursprung als „Ein-bildung“ zurück. Damit schließt sich ein Kreis. Waren technische und menschliche Dimensionen seit dem Beginn der Moderne immer stärker voneinander getrennt, wachsen sie heute wieder zusammen, jedoch in ambivalenter Weise. Damit sind ebenso viele Fragen verbunden, wie sich Potential nach verschiedenen Seiten eröffnet. Das Zusammenwachsen von Information und Einbildung ist nicht nur eine anthropologische Schlüsselbewegung, sondern auch eine kontextpolitische Kernentwicklung der Gegenwart. Die Zukunft der Einbildung wird von der Sicherheit der Information abhängen.

Eine neue Konstellation

Wie stark die globale Konstellation von der Beherrschung und Manipulation von Information abhängig geworden ist, hat im Sommer 2013 der Fall Edward Snowden gezeigt. Für viele überraschend, zeigte Snowden am Beispiel der Totalüberwachung von Internet und Telekommunikation durch amerikanische, britische und französische Geheimdienste auf, dass das Selbstbild offener Gesellschaften wenigstens teilweise zur Einbildung geworden ist. Denn es hängt von Überwachungsmechanismen ab, die Kernbegriffe wie Individualrechte und Privatsphäre ignorieren, ja außer Kraft setzen. Snowden war allerdings keineswegs der erste, der auf die mittlerweile fundamentale Abhängigkeit offener Gesellschaften und ihrer dialogischen Rationalität von einer zweiten, hinter ihr liegenden unsicht-

baren Sphäre verwies, die nicht demokratischen Gesetzen folgt und auch nicht offen ist. Vor Snowden hatten bereits „Whistleblower“ (das heißt Geheimnisverräter, die ihren Verrat damit begründen, dass er dem Wohl der Öffentlichkeit, der Förderung von Demokratie und Pluralismus und der Verteidigung von Bürgerrechten diene) wie Bradley Manning oder Aaron Swartz die Entstehung von Parallelwelten aufgewiesen – von chinesischen Hackern ganz zu schweigen, deren Namen man allerdings in der Regel nicht kennt, da China keine Demokratie ist und mit ihnen kurzen Prozess macht. Dass China, Russland und andere illiberale oder autoritäre Staaten keineswegs anders als die USA oder Großbritannien verfahren, im Gegenteil alle Anstrengungen unternehmen, um den Westen in den Überwachungsmaßnahmen zu überflügeln, dazu offen einen Cyberkrieg gegen den Westen führen und nach innen massive Zensur ausüben, mag angesichts des Ausmaßes von Snowdens Enthüllungen nicht mehr sonderlich überraschen. Die amerikanische Überwachung, die bereits Anfang des Jahrtausends – vor den Terroranschlägen des 11. September 2001 – begann, ist nicht zuletzt eine Reaktion auf Chinas massive Offensive in der Internet- und Kommunikationsspionage, die, organisiert unter anderem in einer eigenen geheimen „Armee-Einheit 61398“, einen epochalen Erfolg nach dem anderen feiert. Ihre Tätigkeit führte im ersten Halbjahr 2013 unter anderem zum Diebstahl der Baupläne des modernsten US-Kampflugzeugs F-35 sowie anderer kritisch

wichtiger Waffensysteme, aber auch industrieller Hochtechnologie, was die Abkürzung von Jahrzehnten Entwicklung bedeutet. Die chinesischen Erfolge in der Internet-Spionage nach innen (gegen die eigenen Bürger) und nach außen (gegen andere Mächte) sind faktisch weit wichtiger als alle möglichen Erfolge in militärischen Konfrontationen, die dadurch überflüssig oder jedenfalls weniger wichtig werden.

All dies zeigte, in der historischen Symptomatologie weniger Monate gebündelt, erneut auf: Wer heute und künftig über Information gebietet, gebietet über Ideen. Der alte humanistische Gegensatz insbesondere in der zentraleuropäischen Welt zwischen Idee und Information, Imagination und Technologie, Humanität und Abstraktion, geschuldet einer etwa noch bei Günther Anders und Martin Heidegger kulminierenden Technikaversion, die ihre Wurzeln noch im 19. Jahrhundert hatte, wird obsolet.

Aufsehenerregende Fälle wie Snowden oder der „pazifische“ Cyberkriegs zwischen China und den USA sind aber nur die Spitze des Eisbergs. Sie taugen für vorübergehendes Sensationsheische und wohliges öffentliches Erschauern, berühren aber den gestaltbaren Alltag der meisten Bürgerinnen und Bürger nicht. Doch die Problematik an der Schnittstelle zwischen Information und Lebenswelt reicht heute bereits viel tiefer – und nimmt viel alltäglichere Formen an, deren Bedeutung wir jedoch noch immer weit unterschätzen.

Die Durchdringung des Alltags

Im Mai 2013 führten global operierende Internet-Kriminelle einen Jahrhundert-Bank-

raub aus. Sie manipulierten zeitgleich die Daten von Bankomatkarten in 26 Ländern und machten innerhalb von 10 Stunden auf mehreren Kontinenten eine Beute von 45 Millionen Dollar. Nicht erst dieser Fall zeigte es erneut eindrucksvoll auf: Information und Informationssicherheit bestimmen den Zugang zu globalen Kernbereichen und gesellschaftlichen Basisvorgängen Jahr für Jahr stärker. Wer Information beherrscht, indem er Informationssicherheit umgeht, kann die Kybernetik hypermoderner transnationaler Schaltstellen ganz unterschiedlich für sich nutzen.

Intelligente Kriminelle, die, wie es die New Yorker Staatsanwältin Loretta Lynch ausdrückte, „statt Pistolen und Masken Laptops und das Internet verwenden“ und mit der Fähigkeit zu Zugang, Koordination und Logistik ausgestattet sind, werden mithilfe der neuen Kommunikationstechnologien und der immer stärkeren Virtualisierung des Geldsektors fähig, hoch komplexe strategische Operationen in Echtzeit auf globaler Ebene durchzuführen. Entscheidend sind dabei nicht vorrangig ihre technischen Fähigkeiten, sondern ihr Vorstellungsvermögen, das heißt ihre Antizipationsfähigkeit „kybernetisch“ vernetzter Prozesse, die sie besser vorwegnehmen müssen als die professionellen Abwehrstrategen von Nationen und Institutionen.

Damit entsteht erstmals eine wirkliche vierte Ebene neben Staaten, NGO's und transnationalen Organisationen. Es ist die Dimension „anderer“ globaler Akteure, die nicht mehr wie herkömmliche Kriminelle operieren und in Fähigkeiten und Instrumenten den Potentialen von Staaten prinzipiell unterlegen sind, sondern sich wegen des Übergangs der „Werkzeuge“ von

Waffen zu Computern erstmals voll und ganz auf demselben Niveau wie diese befinden. Konnten Kriminelle bislang das Gewaltmonopol des Staates schon wegen ihrer unterlegenen Waffen nicht brechen, so sieht das im Internet anders aus. Und nicht nur das: sie sind wegen der elektronischen Allverbindung und Internetabhängigkeit des Großteils kritischer Information, die ohne solche Verbindung nicht mehr effektiv genutzt werden kann, auch direkt mit deren innersten Bereichen vernetzt, haben jederzeit Zugriff auf die Zentren. Waren früher Raum- und Zeitfaktoren die am schwierigsten zu überwindenden Hindernisse, so sind diese heute durch das Internet trotz aller Schutzbemühungen faktisch ausgeschaltet. Nicht nur finanztechnische, sondern auch militärische und zivile Entwicklungen sind davon immer umfassender betroffen.

Sehr unterschiedliche Kräfte machen sich diese Konstellation zunutze. Die entsprechenden Phänomene häufen sich von Monat zu Monat, ja von Woche zu Woche. So meldete Yahoo Japan in der dritten Mai-Woche 2013, sein System sei gehackt und mehr als 22 Millionen Benutzerdaten entwendet worden. Man habe das erst eine Woche nach der Attacke bemerkt. In derselben Woche hackte die „Syrian Electronic Army“, eine Gruppe von Syrern, die Präsident Assad unterstützt, Webseite und Twitter-Feeds der „Financial Times“, um darauf Links zu einem Youtube-Video zu posten, das angeblich die Hinrichtung syrischer Regierungssoldaten durch Rebellen zeigt. Bereits im April hatte die „Electronic Army“ den Twitter-Feed der Nachrichtenagentur AP gekapert. Eine gefälschte Meldung über Explosionen im Weißen Haus löste damals an den Aktienmärkten

einen Kursrutsch aus. Nachdem ein spanischsprachiger Sender Anfang 2012 berichtet hatte, die damalige venezolanische Konsulin in Miami habe Pläne für eine gemeinsame Cyber-Angriffe Venezuelas mit Kuba und dem Iran auf die USA entworfen, wurde die Frau von der Regierung der Vereinigten Staaten des Landes verwiesen, worauf der venezolanische Geheimdienst mit der Überwachung zweier Journalisten des Senders in den USA reagierte.

Die Reaktion der Angegriffenen ist meist dieselbe: Sie reagieren mit teuren Sicherungsmaßnahmen, die nicht selten von ehemaligen Hackern ausgeführt werden, die für viel Geld oder auf Regierungs- und Polizeidruck die Seiten gewechselt haben. Dass diese Reaktionen zu 99% Reaktionen bleiben und das strategische Heft der Offensive in fast allen Fällen in der Hand der Angreifer verbleibt, die im Netz aufgrund dessen Grundstruktur sowohl virtuell allpräsent wie ungreifbar sind, ändert sich dadurch freilich nicht. Nach den Maßnahmen wird regelmäßig bekannt gegeben, die Zugänge seien gesichert worden. Doch wie verletzlich die bestehenden Arrangements bleiben, zeigt unter anderem die Meldung, dass „eine simple Computer-Abfrage in Süddeutschland Anfang Mai 2013 beinahe einen Totalausfall der Stromnetze in Österreich verursacht hat. Das zeigt, wie verletzlich die wichtigen Versorgungsnetze und andere Einrichtungen wie Wasserleitungen, Kraftwerke, große Spitäler durch Internet und Computer-Vernetzung geworden sind. Damit diese im vorliegenden Fall in Summe 180 Einrichtungen künftig vor Cyber-Attacken besser geschützt sind, richtet das Österreichische Innenministerium nun ein neues Zentrum

zum Schutz dieser ‚kritischen Infrastruktur‘ ein.“ (ORF Teletext, 18.05.2013, S. 115). Also ungefähr zehn Jahre zu spät – wie die meisten anderen Länder auch. Trotz des zunehmenden Drucks von mutmaßlich aus China stammenden Cyber-Attacken auf Infrastrukturen, Firmen und Know-how, der im Westen allmählich zu einem Bewusstseinswandel führt, verringert sich der notorische Rückstand der „Beschützer“ gegenüber den „Angreifern“ nur langsam.

Die Herrschaft der Information: Alle Felder sind betroffen

Im Gefolge dieser Entwicklung gilt: Die Weltmeere und mit ihnen die wichtigsten strategischen Ressourcenwege wurden seit dem zweiten Weltkrieg physisch weitgehend gesichert, wenn auch in den vergangenen Jahrzehnten weniger zum Wohl der Menschheit, als vielmehr zum Vorteil einzelner Leitmächte und ihrer Allianzen, von deren diplomatischer Verhandlungsmaße sie Teile waren. An ihrer Stelle wird heute das Internet zum globalen Feld der Piraten – und die Kriegsschiffe, die die Schifffahrtsrouten der Zukunft im Cyberspace sichern, wurden noch kaum bis gar nicht entwickelt, geschweige denn eingesetzt.

Der Grund dafür ist einfach. Die internationale Gemeinschaft scheint angesichts überproportional angreifbarer Infrastrukturen und mangelhafter Sicherheitseinrichtungen immer noch nicht ausreichend bemerkt zu haben, dass hier ein Kernaspekt der anstehenden zivilisatorischen Entwicklung auf dem Spiel steht. Dieser reicht nicht nur in alle sechs Schlüsselfelder der heutigen „globalen Systemverschiebung“: Wirtschaft, Politik, Kultur, Religion, Tech-

nologie und Demographie hinein. Sondern er betrifft einen weit grundlegenderen Bereich: die Anthropologie, die Dimension des Menschlichen selbst. Denn „Information“ heißt wörtlich: „Ein-bildung“. Wer sie beherrscht, beherrscht in der Epoche universaler Technisierung damit nicht nur die abstrahierten Werteströme, sondern auch die Voraussetzung aller anderen Bereiche. Das zeigen bereits die obigen Beispiele, bei denen Einbildung wichtiger war als Realität. Geht es also bei „Informationssicherheit“ in den kommenden Jahren buchstäblich um nicht weniger als um die Sicherung der „Einbildungskraft“ – verstanden als die gestaltende Grundkraft von allem, was Form annimmt?

Aufstieg der Cyberwelt zur wichtigsten Sparte von Kontextpolitik

Während die internationale Wirtschaftsspionage mittels Internet boomt und zu einem realpolitischen High-Tech Faktor weltweiter Machtbeziehungen wird, werden kalte und auch „heiße“ Kriege zunehmend auf virtueller Ebene mittels Hackerangriffen geführt. Das haben zuletzt die sich seit 2012 auffallend häufenden gegenseitigen Internet-Gefechte um kritische Information zwischen den „G-2“ des 21. Jahrhunderts, China und den USA, sowie ihren „Stellvertretern“ in großen Weltfirmen wie Google, Yahoo, Apple oder Microsoft gezeigt. Nicht zufällig fand die Mehrzahl der mutmaßlich von Chinas geheimer „Militäreinheit 61398“ ausgehenden Hackerattacken auf Silikon Valley statt – denn dort holt man sich nicht Produkte der Information, sondern deren Basisbausteine, von denen aus dann alle anderen Bereiche zugänglich werden. Davon ausgehend werden politische Strategien und diplomatische Warnungen zunehmend mit

Viren-Attacken kombiniert, wie etwa die auffällig auf den Nahen Osten (Iran) begrenzten Fälle Stuxnet und Flame unterstreichen. Kriege zwischen konventionellen Armeen ohne vorhergehende Cyber-Attacken auf Verteidigungssysteme und Abwehrnetzwerke sind bereits seit dem Kosovo-Krieg 1998-99 undenkbar.

Die *ökonomische* und die *politisch-militärische* Dimension sind aber keineswegs die einzigen, ja vielleicht nicht einmal die wichtigsten im neuen virtuellen „Great game“. Kaum woanders zeigt sich die Entstehung einer multidimensionalen Zivilisation und der weltweite Aufstieg von Kontextpolitiken zu neuen Zentren des Politischen, welche die traditionelle Vorherrschaft des ökonomisch-politischen Komplexes und damit von Partei- und Institutionenpolitiken brechen, so deutlich wie im Aufstieg der Bedeutung von Information auf anderen Feldern der entstehenden Weltzivilisation. *Kulturell* dienen Cyberkriege zunehmend der Unterminierung der Vorherrschaft des Westens und der Etablierung einer Welt der „competing modernities“, in der verschiedene globale Ordnungsvisionen konkurrieren. Und selbst *religiöse* Botschaften werden spätestens seit 2001 zunehmend mit Cyberkämpfen um Recht und Unrecht kombiniert – was unter anderem dadurch bewiesen ist, dass im Jahr 2012 nach offiziellen UNESCO-Statistiken nicht erotische oder militärische, sondern religiöse Internet-Seiten die mit Abstand infektionsgefährlichsten der Welt waren. *Technologisch* wird der Cyberwar zu einem Experimentierfeld der fortgeschrittensten Avantgarden, der in seiner Vorreiterrolle Raumfahrt und Hochtechnologie-Rennsport überholt hat. Und auch die *Demographie* spielt eine Rolle. Denn

nicht nur individuelle Begabung, sondern auch Migrationsströme zwischen Hacker-Kulturen und -Gesellschaften, die rasche Vervielfältigung durch den Generationenwechsel (die neuen Generationen sind mit dem Internet aufgewachsen und sind „natürlich“ fähiger, und sie sind es biographisch früher) sowie die Anzahl verfügbarer Cyber-Krieger sind von wachsender Bedeutung im „Kräftemessen hinter dem Vorhang“.

Information und Einbildungskraft

All diese sechs Schüsseldimensionen drehen sich bereits heute im Zentrum um ähnliches, wenn nicht gar dasselbe: um „Cyberdialektiken“. Diesen geht es nicht um Gegenstände oder Ressourcen, sondern um das künftig allem Wesentlichen Voraus- und Zugrundeliegende: um Information. Sie drehen sich um das Wesen und die Praktiken von „Ein-Formung“ (informare): also nicht um das Ergebnis von Imaginations-, Gestaltungs-, Portionierungs- oder Proportionsvorgängen (0 und 1), sondern vielmehr um den Prozess, der diese ausmacht. Sie drehen sich also genau genommen nicht um die Einbildung als Produkt, sondern um die *Einbildungskraft* als Vorgang und Befähigung. Oder etwas aristotelischer ausgedrückt: Es geht in ihnen weniger um die Aktualisation einer bereits vorliegenden Form, sondern um den Schnitt- und Übergangspunkt zwischen Potentialität und Aktualisation.

Was anderes als „In-formation“ in eben diesem Sinne aber ist Einbildungskraft in den intellektuellen und kulturellen Traditionen des Westens? Es ist genau an diesem noch kaum ausreichend wahrgenommenen Punkt, wo sich die humanistischen und anthropologischen Traditionen, dar-

unter in Europa vor allem auch die des deutschen Idealismus, auf unverhoffte Weise in den postmodernen Informationskulturen nicht nur wiederfinden und ihre Probleme und Chancen wiederholen, sondern auch „aufheben“ im Hegelschen Doppelsinn: sich sowohl in die Zukunft hinein aufbewahren wie auch auflösen, und zwar beides zugleich.

Die Perspektiven dieses paradoxalen Vorgangs, den man nicht zu Unrecht als zweiseitiges Schwert bezeichnen kann, sind heute noch kaum absehbar. Sicher ist, dass sie sehr tief reichen werden, ja zu einer „Umwertung aller Werte“ führen könnten – und zwar nun in ganz buchstäblichem, „informatischem“ Sinn. Der Beispiele, wo Einbildungskraft und Information eins werden und dabei zu einer Umwertung beider beteiligten Dimensionen führen, sind viele.

Auf der einen Seite entstehen heute in den USA unter den jüngeren Generationen die neuen Kulturen des „Bodyhacking“ und „Biohacking“. Biohacker sind

„...besessen von der Idee, den menschlichen Körper zu verbessern, indem sie neue Wege erkunden, Maschinen und technische Geräte in ihre Körper einzufügen. Sie fügen zum Beispiel magnetische Implantate in ihre Körper ein... Computer sind für sie die Hardware. Apps sind die Software. Menschen sind die Wetware. Biohacker sind anti-autoritär eingestellt, sowohl gegen Anarchisten wie gegen Christen... sie sind Techno-Libertarians. Magnetchips aus seltenen Erden wie Neodymium in den Körper einzupflanzen, wurde von Künstlern aus der Avantgarde der Piercing-Kultur sowie Transhumanisten vorgemacht, die daran interessiert waren, mit der Entwicklung eines sechsten Sinnes zu experimentieren. Steve Harworth, der sich als einen „Menschen-Evolutionskünstler“ (human evolution artist) bezeichnet und dessen Spezialisierung die

Körpermodifikation ist, inspirierte eine ganze Generation, sich magnetische Chips implantieren zu lassen... Das Implantat erlaubt es einer Person, elektromagnetische Felder in der Umgebung zu fühlen: einen Mikrowellen-Ofen in der Küche, eine U-Bahn, die unterirdisch vorbeifährt, oder die Hochspannungsleitungen hoch über dem Kopf. Diese zusätzliche Wahrnehmung ist zwar interessant, hat aber weniger Nutzen. Aber der Magnet ist, glaubt man seinen Propagatoren, nur ein erster Schritt auf dem Weg zu Größerem. Der Eingriff ist billig, mit einem Minimum an invasiver Operation. Der Empfänger gewöhnt sich daran, etwas Fremdes im eigenen Körper zu tragen, und er erkennt, wieviel mehr der menschliche Körper kann, wenn er ein wenig Hilfe... in Form digitalen Inputs erhält. Ein weiteres Beispiel ist ein Gerät, das sich Großer Tümmler (Bottlenose) nennt, ein kleines schwarzes Rechteck von der halben Größe einer Zigarettenschachtel, das man über den Finger stülpt. Wie sein Namensgeber sendet es einen elektromagnetischen Impuls aus und misst die Zeit, die er braucht, um als Echo zurückzukommen. Damit kann man Wahrnehmungs- und Entfernungsbilder der Umgebung erhalten... Unser Gehirn arbeitet ohnehin mittels Elektrizität, also warum nicht dabei helfen, das zu intensivieren?, so die Frage der Bodyhacker.“ (B. Popper: Cyborg America. Inside the Strange New World of Basement Body Hackers. In: The Verge, August 8, 2012, <http://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers>. Übersetzung aus dem Englischen: Roland Benedikter).

Auf der anderen Seite ging im August 2008 die Meldung um die Welt, es sei Wissenschaftlern gelungen, mittels des Scans von menschlichen Gehirnen Daten aus diesen zu extrahieren – also gewissermaßen Gedanken zu lesen. Unter dem Titel: „Gedankensteuerung: Interface hackt Gehirn. Forscher extrahieren Informationen wie Pin-Codes aus Köpfen“ meldeten die Nachrichtenagenturen:

„Hirn durchleuchtet: Informationen nicht sicher. Wissenschaftler haben einen Weg gefunden, Gedankensteuerungs-Interfaces dazu zu verwenden

den, Informationen aus den Gehirnen von Probanden zu extrahieren. Forscher der Universitäten Oxford, Kalifornien und Genf haben gezeigt, dass Daten wie Pin-Codes gefunden werden können, indem den Versuchspersonen passende Bilder gezeigt werden, während sie Elektroden auf dem Kopf tragen. Bei bekannten Bildern verrät das Gehirn sich durch spezifische Signale. Das Verfahren ist bei weitem noch nicht perfekt, aber in 20 Prozent der Fälle konnte ein vierstelliger Pin-Code im ersten Versuch erraten werden. Ihre Ergebnisse haben die Forscher bei der USENIX-Konferenz in Bellevue in den USA präsentiert (On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces, USENIX Security Conference, August 8-10, 2012, <http://bit.ly/NMHiHo>). Der Versuchsaufbau ist einfach nachvollziehbar. Haben die Probanden Assoziationen zu den gezeigten Bildern, entsteht im Hirn ein anderes Signal. Das evozierte Potenzial kann über die Elektroden abgelesen werden. Beim Erraten des Geburtsmonats der Versuchspersonen betrug die Erfolgsquote im ersten Anlauf sogar beinahe 60 Prozent. Hier wurden die Probanden via Bildschirm gefragt, in welchem Monat sie Geburtstag haben. Anschließend wurden in zufälliger Reihenfolge die Monatsnamen kurz eingeblendet und nach den verräterischen Hirnströmen gesucht. Mit ähnlichen Versuchsanordnungen haben die Wissenschaftler auch den Wohnort und den Namen der Bank, bei der die jeweilige Versuchsperson Kunde ist, zu erraten versucht. Hier liegen die Erfolgsquoten zwischen 20 und 30 Prozent. Mit implantierten Elektroden könnte die räumliche Auflösung noch deutlich erhöht werden. Das Signal, auf das sich die Forscher konzentrieren, heißt P300. Zur Kalibrierung des Neuro-Interfaces mussten die Probanden einige Testläufe mit Bildern von Ziffern machen. So konnten die Forscher ihre Apparaturen auf die individuellen Hirne einstellen...

Mit ihrer Arbeit wollen die Wissenschaftler darauf hinweisen, dass Gedankensteuerungs-Interfaces, die sich unter anderem unter Videospiele immer größerer Beliebtheit erfreuen, ein Sicherheitsrisiko darstellen. Solche Interfaces haben für Computerspiele sicher großes Potenzial. Der eigentliche Nutzen liegt aber in der Medizin, wo vielen Patienten geholfen werden kann. Die Wis-

senschaftler haben für ihre Experimente eine kommerziell erhältliche Elektrodenhaube verwendet. Die Geräte kosten mittlerweile nur noch um die 200 Euro. Über die Programmierschnittstellen können die gemessenen Hirnstrom-Daten praktisch beliebig verwendet werden. Mit cleveren Tricks könnten sich Außenstehende auf diesem Weg sensible Informationen aus den Köpfen der User holen.“ (Presstext Deutschland, 21.08.2012, <http://www.pressetext.com/news/20120821025>).

Das Kernparadoxon: Während die Bedeutung der Schnittstelle zwischen Information und Einbildungskraft für das Leben steigt, wird der Abgrund zwischen dem Information-Einbildungs-Komplex und der Lebensrealität größer

Es sind nicht einzelne dieser Entwicklungen, sondern ihre Kombination am Schnittpunkt aller sechs Kerndimensionen der heutigen globalen Systemverschiebung sowie – vor allem – ihr Übergang von Einzelfällen zu grundlegenden Systemkonstanten, was Information und Informationssicherheit zu zentralen Faktoren des Weltkonflikts des 21. Jahrhunderts macht: der Dialektik zwischen demokratischen und nicht-demokratischen, liberalen und illiberalen Gesellschaften. Denn auch das Konzept globaler westlicher Vorherrschaft im 21. Jahrhundert: „Soft Power“ (Joseph Nye, Hillary Clinton), also die Dominanz der Demokratie mittels der größeren Attraktivität und Überzeugungskraft von Ideen der Offenheit, Pluralität, Gleichheit, Freiheit und Individualität sowie der dazugehörigen Lebensstile und Gesellschaftssysteme beruht letztlich auf Information und ihrer Sicherheit: auf der Sicherheit, dass Informationen erstens gelten, dass sie zweitens fair und allgemein zugänglich sind, dass sie drittens ausreichend transparent sind und dass sie viertens in offenem, globalem Vergleich mit-

einander positiv konkurrieren dürfen. Was mit der traditionell aufgefassten Einbildung im Konzert der Weltkulturen bisher nicht immer der Fall war.

Doch als Reaktion auf die exponentiell wachsende Bedeutung von Information, die im wahrsten Sinn des Wortes zum kapillaren Grundbaustein der entstehenden Weltgesellschaft wird, bilden Regierungen derzeit zunächst weltweit immer größere Sicherheitsteams für die Verteidigung im Internet. Zugleich nimmt die innenpolitische Überwachung und das Spiel mit dem Durchbrechen dieser Überwachung durch hochqualifizierte Gruppen rapide zu, und zwar sowohl in demokratischen Gesellschaften wie den USA wie in nichtdemokratischen wie China.

Im Wechselspiel der daraus resultierenden Professionalisierung auf allen Seiten steigt das Niveau der Informationssicherheit rapide an. Dadurch vergrößert sich der Abstand zwischen dem Bewusstsein und den Fähigkeiten des Bürgers und den Anforderungen der Realität. Das ist letztlich auch ein Effekt der jahrhundertlangen, universalen Kultivierung des Realen. Während immer mehr Menschen Privates in sozialen Netzwerken preisgeben und sich damit bewusst Risiken aussetzen, werden in Kernländern Europas wie zum Beispiel Italien jedes Jahr mehr als 1 Million Überwachungen durchgeführt, ohne dass sich die Bürger dieser Dimension bewusst sind. Die Sicherheit der dadurch gewonnenen Daten ist prekär. Als der 2011 im Amt befindliche italienische Ministerpräsident Silvio Berlusconi im Rahmen eines Handy-Privatgesprächs aus seiner schwer bewachten Privatwohnung um Mitternacht den Satz formulierte: „Italien ist ein Scheiß-

land“, stand es am nächsten Tag in allen Zeitungen. Obwohl Barack Obamas Telefon weit besser bewacht wird und die Informationssicherheit in den USA ein anderes Niveau hat als im Cyber-Entwicklungsland Italien, ist es im Prinzip doch ebenso angreifbar. Zugleich versuchen internationale Abkommen wie zwischen den USA und der EU, individuelle Informationssicherheit etwa betreffend Identität, Aufenthaltsort und Reisepläne zu relativieren oder zu umgehen. Das Bankgeheimnis wird aufgehoben, so wie seit 2012 in Italien, und automatischer Datenaustausch über intime Steuerdaten zwischen EU-Staaten wird forciert.

Währenddessen konzipieren führende „global player“ wie China und die USA ihre Rolle zwar über die „soft power“ des Internet neu. Sie nutzen Cybertechnologien aber gleichzeitig und parallel dazu verstärkt zur Umgehung konventioneller Kriegsführung. So etwa mittels global einsetzbarer, ferngesteuerter Drohnen und „Neurowarfare“, d.h. der Kriegsführung mittels direkter Verschaltung von menschlichem Nervengewebe mit Maschinen, die den sogenannten „super soldier“ zum Ziel hat und auf der Annahme beruht, dass das menschliche Bewusstsein: genauer, das Gehirn, „von Natur aus aggressiv“ sei und daher effektiver in der Reaktions- und Aktionsfähigkeit im Auseinandersetzungsfall sei. Diese These diskutierte unter anderem der jüngste Neurotechnologiebericht 2013 des Pentagon und der U.S. Army (Joint chiefs of staff) in einem White Paper, an dem ich mitarbeitete, kürzlich kritisch (D. de Euliis and H. Cabayan: Topics in the Neurobiology of Aggression: Implications for Deterrence. A Strategic Multi-Layer (SMA) Publication, The

Pentagon and U.S. Ministry of Defense, February 2013). Sowohl die US- wie die chinesische Militär-Forschungsbehörde arbeiten an der Direktverschaltung von Gehirn und Computer, um die Informationsverarbeitung einerseits zu vermenschlichen und daher „sicherer“ zu machen, andererseits zu beschleunigen.

Kriege auf virtueller Ebene: Werden Information und Einbildung eins?

Was wir angesichts dieser Entwicklung *nicht* tun sollten, ist zweierlei.

Erstens: Wir sollten nicht glauben, dass die Rede vom „Cyberwar“ Zukunftsmusik ist. Wir stehen längst im Cyberwar, sei es zwischen global operierenden Kriminellen und Gemeinwesen wie zwischen Regierungen, kombiniert mit dem raschen Aufstieg von Neurokriegsführung zum Kern künftiger Kriegsführung. Letztere ist zu einem der wichtigsten Investitionsthemen sowohl privater Firmen wie öffentlicher Institutionen geworden, auch wenn das Thema in der Diskussion noch nicht den Stellenwert hat, dem ihm faktisch bereits in den Mechanismen der Weltordnung zukommt.

In der „Neurowarfare“ wird die Frage der Information vielleicht am endgültigsten zur Frage der Einbildung: beide gehen ineinander über – zum Beispiel in der medial vermittelten und künftig über direkte Brain-Machine Interfaces (BMI's) gesteuerten Tötung von Menschen mittels Drohnen in tausenden Kilometern Entfernung, die von der neuen Berufsgruppe professioneller „Virtualkriegsmanager“ bedient werden. Diese Personen führen ein kleinbürgerliches Leben in einer Vorstadt, frühstücken am Morgen mit ihren Kindern, gehen zur

Arbeit, töten in den Bürozeiten mittels Drohnen Menschen meist auf anderen Kontinenten (obwohl sich das mit der US-Drohnenrichtlinie zum möglichen Einsatz im Mutterland bald ändern könnte), leisten anschließend die nötige Schreibtischarbeit zur Dokumentation und lassen den Abend dann mit ihrer Familie zuhause bei Abendessen und Fernsehen ausklingen. Die Imagination dieser „Verteidigungsfacharbeiter“, die keine Waffen mehr bedienen, sondern einen Bildschirm per Computerstick, ist einerseits völlig von ihrem Leben abgetrennt. Andererseits ist für sie Information und Einbildung zu exakt demselben geworden. Sie handeln in der Welt nicht aufgrund direkter, sondern ausschließlich medial vermittelter Wahrnehmung; und ihre Gedanken und Urteile sind – notgedrungen – eins mit den erhaltenen Informationen. Man kann die neuen Tötungsberufe per Mausklick also getrost als „eingebildete Berufe“, als „Einbildungsberufe“ oder, etwas zynischer, als „Fachberufe für die Arbeit mit Einbildungskraft“ (wobei das in das Reale „Eingebildete“ hier dann eben der Tod ist) bezeichnen. Obwohl es diese Berufe bereits gibt und sie ständig an Bedeutung zunehmen, steht zu bezweifeln, dass wir auf die damit entstehende neue Beziehung zwischen Information und Einbildung politisch, philosophisch, vor allem aber: menschlich vorbereitet sind.

Zweitens: Wir sollten nicht (mehr) glauben, dass eingebildete Gemeinschaften (imagined communities), Identitäten sowie die dazugehörigen Feindschaften und Vorurteile weiterhin weniger „real“ sind als „physische“. Erstere werden heute, im Zeitalter des „global imaginary“, das erstmals entsteht, wichtiger denn je. Das hat mit

der Rückkehr des Denkens in Kämpfen zwischen (imaginären) Kultur- und Zivilisationstypologien ebenso zu tun wie mit der rein virtuellen Hochstilisierung von „celebrities“ zu globalen Wiedererkennungsmarken. Es besteht wenig Zweifel daran, dass im Zeitalter des Aufstiegs der Einbildungskraft „die Eingebildeten“ in „natürlicher“ Weise zunehmen – ja zunehmen müssen. Die Folge: Kritik wird schwieriger. Wir sollten nicht wie bisher einseitig einzelne Mächte kritisieren, wie heute noch oft üblich. Eher geht es darum, einen Mechanismus ins Auge zu fassen, der Mächte und Menschen in neuer Weise zueinander in Beziehung setzt – wenn es denn überhaupt eine „Beziehung“ im bisherigen Sinn des Wortes ist.

Die Epoche des Futurperfekts: Zwischen Humanismus und Kommerzialisierung

Wenn diese – sicherlich unvollständigen und ergänzungsbedürftigen – Prämissen der Fall sind: Worin besteht dann – zumindest in wesentlichen Teilen – die Zukunft der Einbildung, vor allem: der Schnittstelle zwischen Wahrnehmung und Erscheinung, Objekt und Begriff, die sie darstellt? Mit anderen Worten: Was wird aus der Einbildung im Zeitalter der Informationssicherheit?

Der deutsche Sozialphilosoph Jürgen Habermas hat am Anfang des Jahrhunderts von der Gegenwart als einem Zeitalter der „neuen Unübersichtlichkeit“ gesprochen. Inzwischen sind wir aber offenbar weiter. Heute gilt in Wirklichkeit besser und wichtiger: Wir leben im Zeitalter der „neuen Informationsunsicherheit“. „Unsicherheit“ ist dabei gemeint für alle Dimensionen des Begriffs: Bezogen auf den *Gebrauch* von

Information durch verschiedene gesellschaftliche Akteure; die politische, ökonomische, soziale und kulturelle *Rolle* von Information; aber auch das *Wesen* von Information für das Menschliche und Unmenschliche. Nicht zuletzt: für ihre zunehmend zentrale Rolle für die Selbstbegriffe des Menschen und ihre Zukunftsprojektionen.

Zwischen Anwesenheit und Abwesenheit, Anfang und Ende, Agitation und Verschwinden werden die Grenzen brüchig. Die Umrisse verschwimmen; Abgrenzungen zwischen Vergangenheit, Gegenwart und Zukunft werden flüssig. Siehe den mittlerweile politisch-militärischen Vorreiter- und zugleich bereits kulturellen Ikonenstatus des Virus Flame. Dieser war so hoch komplex, dass er während seiner Angriffe bereits damit begann, sich zugleich selbst zu zerstören, um aus der Perspektive des Futurperfekts „nicht da gewesen zu sein“. Der Virus hatte nicht nur bestimmte Ziele (die Auslöschung der gesamten Sparte grundlegender Infrastruktur eines Landes), sondern gleichzeitig auch seine Selbstausschöpfung „genetisch eingebaut“ – was ihn einem Menschen nicht unähnlich, sondern im Gegenteil ähnlicher als alle seine Vorgänger macht. Nur dass es das „sterbliche“ Leben eines „Stellvertreter-Menschen“ ist.

Eine Lehre zumindest kann daraus sicher gezogen werden. Die Perspektive, der Zeitmodus des Futurperfekts wird die kommenden Jahre: die werdende Informationszivilisation immer stärker bestimmen. Inwiefern?

Das Futurperfekt ist aus meiner Sicht bereits grundsätzlich die interessanteste Zeitform. Vielleicht noch nicht in der Gegen-

wart, aber sicher in den kommenden Jahren wird sie auch zivilisatorisch immer wichtiger werden – auf Kosten aller anderen Zeitformen: Vergangenheit, Gegenwart und Zukunft eingeschlossen. Sie ist, wie Peter Handke einmal hervorhob, nicht nur die künstlerisch-literarischste, sondern auch die realistischste. Denn sie schwebt zwischen dem erwartungsvollen Erhabenen des Humanismus und dem Immer-schon-Gewesen-Sein des Pragmatismus, zwischen Streben und Einstimmung, Idealismus und Konkretisierung, einschließlich (wenigstens bis zu einem gewissen Grad) materialistische Kommerzialisierung. Wenn man in ihr die Dinge betrachtet, erscheinen sie in Feierlichkeit und Nüchternheit zugleich. Der Virus Flame war nur ein Ankündigungssymptom ihrer beginnenden globalen Herrschaft.

Mit der Macht eines Virus über ein ganzes Land ist aber auch eine weitere Dimension der Epoche der neuen Informationsunsicherheit beschrieben: die Grenzen zwischen klein und groß verschwinden. Es ist die Relation zwischen kleiner Ursache und riesigem Effekt, welche die Frage der Informations(un)sicherheit geradezu als Kernaspekt kennzeichnet – interessanterweise ebenso wie vorher die Fragen des Humanismus nach dem Willen und der Macht des Einzelmenschen und deren Verhältnis zu gemeinschaftlicher Moral.

Die humanistische Annahme war zumindest in individualitätsorientierten Zivilisationen wie den USA, dass der Einzelne alles entscheidet – letztlich auch das Schicksal der Gesellschaft, und dass von seinem Erfolg oder Scheitern, seinem Durchhalten oder Aufgeben das Schick-

sal ganzer Gesellschaften abhängt. Das zeigt jeder US-Blockbuster Film, in dem ein Held vorkommt: der Held setzt sich immer gegen Zweifel, gegen sich selbst und gegen „die anderen“ durch. In einer gewissen Analogie dazu hat in der globalisierten Informationskultur jedes kleinste Leck sofort riesige Folgen, weil das Kleinste in der Informationslogik immer mit dem Ganzen, dem Größten verbunden ist. Das ist eine einigermaßen neue Relation. War früher das Kleine klein und das Große groß, so werden im Rahmen der Informationszivilisation das Kleinste und das Größte eins. Sie werden aufgrund ihrer direkten und vollständigen Interdependenz ununterscheidbar.

Damit vollendet sich nicht nur der hermeneutische Zirkel, der zuerst (im 19. und 20. Jahrhundert) eine philosophische, dann (seit dem Beginn der Globalisierung) auch eine politische Tatsache beschrieb, nun bis hin zu seiner – wiederum doppel-sinnigen und tiefenambivalenten – „Aufhebung“ durch die technische Realität. Sondern es verschwinden auch die Logiken von Größenverhältnissen und Proportionen, an die wir gewohnt waren. Damit ist eine Verschiebung und mittelfristig Veränderung unserer Wahrnehmung, ja unseres gesamten Seins verbunden. Das Zusammenwachsen von Klein und Groß, das allmählich Proportionen ununterscheidbar macht, ist in gewisser Weise die technologische Entsprechung zur politischen und wirtschaftlichen Vernetzung, zur multipolaren Weltordnung mit überproportionaler Bedeutung kleiner Nationen und zum globalen Zusammenwachsen der Kulturen, letzteres nicht zuletzt wegen der Ersetzung von Kultur durch transnationale Technologie.

Das exponentielle Anwachsen der Online-Kriminalität, unter anderem mittels des Abbuchens von Kleinstbeträgen wie 50 Cent von 1 Million Konten, ist dazu die Analogie, vielleicht auch Karikatur auf kriminologischem Gebiet. Man merkt es nicht, aber der Gesamteffekt ist riesig. Das Kleine hat große Effekte. Wie die deutsche Kriminalstatistik im Mai 2013 berichtete, wuchsen Internet-Straftaten allein 2012 um 7,5%, zwischen 2007 und 2012 um 87%. Die meisten von ihnen hatten ihren Schwerpunkt eben am Überschneidungspunkt zwischen klein und groß.

Wie die US-Statistikbehörde im Februar 2013 berichtete, stiegen die Cyberattacken gegen die Informationsinfrastrukturen von US-Organisationen zwischen 2006 und 2012 um 782%. Darunter waren das Energieministerium, TD Bank, Wells Fargo, Apple, Facebook, Microsoft, aber auch wichtige Zeitungen wie die New York Times, das Wall Street Journal und die The Washington Post. Das Interesse der Angreifer galt vor allem dem Diebstahl geschützter Informationen aller Art, darunter Businesspläne, interne Strategien, Produktions- und Handelsgeheimnisse, Banktransfers und Kundendaten.

Dazu kommt die ebenfalls exponentiell steigende Zahl von Internet- und Handy-Mobbing, die zu einem der größten Probleme der Jugendkulturen avanciert ist. Wie das Kölner „Bündnis gegen Cybermobbing“ im Mai 2013 berichtete, sind ein Fünftel aller Schüler in Deutschland bereits einmal Opfer eines Mobbings mittels des Internet geworden, davon der größte Teil über soziale Netzwerke wie Facebook, etwa gleich viele gaben zu, mindestens einmal gemobbt zu haben. Das

Problem stellt vor allem deshalb einen „Kontinent der Finsternis“ dar, weil das meiste darüber unbekannt ist, da es nie an die Öffentlichkeit gelangt: Die angenommenen Dunkelziffern in diesem Bereich übertreffen alle vergangenen Rekorde und erreichen Jahr für Jahr neue Höchststände.

Business Cybersicherheit: Fragen zwischen öffentlich und privat

Im Gegenzug wird Informationssicherheit heute zu einem der größten Business-Zweige der Welt – nicht zuletzt wegen der zunehmenden Verlagerung breiter und zum Teil auch sensibler Speicherkapazitäten ins Internet beziehungsweise auf ausgelagerte kommerzielle Speicher, die per Internet zugänglich sind (Cloud-computing). In Asien, etwa in Südkorea, hält sich bereits jede mittlere bis größere Firma spezialisierte Abwehr-Teams, weil man sich der Nähe Chinas bewusst ist. Seoul betreibt wegen der Nähe zu Nordkorea eine große Abteilung der Armee, die – wie alle künftigen Armeen – als einen zentralen Bestandteil den Schnittpunkt zwischen Technisierung und Information bearbeitet.

Dazu kommt heute noch weitgehend unterbewertet die anthropologische Frage. Diese bewegt sich genau am Schnittpunkt zwischen öffentlich und privat und drückt sich auf *zweierlei* Weise aus.

Auf der einen Seite steigt Identitätsdiebstahl (Identity theft) stark an. Das Problem wird in den kommenden Jahren für die meisten westlichen Bürger schlimmer sein als internationale Angriffe und ökonomische Unsicherheiten, und in Zukunft zu einer wichtigeren Kulturfrage als die meisten anderen werden. Bedeutet das: Die Zukunft gehört der Informationssi-

cherheit des Einzelnen, nicht zwischen-nationaler Informationskanäle?

Auf der anderen Seite greifen invasive, das heißt in den menschlichen Körper eindringende Technologien im Zeitalter des „Transhumanismus“ um sich – und zwar zunächst vorrangig am neuen Schnittpunkt zwischen Mediatisierung, Körper und Gesundheit. Sinne werden ersetzt durch technische Geräte, die direkt mit dem Gehirn verbunden sind. Es ist bereits Standard, dass Radiowellen ein Kind, dessen Hörnerv funktioniert, mittels im Ohr implantierter Empfänger (Cochlea-Implantat) über unter der Haut eingesetzte Außenmikrophone hören lassen. Die Arbeit an entsprechenden Implantaten für Hörnerv-Geschädigte mittels direkter Anbindung an das Gehirn sind bereits weit fortgeschritten. Kamerabrillen mit Chipimplantat im Sehzentrum des Gehirns ermöglichen bereits seit Ende der 1990er Jahre sehähnliche Eindrücke. Man kann heute einen Rollstuhl mit Gedanken steuern, man kann das Licht mit Gedanken ein- und ausschalten, auch bereits auf größere Distanzen. Nach Erwartung der meisten Beobachter werden die kommenden Jahrzehnte die drahtlose Gedankensteuerung von Geräten mittels Gehirn-Computer-Direktschaltungen (Brain-Computer Interfaces, BCI's) zur weithin selbstverständlichen Praxis machen, so etwa die Kontrolle eines Hauses mittels Gedanken sogar von einem anderen Kontinent aus. Diese Entwicklung der „Kulturstreuung“ wird voraussichtlich von raschen Fortschritten in dringlichen Spezialanwendungsbereichen wie Prothetik und Gesundheit angesprochen.

Bei alledem zeichnet sich jedoch ein noch weitgehend unterschätztes zentrales Di-

lemma der Zukunft ab: Man kann wieder hören, wieder sehen – aber über den Umweg eines technischen Mediums. Ist es verlässlich? Was, wenn sich jemand genau am Übergang zwischen Wahrnehmung und Begriff, Sinn und Gedanke, Maschine und Gehirn einschaltet – also an den bereits heute meist immateriellen (kabellosen) Schnittpunkt zwischen „Einspeisung“ von Information und „Verarbeitung“ im Bewusstsein? Das ist im Prinzip nicht schwerer, als in die schwebewachte Information von US-Ministerien einzudringen oder die Daten von hunderttausenden Bankkunden oder Millionen Internetusern zu stehlen. Wer schaltet sich dazwischen: Ist es mein Freund – oder mein Feind? Und wenn letzteres der Fall sein sollte: Was bezweckt er? Vor allem: Was kann ich dann tun, da meine „Einbildung“ von manipulierten Information gespeist wird – was ich aber nicht wissen kann, da sie direkt in meinem Bewusstsein erscheinen?

Klar ist: Die Sicherheit des Übergangs wird, je weiter die neuen Humantechnologien fortschreiten, alles entscheidend – und zwar in anthropologisch viel tiefreichenderem Maß als bisher angenommen. Damit stellen sich nicht nur philosophische und praktische, sondern auch neue Legitimationsfragen: Wer kontrolliert den Übergang zwischen Sinneswahrnehmung und Bewusstseinsakt, also das, was von außen eingespeist innen ankommt? Wer ist von wem wie dazu befugt? Das ist die größere Dimension der Informationssicherheit heute. Wenn, wie in den kommenden Jahren notwendig, der Zusammenhang zwischen Wahrnehmung und Begriff, äußeren Datenmengen und innerer Verarbeitung neu geregelt wird – wer ist dann der Legislator? Eine Frage der Informationssicher-

heit im wörtlichsten Sinn der „Einbildungskraft“.

Philosophisch ist es die erneuerte Frage nach dem „Ursprung“ und der „Eigentlichkeit“, die damit verbunden ist. Was ist die „eigentliche“ Information, die ankommen soll, und wie kommt sie wirklich an? Zum Beispiel die Entscheidung eines Menschen zu sterben, die über Medien vermittelt werden muss, weil er nicht mehr in der Lage ist, sich anders zu äußern. Damit ist eine riesige Dimension der Informationsdimension beschrieben, die heute noch gar nicht wirklich in den Blick genommen ist. Und was, wenn „Humanforscher“, die selbst aktiv zu Cyborgs werden wollen wie Kevin Warwick von der Universität Reading, Recht damit haben, dass die Zukunft die Realisierung der Noosphäre durch die drahtlose Zusammenschaltung nicht mehr von Computer mit Gehirnen, sondern von Gehirnen mit Gehirnen ist? Gerade der Transhumanismus ist ohne Informationssicherheit nicht denkbar, und schon gar nicht realisierbar. Und der Begriff der „Einbildung“ spielt auch hier im vollen Spektrum seines Bedeutungsumfangs die zentrale Rolle.

Das sind grundlegende Fragen nicht nur aus Anwendungsperspektive, sondern auch grundlegend anthropologisch für die Zukunft der Menschheit. „Grundlegend“ im Sinn von: an der Basis liegend, an den Ursprung zurückreichend, aber eben auch: neuen Grund legend. Genau wie in der klassischen Philosophie. Überall spielt die Informationssicherheit in Zukunft die zentrale Rolle: Sogar für die Frage, welche Wesen wir sind, und wie wir uns selbst erfahren: Die Sicherheit der „Übertragung“ von Information von einem Ort zum an-

deren. Nicht zufällig ist die für die Informationssicherheit so zentrale Frage der „Übertragung“ auch ein Kernbegriff der Psychoanalyse.

Politische Avantgarde-Phänomene der globalisierten Virtualkultur: Fortschritt oder Rückschritt?

In einer *dritten* und letzten Dimension gilt Cyberkultur paradoxerweise – und im Widerspruch dazu – vielen heute aber auch als in ihren Grundcharakteristiken zumindest potentiell „postmaterialistische“ Kultur. Oder wie es die südkoreanische Mediensoziologin Ji-Young Kim geradezu euphorisch ausdrückt:

„Die entstehende Charakteristik der Cyberkultur... ist: dass sie im Prinzip postmaterialistisch ist. Denn sie fördert und unterstreicht Lebensqualität, Selbstrealisation und Teilhabe. Der Trend zu postmaterialistischen Werten ist eine Paradigmenverschiebung im Licht der Kommunikationseffekte hinsichtlich politischer Partizipation, weil sie Protestpolitiken von unten aufwertet. Eben aufgrund der hohen Konnektivität des Internet sind die gesellschaftlichen Implikationen der postmaterialistischen Cyberkultur bedeutsam. Vor allem legt sie eine strukturelle Beziehung zwischen Postmaterialismus, Cyberkultur und politischer Beteiligung nahe, indem sie den Fokus auf drei Faktoren legt, die das Internet mit postmaterialistischen Werteorientierungen verbinden: kognitive Mobilisierung durch steigende Bildungsniveaus, Informationsstreuung und politische Entscheidungsprozesse sowie die Entwicklung neuer sozialer Bewegungen.“ (Kim, Ji-Young: *Cyberculture of Postmaterialism and Political Participation*. In: *The Review of Korean Studies*, Vol. 10, No. 4, December 2007, pp. 291-320. Übersetzung aus dem Englischen: Roland Benedikter).

Ich halte dies zwar analytisch im Prinzip für richtig und einen Teil des in sich tiefenambivalent strukturierten Gesamtphänomens, begrifflich allerdings für ein Missverständnis, geboren vor dem spezifischen

Hintergrund der südkoreanischen Situation und Kultur, da hier der Begriff „post-materialistisch“ anders – und für den vorliegenden Kontext meines Erachtens sachfremd – gebraucht wird. Richtig wäre, im Zusammenhang der Cyberkultur nicht von „postmateriell“, sondern von „immateriell“ zu sprechen, wie dies bereits Jean-Francois Lyotard in seinen späten Werken vorgeschlagen hat. Die entsprechenden Impulse tragen sowohl einschließende wie ausschließende Perspektiven in sich, schon aufgrund der mit ihnen verbundene Fähigkeitsanforderungen, die den Bereich stark elitär färben. Ihr demokratiepolitisches Potential halte ich noch für keineswegs ausgemacht.

Das zeigt unter anderem die wachsende Ambivalenz der Sicherungsmechanismen. Die Zukunft von Einfluss und Herrschaft liegt in „soft power“, also in der Imagination bestimmter Ideale; und soft power ist ohne Informationssicherheit, auf der Freiheit beruht, nicht denkbar. Paradoxerweise wird daher Freiheit immer stärker an Sicherheit der Einbildung, also Kontrolle der Information angewiesen sein. Das könnte die Freiheit selbst untergraben – zumindest ihrem bisherigen Begriff nach. Ein Beispiel für die entsprechenden Widersprüchlichkeiten ist Wikileaks – von vielen als politisches Avantgardephänomen der Cyberkultur angesehen. Wikileaks benutzt das Internet, um geheime Informationen, darunter sicherheitsrelevante, meist des Westens global zugänglich zu machen. Der Anspruch ist, für „totale Transparenz“ zu sorgen und bisherige Machtpraktiken zu verunmöglichen. Die Hintergründe von Wikileaks liegen in den radikalpluralistischen und anarchistischen Bewegungen des Westens. Doch in Wikileaks hat der

Westen Informationsoffenheit zum Credo der Demokratie erhoben bis zu einem Punkt, an dem er sich selbst damit zu untergraben droht. Am ersten Tag der Veröffentlichung vertraulicher US-Depeschen durch Wikileaks im März 2011 setzte China mutmaßlich 600 professionelle Staats-hacker an, um das Material systematisch danach durchzusehen, ob sich daraus Vorteile für China gegen den Westen ergeben. Fazit: Zu große Informationsoffenheit, die zu Informationslecks führt, die auf Informationsunsicherheit beruhen, untergraben eben diese Informationsoffenheit. Zu viel Pluralismus unterminiert die pluralistische Gesellschaft und spielt ihren Feinden in die Hände. Zu viel Avantgarde droht, die Voraussetzungen dieser Avantgarde zu verunmöglichen.

Der Fall Wikileaks zeigt vielleicht mehr als andere: Informationssicherheit ist immer weniger nur ein rein technisches Problem, sondern der menschliche Faktor spielt eine zunehmend wichtige Rolle auf beiden Seiten: von Sicherern und Angreifern gleichermaßen. Wenn in der exponentiell professionalisierten und hochqualitativen technischen Informationssicherheitswelt die Sicherheit immer besser wird, wird der menschliche Faktor entscheidend – und es wird sich immer klarer zeigen, dass das ebenso Chance wie Problem ist.

Fazit: Was wissen wir? Was wissen wir nicht? Und: Womit sollen wir rechnen?

Der ehemalige US-Verteidigungsminister Donald Rumsfeld (1975-77 und 2001-06) war gewiss kein Verächter der Virtualisierung von Krieg noch der Abstraktion von Realität, sofern damit größtmögliche Vorteile und Effektivität für die westlichen

Leitmächte verbunden sind. Er unterschied in einem ebenso berühmten wie viel verspotteten, insgesamt aber weit unterschätzten Diktum kurz vor seinem Abgang vier analytische Kernfelder für die Zukunft strategischer Entscheidungen, die in jede Planung einzubeziehen sind: 1. Es gibt Dinge, von denen wir wissen, dass wir sie wissen. 2. Es gibt Dinge, von denen wir wissen, dass wir sie nicht wissen. 3. Es gibt Dinge, von denen wir nicht wissen, dass wir sie wissen. 4. Es gibt Dinge, von denen wir nicht wissen, dass wir sie nicht wissen.

Wenn man dazu Napoleons berühmten Ansatz nimmt, wie man überhaupt in die Zukunft hinein Entscheidungen antizipieren kann: Nur durch Kombination aller verfügbaren Informationen a) über Intentionen und b) Kapazitäten sowohl von Selbst wie von Anderem, dann gilt: Wenn es heute ein Gebiet gibt, auf dem Rumsfelds Punkte 2-4 gelten und auf dem uns der Großteil beider Dimensionen Napoleons unbekannt ist, dann ist es die Informationsfrage und die damit zusammenhängende Kulturfrage. Wir haben noch keine ausreichende „Einbildung“ davon, was vor sich geht.

Was wir aber mit Sicherheit wissen, ist dreierlei.

Erstens: Die Aussicht ist eindeutig. Die Bedeutung der Information wird quantitativ und qualitativ weiter wachsen, und sie wird ihren – bereits bisherigen – Status als einer der zentralen Bereiche globalisierter Zivilisation weiter ausbauen. Warum? Weil sich das Thema mit der universalen Vernetzung und Virtualisierung auf alle Kernbereiche, gesellschaftlichen Sub-

Systeme und typologischen Systemrationalitäten der entstehenden Weltgesellschaft ausdehnt. Wenn Bücher zunehmend nur mehr im Internet publiziert werden und die Wahrnehmung transnational technisiert wird, dehnt sich das Thema der Information und ihrer Sicherheit von den bisherigen kritischen Strategiebereichen Politik (Spionage, soft power) und Wirtschaft (know-how) auf die globale Kulturebene aus. Das wird umso mehr der Fall sein, als bisherige nationale Kulturen an Bedeutung abnehmen.

Zweitens: Mit der Virtualisierung kehrt die Frage der Information an ihren Ursprung zurück: informare = einbilden. Wenn die Welt unsere Sinne zunehmend über Medien, also technisch vermittelt unser Bewusstsein erreicht, dann wird mittels Information unsere Einbildung bestimmt, und zwar in beiden dabei im Spiel befindlichen Polen: Wahrnehmung und Begriff, Sinneseindruck und Gedanke. Am wichtigsten wird aber die Kontrolle ihrer Schnittstelle werden: der Ort, wo Wahrnehmung und Begriff, Sinneseindruck und Gedanke ineinander übergehen und sich verbinden – also jener Ort des menschlichen Bewusstseins, über den wir heute noch wenig wissen, und der mit die größten Forschungspotentiale bereithält. Genau an diesem Übergang findet Information statt – im wörtlichen Sinn von einbilden. Was wird eingebildet? Wahrnehmungsinhalte ins bewusste Denken. Wer kontrolliert den Übergang, an dem dies geschieht? Wer also kontrolliert die Einbildung? Wer ist dazu autorisiert und wer nicht? Wer will sich dazwischenschalten und den Schnittpunkt mitkontrollieren? Wie wird sich dabei der Daten-Begriff entwickeln? Das sind langfristig die wichti-

geren strategischen Fragen als die meisten militärischen, diplomatischen und politischen – jedenfalls in den Formen, wie wir sie heute kennen.

Drittens: Wenn sich das Thema weiterentwickelt, wird es zentral zu verstehen sein, dass weder die Kontrolle des einen noch des anderen Pols entscheidend sein wird: Weder die Kontrolle der Wahrnehmungs- oder Dateninformation noch der Art und Weise, wie Information bewusstseinsmäßig verarbeitet wird von ihren Empfängern. Sondern der entscheidende Punkt, um den in den kommenden Jahrzehnten zweifellos viele Auseinandersetzungen und Kämpfe sowohl in Worten wie in Taten geführt werden werden, ist der Kampf um die Schnittstelle zwischen Wahrnehmung und Begriff, Empfang und Verarbeitung – also um Information nicht als Datenmenge, sondern als Prozess der „Einbildung“.

Ausblick

Was wird die Zukunft bringen?

Versuche zum Umbau des Menschen zum Cyborg stehen ebenso unmittelbar bevor wie zur Expansion der Menschheit in das umgebende Weltall. Sie werden, unabhängig davon, welche Formen sie im Detail annehmen, das Leben der kommenden drei Generationen maßgeblich mitbestimmen: erstere nach innen, letztere nach außen. Aber auch Umbrüche in der Wirtschafts- und Finanzwelt sowie das Ende der bisherigen politischen Weltordnung mit dem Aufstieg Chinas und der Entstehung einer multipolaren Welt, die damit verbundene „Post-Empire“-Depression des Westens, der bereits erfolgte Beginn von Cyberkriegen sowie „humanpenetrative Mobilität“ an der Grenze zwischen Maschine und Bewusstsein prägen die Gegenwart. Mit

ihrem Aufstieg zu bestimmenden gesellschaftlichen Kräften ist ein neuer Weltanschauungskampf verbunden, der hinter den Kulissen politisch korrekter öffentlicher Rationalität längst im Gang ist: der zwischen einem schwächelnden, bereits weitgehend historisierten Humanismus und einem „Transhumanismus“, der – mit intellektuellem Hauptsitz am „Zukunft der Menschheit Institut“ der altherwürdigen Universität Oxford – mit allen Kräften aktiv über den bisherigen Menschen hinaus will. Mit diesen Entwicklungen tritt eine Fragenhäufung auf, die wenige Beispiele in der Geschichte der Moderne hat.

Obwohl Europa trotz jahrelanger Krisen bis heute eine der größten und vor allem sozial erfolgreichsten Wirtschaftszonen der Welt bleibt, braucht es nun nicht nur die Neubefragung seiner humanistischen Tradition, die bisher kaum erfolgt. Sondern es benötigt auch einen stärkeren Anschluss an globale Zukunftsthemen im Spannungsfeld zwischen Technologie, Intelligenz und Kultur. Denn deren Überschneidungspunkt nimmt an Bedeutung rapide zu. Cyberrealitäten, die nicht mehr nur auf Information beruhen, sondern aus ihr bestehen, bleiben als gelebte Kontextpolitiken keine Rand- oder Spezialthemen mehr, sondern steigen zu neuen Zentren des globalen Politischen auf.

Wir müssen auf diese neue Konstellation reagieren und künftig eine äußere und eine innere Dimension technologischer Veränderung des Humanen bei zumindest teilweiser gleichzeitiger menschlicher „Reinforcement“ der Technik unterscheiden. Diese kann – als Wechsel- und zumindest teilweise stark widersprüchliche Doppelbewegung – auf den sechs Feldern Wirt-

schaft, Politik, Kultur, Religion, Technologie und Demographie aufgewiesen werden. Sie verbindet sich auf ihnen zu einem großen Veränderungsvorgang. Weil in diesem Rahmen Information nach und nach zu ihrem Ursprung als „Einbildung“ zurückkehrt und diesen zugleich immer stärker in eine „transhumanistische“ Dimension hinein überschreitet, steht mit der Zukunft von Information und Informationssicherheit auch die Zukunft von Einbildung und Einbildungskraft zur Disposition. Es liegt (wie immer) an uns, was wir daraus machen.

Zum Autor

Roland Benedikter, geboren 1965, ist Europäischer Stiftungsprofessor für multidisziplinäre Politikanalyse und Politische Antizipation an der Universität von Kalifornien in Santa Barbara und Visiting Scholar an der Stanford University, Regierungsberater am Potomac Institute Washington DC und Trustee der Toynbee Prize Foundation Boston. Vorlesungen in Asien, USA und Europa, Mitarbeiter am Pentagon White Paper über die Militarisierung der Neurotechnologie, Publikationen in führenden Fachzeitschriften wie Foreign Affairs, The National Interest und Blätter für deutsche und internationale Politik, Kommentare in den Tageszeitungen Die Welt, Der Standard, Frankfurter Rundschau, Die Presse. Homepage: http://europe.stanford.edu/people/roland_benedikter. Kontakt: rben@stanford.edu.