sich interessant und gut lesbar – auch, weil Lemke es versteht, sowohl die aufgegriffenen Konzepte etwa der Biopolitik, Biosozialität und politischen Ökologie als auch konkrete Probleme wie das der genetischen Diskriminierung nicht nur luzid darzustellen, sondern zugleich einer systematischen und gut nachvollziehbaren Kritik zu unterziehen. Was freilich fehlt ist ein bilanzierender und weiterführender Schlussaufsatz, der auf der Grundlage der in den Aufsätzen ausgelegten Fährten die eingangs angemahnte Entwicklung eines dritten Weges der Integration von Gesellschaft und Natur jenseits naturalistischer und sozio-zentrischer Herangehensweisen genauer theoretisch-konzeptionell ausgearbeitet hätte. So bleibt es bei durchaus interessanten Puzzleteilen aus Konzepten, Problemen und Kritik, die auch am Schluss nicht zu einem Gesamtbild zusammengefügt werden.

« »

Der Verlust von Datensicherheit und Innovativität

Positionen etablierter Wissenschaftler im „Neuland“

***D. Klumpp, K. Lenk, G. Koch (Hg.)*: Überwiegend Neuland. Positionsbestimmungen der Wissenschaft zur Gestaltung der Informationsgesellschaft. Berlin: edition sigma 2014, 208 S., ISBN 978-3-8360-3599-6, Euro 17,90[1]**

von Arnd Weber, ITAS

Der Band hat einen ambitionierten Titel. Erstens bezieht er sich auf die deutsche Kanzlerin, die im Zusammenhang mit den Enthüllungen über die NSA-Abhöraktionen von „Neuland“ sprach (Spiegel Online 2013). Da die Autoren sich teilweise seit Jahrzehnten mit der Nutzung des Internets beschäftigen, bezieht sich die Erwähnung des Begriffs im Titel auf die verbreitete Kritik an dieser Charakterisierung. Gleichzeitig wollen die Autoren jedoch ausdrücken, dass noch viele Fragen der „Gestaltung der Informationsgesellschaft“ offen seien. Darauf lässt auch der Untertitel schließen: Der Band enthalte hierzu die „Positionsbestimmungen der Wissenschaft“, nicht mehr und nicht weniger. Der Verlag stellt auf der Rückseite des Buches klar, in diesem Buch gehe es darum, „Risiken ab(zu)wehren, wie sie … durch die NSA-Enthüllungen … deutlich wurden“. Insofern wird die Messlatte für die Bewertung der Gestaltungsvorschläge sehr hoch gelegt.

1 Schutz vor Unterminierung und Spionage?

Die Versprechungen, die der Titel und die Buchrückseite enthalten, beziehen sich auf Themen, die auch in der IT-bezogenen Politikberatung des Instituts für Technikfolgenabschätzung und Systemanalyse (ITAS) zentral sind. Was kann man z. B. gegen den „full take“ des Internets machen, den die NSA speichert? Was gegen die Unterminierung von Computern und Verschlüsselungssoftware („insert vulnerabilities into commercial … IT systems and communications devices“, so hieß es auf den Slides von Snowden)? Was kann man dagegen tun, dass die NSA verschlüsselte Informationen zur späteren Analyse aufhebt, also anscheinend in der Lage ist, sich Zugang zu den Schlüsseln oder zum Klartext zu verschaffen?

Dieter Klumpp ist Leiter der Alcatel-Stiftung. Er schreibt bezugnehmend auf diese Fragen in seinem Artikel, dass ein innovationsorientierter Datenschutz gut wäre (S. 200). Das ist einerseits eine Anforderung, die dem Vorwurf des Datenschutzes als Hindernis entgegenwirkt. Es bleibt aber unklar, wie ein besserer rechtlicher Datenschutz, selbst eine teilweise Vermeidung der Entstehung personenbezogener Daten, gegen die Unterminierung tendenziell aller Rechner und gegen den „full take“ helfen soll.[2] Und was meint der Ko-Herausgeber Klaus Lenk dazu? Lenk ist u. a. Vorstand des (deutschen) „Nationalen eGovernment Kompetenzzentrums“. Er schreibt in seinem Beitrag, dass wesentliche Teile der Informationstechnik der politischen Gestaltung durch Europäer entzogen seien (S. 204). Dem kann aus zwei Gründen nicht zugestimmt werden. Der eine ist, dass derzeit durchaus diskutiert wird, durch Regulierung ein höheres Niveau der Sicherheit der Endgeräte zu erzielen, so durch Gernot Heiser (2013), Sandro Gaycken (2014) oder auch durch den Autor dieser Rezension schon vor Bekanntwerden der Snowden-Enthüllungen (Weber/We-

ber 2010). Wenn die Endgeräte nicht unterminiert wären, ließen sich praktisch eine nicht brechbare Verschlüsselung und sogar anonyme Nutzungen erreichen. Unklar bleibt auch, wieso die Europäer nicht genauso wie das US-Verteidigungsministerium an eigenen, hochsicheren Computersystemen arbeiten können. So hat beispielsweise die US-amerikanische Behörde *Defense Advanced Research Projects Agency* (DARPA) ihr HACMS-Programm (High-Assurance Cyber Military Systems; ZDnet 2013), das u. a. an unangreifbaren Drohnen arbeitet. Ähnlich arbeitet die Universität Cambridge (UK) in ihrem „clean slate"-Programm am Neudesign von Computern (University of Cambridge 2014). Gäbe es in Deutschland und Europa keine Wege, solche Systeme für militärische oder zivile Einsätze zur Produktreife zu entwickeln und ihren Einsatz z. B. in kritischen Infrastrukturen vorzuschreiben?

Auch unterhalb der Ebene hochsicherer Hard- und Software haben die Europäer Gestaltungsmöglichkeiten, die die Autoren nicht erwähnen. Michael Waidner argumentiert, dass der Staat den Einsatz von Verschlüsselung fördern könne (Waidner 2014), was die Arbeit der NSA erschweren würde, da sie nicht alles entschlüsseln kann. Caspar Bowden (2013) argumentiert, dass in Europa eine Gesetzgebung helfen würde, wonach Daten europäischer Bürger nur bei europäischen Betreibern, die mit europäischem Personal und nach europäischem Recht arbeiten, verarbeitet werden dürfen. Dies würde den „full take" erschweren.

Zum anderen kann Lenks These des Mangels an Gestaltbarkeit auch deshalb nicht zugestimmt werden, da er den Verlust der europäischen Bestimmung der Informationstechnik unzureichend thematisiert. Bis etwa 2007 waren europäische Unternehmen im Mobilfunkbereich sogar dominant. Europäischen Investoren, Hersteller und Netzbetreiber hatten überwiegend auf eigene Techniken gesetzt, wie SMS und WAP (Weber et al. 2011). Diese waren gegenüber den Internettechniken schlechter, z. B. war praktisch keine Übermittlung von Links in Nachrichten möglich. In kartellartiger Form wurden letztere jedoch teuer vermarktet (1 MB per SMS hätte 1000 Euro gekostet; WAP wurde als „wait and pay" kritisiert; vgl. Weber et al. 2011). Ewan Sutherland warf den Mobilfunkbetreibern vor, Daten wie Wasser in der Wüste zu verkaufen (2005). Da die Kunden die europäischen Mobilfunkmarken zu Recht mit hohen Preisen und schlechter Qualität assoziierten, verkauften sich diese Dienste, von SMS abgesehen, kaum. Wie René Obermann, damals Chef von T-Mobile, sagte: „Die Qualität der Dienste ist nicht hoch genug" (2004 auf dem Petersberg). Dies wurde erst anders, als *Apple* das mobile Internet mit einer Flatrate und einwandfrei funktionierenden Geräten anbot.

Dass man in Europa die Trends zum Internet und zu Smartphones verschlafen habe (S. 182, 191), kann damit nicht unwidersprochen bleiben. Die europäischen Hersteller und Betreiber wussten von den Vorteilen der Internettechniken, wollten jedoch lieber ihre eigenen teuer verkaufen und boten Internettechniken ausschließlich zu noch höheren Kosten an. Dass man in der deutschen Wirtschaft generell nicht „big" denken könne (S. 191), kann angesichts der Erfolge der deutschen metallverarbeitenden Industrie auf dem Weltmarkt auch nicht behauptet werden. Auch Nokia dachte „big" mit dem Versuch, den Erfolg von SMS mit MMS, WAP etc. fortzuführen. Datendienste künstlich verteuert anzubieten, führte jedoch zu keinem dauerhaften Markterfolg. Bouwman (2014) nannte Nokia „arrogant" und „inkompetent" in Bezug auf die Anwendungen für *Symbian* und *Ovi*. Anbieter, die ihre Dienste auf der Basis des effizienten Internetprotokolls anboten, wischten schließlich die europäischen Handyhersteller beiseite.

In Bezug auf die NSA und die Bestimmung der Informationstechnik wäre es also wünschenswert gewesen, die internationalen Fachdiskussionen stärker aufzunehmen.

2 Schwerpunkt eGovernment

Die weiteren Beiträge des Buches behandeln im Wesentlichen die Gestaltbarkeit der IT-Nutzung, v. a. im Bereich eGovernment (in Bezug auf in Deutschland, mit einem Seitenblick auf Österreich).[3] Was sind hier die zentralen Aussagen? Zunächst wird ein Rückblick auf die Nutzung der Informationstechnik in der öffentlichen Verwaltung gegeben, und zwar in den Artikeln von Klaus Lenk und von Arthur Winter, letzterer ein

leitender Mitarbeiter des österreichischen Finanzministeriums. Einerseits wird festgestellt, dass der IT-Ansatz im öffentlichen Dienst letztlich dem Gemeinwohl dienen soll, so Lenk. Andererseits springt die Frage nach der Effizienz von eGovernment-Maßnahmen in Auge. Der Bürger tritt ja nur sehr selten in Kontakt mit Behörden. Gerhard Schwabe benennt in seinem Artikel das Beispiel wie „ich meinen Umzug abwickle" (S. 69). An anderer Stelle schrieb Klumpp, dass es „durchschnittlich drei Behörden-Interaktionen pro Jahr" gäbe (Klumpp 2013). Das zeigt, dass es schwierig ist, die Einführung von Chipkarten, elektronischen Ausweisen und ähnlichem zu rechtfertigen. Die Formulierung von Winter, wonach es „bis zu durchschnittlich 130 Verwaltungskontakte pro Jahr für ein Unternehmen" gäbe, wirft unmittelbar die Frage auf, wie viele Kontakte es denn nun im Schnitt sind. Die Effizienz von eGovernment wird aber nicht behandelt, obwohl sie durchaus auf dem Radarschirm internationaler Forschung ist (Misuraca et al. 2012).

Die Beiträge von Bernd Holznagel, Wolfram Felber und Jörn von Lucke geben einen Überblick über „open government" und „open data", d. h. die Zurverfügungstellung von Regierungsdaten an Bürger und Unternehmen. Hier steht offenbar noch der Klärungsprozess darüber aus, welche Daten angeboten werden sollen und welche Nutzung erlaubt werden soll. Günter Cyranek weist in seinem Artikel darauf hin, dass es in Südamerika Bestrebungen gibt, Bildungsmaterialien als „open content" zur Verfügung zu stellen. Zu den öffentlichen Daten gehören auch die Medienangebote der öffentlich-rechtlichen Anbieter, die bisher nur beschränkt Daten ins Internet stellen dürfen. Nach Volker Grassmuck sollte dies von den Bürgern in einem Gesellschaftsvertrag kontrolliert werden.

Helmut Krcmar und Petra Wolf sprechen sich in ihrem Beitrag für eine Zertifizierung der Anwender von Cloud-Diensten aus. Diese würde z. B. öffentlichen Auftraggebern ermöglichen, zu sehen, dass gewisse Sicherheitsvorgaben bestätigt wurden. Was dies nach Snowden bedeutet, was dies für US-Anbieter bedeutet, die US-Geheimgesetzen unterliegen, was dies bei der Existenz von Hintertüren bedeutet, ob verschlüsselte Daten durch US-Stellen im Klartext abgezogen werden können etc. wird von den Autoren leider nicht diskutiert, wurde aber durchaus in internationaler Forschung untersucht (Bowden 2013).

3 Probleme beim Netzausbau?

Einige Beiträge thematisieren die Entwicklung elektronischer Netze als Infrastrukturen. Im Artikel von Nico Grove werden Infrastrukturentscheidungen als schwer reversibel gekennzeichnet (S. 127), weshalb der Staat Investitionsstrategien festlegen müsse (S. 131). Groves Prämisse bleibt jedoch unbelegt. Funknetze können relativ leicht auf- und abgebaut werden (vgl. Shinohara et al. 2014). In Ländern mit oberirdischer Kabelverlegung können auch Festnetze relativ leicht ergänzt werden. Wie der Staat am besten wissen solle, welche IT-Infrastrukturen zukünftig nachgefragt werden, bleibt unklar. Thomas Hart weist in seinem Artikel darauf hin, dass es v. a. um den Konsum von Videos gehe. Ob der Staat hier so große Kapazitäten schaffen müsse, dass sie für ein Streaming reichen, bleibt dem Rezensenten unklar. Gleichwohl haben einige Länder große Glasfasernetze gelegt, wie Schweden oder Japan (Sandgren/Mölleryd 2013), worauf die Autoren aber nicht eingehen.

Im Artikel von Klumpp wird der weitere Ausbau der Netze mit Glasfaser thematisiert. Es fehlen jedoch klare Aussagen, ob dieser nötig ist. Andererseits findet sich die Aussage, dass die physikalischen Gesetze gelten würden (S. 187f.) – damit muss gemeint sein, dass die Erhöhung der Kapazitäten der Kupferkabel und der drahtlosen Netze zur Versorgung nicht ausreicht. Auch wird darauf hingewiesen, dass der Ausbau nicht mehr koste als die UTMS-Versteigerungserlöse erbracht hätten (S. 196). Diese Stellen lassen sich so interpretieren, dass ein Glasfaserausbau von Klumpp befürwortet wird. Ähnlich äußert sich Hart, dass der Netzausbau stocke (S. 134). Klumpp fordert in diesem Zusammenhang eine Abkehr vom wettbewerbsorientierten Partikularismus (S. 200). In Klumpp (2014) führt er aus, dass mehr Kollaboration und Kooperation nötig seien, weniger Wettbewerb. Man muss nun vermuten, dass es den Autoren darum geht, der *Deutschen Telekom* zu erlauben, zukünftige Glasfaserkabel nur relativ teuer an Wettbewerber zu vermieten (Sietmann 2010). Es wird der Eindruck erweckt,

für eine Informationsgesellschaft seien solche Investitionen notwendig. Es wird auch darauf hingewiesen, dass Europa immer noch führend bei Netzinfrastrukturen sei: „Europe is still the world leader“, wird Neelie Kroes zitiert (2014). Welche Bedeutung das hat, wo inzwischen ausländische Hersteller wie *Apple* und *Samsung* viel wertvoller sind als *Alcatel-Lucent* oder *Ericsson* und überhaupt der meiste drahtlose Verkehr über WiFi abgewickelt wird, bleibt undiskutiert. Die Autoren argumentieren aus einer Perspektive des Netzes. Wenn die Gesellschaft eine Informationsgesellschaft ist oder wird (kein Kapitalismus, keine Marktwirtschaft), dann müssen Investitionen ins Netz gut sein. Insgesamt wird im hier rezensierten Buch viel vom Netz und dem Internet als solchem und weniger von den Endgeräten und Diensten gesprochen. Dass man das Internet einfach auch als Kanal verstehen kann und es darauf ankommt, seine Enden zu sichern und attraktive Inhalte zu übermitteln, wird dabei übersehen, genauso wie die Möglichkeit, Kommunikation und eCommerce nach Belieben zu verschlüsseln und zu anonymisieren (Chaum 1981).

Insgesamt zeigt sich, dass die Autoren einen Überblick über die deutsche, politische, nichttechnische Diskussion von elektronischen Netzen, Geräten und Anwendungen geben. Wirklich „big“ wäre diese Rundumschau, wenn weltweit auf politische Debatten und technische Lösungsansätze geschaut würde. Dazu wäre in Deutschland ein kritischer Think-tank nötig, den es, unsere TA-Studien zu einzelnen IT-Themen belegen es (z. B. Rader/Weber 2002; Bohlin et al. 2004; Weber/Weber 2010; Jacobi et al. 2013), in ganz Europa nicht gibt.

Anmerkungen

1) Mit Beiträgen von Klaus Lenk, Arthur Winter, Jörn von Lucke, Bernd Holznagel, Wolfram Felber, Gerhard Schwabe, Volker Grassmuck, Wolfgang Coy, Thomas R. Köhler, Nico Grove, Thomas Hart, Günther Cyranek, Monika Ermert, Helmut Krcmar, Petra Wolf, Dieter Klumpp.
2) Der Beitrag von Klumpp entspricht in weiten Teilen seinem Diskussionsbeitrag auf einer Tagung in Österreich im Februar 2014, die er auf S. 181 erwähnt: http://www.domainpulse.at/de/programm (download 26.1.15).
3) Im vorliegenden Band werden auch noch andere Themen angesprochen, etwa autonome Fahrzeuge. Für eine vollständige Inhaltsübersicht siehe http://www.edition-sigma.de/InhaltPDF/Inhalt3599.pdf (download 26.1.15).

Literatur

Bohlin, E.; Lindmark, S.; Björkdahl, J. et al., 2004: The Future of Mobile Communications in the EU: Assessing the Potential of 4G. IPTS Technical Report prepared for the European Commission – Joint Research Centre. Seville; http://ftp.jrc.es/EURdoc/eur21192en.pdf (download 27.1.15)

Bowden, C., 2013: The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and Their Impact on EU Citizens' Fundamental Rights. Briefing Note. Brussels

Bouwman, H., 2014: Why Nokia Failed to Nail the Smartphone Market. Presentation given at ITS Brussels

Chaum, D., 1981: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: Communications of the ACM 24/2 (1981), S. 84–88

Gaycken, S., 2014: Resetting the System. New York; http://www.ewi.info/sites/default/files/Resetting%20the%20System.pdf (download 20.1.15)

Heiser, G., 2013: White Paper Protecting e-Government Against Attacks; http://www.itas.kit.edu/downloads/projekt/projekt_webe12_cosiso_heiser_paper.pdf (download 20.1.15)

Jacobi, A; Jensen, M.; Kool, L. et al., 2013: Security of eGovernment Systems. Conference Report; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Sec%20of%20eGovernment%20-%20Conference%20Report.pdf (download 20.1.15)

Klumpp, D., 2013: Neuartige offene IT-gestützte Formen der Zusammenarbeit beim Regierungs- und Verwaltungshandeln. 5. TICC Round Table Wissenschaft trifft Politik, Stuttgart, 24.1.13; http://www.instkomm.de/4-0-Publikationen.html (download 20.1.15)

Klumpp, D., 2014: Zum Strukturwandel der Wertschöpfung in der informatisierten Wirtschaft; http://www.instkomm.de/files/erp_dru_07.pdf (download 20.1.15)

Kroes, N., 2014: 5G for the Connected Continent. GSMA Mobile World Summit. Barcelona, February 24, 2014; http://europa.eu/rapid/press-release_SPEECH-14-155_en.htm (download 20.1.15)

Misuraca, G.; Savoldelli, A.; Codagnone, C., 2012: Explaining the eGovernment Paradox: An Analysis of Two Decades of Evidence from Scientific Literature

and Practice on Barriers to eGovernment. Presentation given at ICEGOV 2012. Albany

Rader, M.; Weber, A., 2002: Mobile Phones as Carriers of Cash and Tickets? The Outlook in Europe. In: IPTS Report May 2002, S. 43–49

Sandgren, P.; Mölleryd, B., 2013: How Liberalized is the Optical Fiber Broadband Market? Examining the Role of Public Money in the Fiber Deployment in Sweden. Paper presented at ITS Florence

Shinohara, S.; Morikawa, H.; Tsuji, M., 2014: Empirical Analysis of Mobile Broadband Adoption in Major Six Countries From The View of Competition Policy. Paper presented at ITS Rio de Janeiro

Sietmann, R., 2010: Next Generation Access. Das Endspiel: Warum Fiber-to-the-Home nicht vorankommt; c't 4 (2010). http://www.heise.de/ct/artikel/Next-Generation-Access-970831.html (download 20.1.15)

Spiegel Online, 2013: Die Kanzlerin entdeckt #Neuland. 19.6.13; http://www.spiegel.de/netzwelt/netzpolitik/kanzlerin-merkel-nennt-bei-obama-besuch-das-internet-neuland-a-906673.html (download 20.1.15)

Sutherland, E., 2005: Regulation of Cellular Markets; http://www.3wan.net/talks/2005/ES_2005_11_edinburgh.pdf (download 20.1.15)

University of Cambridge Computer Laboratory, 2014: CTSRD – Rethinking the Hardware-software Interface for Security; https://www.cl.cam.ac.uk/research/security/ctsrd/ (download 20.1.15)

Waidner, M., 2014: Stellungnahme zur Anhörung des NSA-Untersuchungssauschusses am 26. Juni 2014; http://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf (download 20.1.15)

Weber, A.; Weber, D., 2010: Options for Securing PCs Against Phishing and Espionage. A Report from the EU-project „Open Trusted Computing". In: Gutwirth, S.; Poullet, Y.; De Hert, P. et al. (Hg.): Computers, Privacy and Data Protection: An Element of Choice. Proceedings of CPDP 2010 Brussels. Berlin, S. 201–207; http://www.springerlink.com/content/t067038412352321/ (download 20.1.15)

Weber, A.; Haas, M.; Scuka, D., 2011: Mobile Service Innovation: A European Failure. In: Telecommunications Policy 35/5 (2011), S. 469–480

ZDnet, 2013: Research for Unhackable UAVs Could Be Used for BYOD: NICTA. May 28, 2013; http://www.zdnet.com/au/research-for-unhackable-uavs-could-be-used-for-byod-nicta-7000015937/ (download 20.1.15)

« »

Autorenhinweise

Wir bitten alle Autorinnen und Autoren, die ein Manuskript bei TATuP einreichen, die folgenden Hinweise zu beachten:

Umfang: Eine Druckseite umfasst max. 3.500 Zeichen (ohne Leerzeichen). Für den Umfang eines Beitrags ist die Rubrik, in der er erscheint, ausschlaggebend. Genauere Angaben erhalten die Autoren von der Redaktion.

Abstract: Autoren, deren Beiträge im Themenschwerpunkt des Heftes oder in den Rubriken TA-Konzepte und -Methoden und Diskussionsforum sowie TA-Projekte erscheinen, werden gebeten, ihrem Beitrag ein Abstract voranzustellen, in dem eine kurze inhaltliche Übersicht über den Beitrag gegeben wird. Die Länge dieses Abstracts sollte 780 Zeichen (ohne Leerzeichen) nicht überschreiten.

Abbildungen, Diagramme und Tabellen: Abbildungen und Tabellen sind sowohl in das eingereichte Manuskript einzufügen sowie auch getrennt von der ersten Fassung des Manuskripts einzusenden. Abbildungen und Tabellen bitte mit Überschrift und Quellenangabe versehen. Wurden sie vom Autor selbst erstellt, bitte die Formulierung „eigene Darstellung" als Quellenangabe verwenden *Zum Format*: Tabellen sind als *Word*-Datei, Diagramme in *Excel* und Abbildungen in *Adobe Illustrator* oder *Powerpoint* zu liefern. Sollten Sie lediglich andere Formate zur Verfügung haben, wenden Sie sich bitte frühzeitig an die Redaktion. Aus Gründen der Seitenplanung und des Layouts liegt die Entscheidung über die endgültige Größe und Platzierung der Abbildungen und Tabellen innerhalb des Beitrags bei der Redaktion.

Bibliografische Angaben: Die zitierte Literatur wird am Ende des Beitrags als Liste in alphabetischer Reihenfolge angegeben. Im Text selbst geschieht dies in runden Klammern (z. B. Wiegerling 2011); bei Zitaten ist die Seitenangabe hinzuzufügen (z. B. Fink/Weyer 2011, S. 91). Bei den Angaben in der Literaturliste orientieren Sie sich bitte an folgenden Beispielen:

Monografien: *Wiegerling, K.*, 2011: Philosophie intelligenter Welten. München

Bei Aufsätzen: Fink, R.D.; Weyer, J., 2011: Autonome Technik als Herausforderung der soziologischen Handlungstheorie. In: Zeitschrift für Soziologie 40/2 (2011), S. 91–111

Bei Beiträgen in Sammelbänden: *Mehler, A.*, 2010: Artifizielle Interaktivität. Eine semiotische Betrachtung. In: Sutter, T.; Mehler, A. (Hg.): Medienwandel als Wandel von Interaktionsformen. Heidelberg

Bei Internet-Quellen: Waterfield, J., 2006: From Corporation to Transnational Pluralism. London; http://www.plugin-tot.com (download 12.3.09)