Der für diese Retrospektive vorgesehene Artikel ist erst fünf Jahre alt, schaut also nicht allzu weit zurück, passt aber gut zum Schwerpunkt. Es handelt sich um eine Art Überblick zum Thema Cyberkrieg, der nichts von seiner Aktualität verloren hat, auch wenn in diesem Kontext inzwischen einiges passiert ist. So hat die Bundeswehr ein Cyberkommando gegründet. So ist das zweite Tallinn-Manual erschienen, in dem die völkerrechtliche Seite von Cyberkrieg aus NATO-Sicht vertieft wird. So hat es jüngst wohl Cyberangriffe der USA auf iranische Raketenabschussanlagen gegeben, was erneut vor Augen führt, dass Cyberkrieg nicht beim Hacken von Webseiten und Datenbeständen und dem Blockieren von Computern Halt macht, sondern auch technische Infrastrukturen zu den Angriffszielen gehören.

Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft

Cyberwar – Schimäre oder reale Bedrohung?

Im Rahmen des Kongresses „Quo vadis NATO? – Herausforderungen für Demokratie und Recht", der vom 24. bis 26. April 2013 in Bremen stattfand, hat der zweite Autor eine Arbeitsgruppe zum Thema „NATO, Cyberwar und das Recht" geleitet und dazu einen Einführungsvortrag gehalten. Der folgende Beitrag fasst den Vortrag zusammen. Er war ursprünglich für einen Kongressreader gedacht, der aber nicht realisiert wurde.

Der Begriff Cyberwar ist schwer zu fassen

Cyberkrieg (englisch: *Cyberwar* oder *Cyberwarfare*) ist ein schillernder Begriff, in dem die Bestandteile *Cyberspace* und *Krieg* verschmolzen sind und der kriegerische Auseinandersetzungen umfasst, die mit Mitteln der Informations- und Kommunikationstechnik (IKT) wie Computer, Softwaresysteme, Internet u. ä. geführt werden. Dabei macht es Sinn, von Cyberkrieg zu sprechen, wenn die Technik selbst Waffencharakter annimmt, im Gegensatz zu militärischen Systemen wie Raketen, Drohnen, Luftabwehr u. a., bei denen IKT-Systeme zentral an Steuerung und Funktion beteiligt sind, aber nicht das wesentliche Merkmal darstellen. Der früher ähnlich gebrauchte Begriff *Information War* trifft vielleicht etwas besser, worum es geht. Auch ist zu beachten, dass nicht jeder sogenannte Cyberangriff schon Cyberkrieg ist. So sind Straftaten mit IKT wie Online-Betrug, Phishing u. ä. der Cyberkriminalität zuzurechnen, politisch motivierte Aktionsformen des Online-Protests lassen sich unter dem Begriff Hacktivismus subsumieren. Bei Sabotage und Terroranschlägen mit Hilfe von IKT ist nicht immer eindeutig und klar, ob es sich um Straftaten handelt oder bereits kriegerische Akte vorliegen. Auch Cyberspionage, die im großen Maßstab stattfindet, ist in vielen Fällen eher wirtschaftlich als militärisch motiviert.

Wettrüsten für den Cyberkrieg

Dass es sich jedoch bei Cyberkrieg nicht um ein Hirngespinst handelt, lässt sich daraus entnehmen, dass eine Vielzahl von Staaten in den letzten Jahren eigene Cyberwar-Einheiten aufgebaut haben: Beispielsweise gibt es in den USA das *United States Cyber Command*, in Großbritannien die *Government Communication Headquarters*, in Israel die *Cyber Defense Taskforce* und in China die *Blaue Armee*, eine offiziell rein defensiv ausgerichtete Hackereinheit. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu besitzen. Russland wird verdächtigt, Cyberwarfare offensiv zu betreiben oder zu unterstützen. Insgesamt haben inzwischen rund 140 Staaten Cyberwareinheiten aufgebaut, wobei die meisten einen offensiven Charakter haben.[1]

Auch Deutschland steht nicht abseits. Seit Februar 2011 gibt es einen *Nationalen Cybersicherheitsrat*, der bei der Beauftragte der Bundesregierung für Informationstechnik angesiedelt ist und in dem das Kanzleramt, das Auswärtigen Amt, die Innen-, Verteidigungs-, Justiz-, Wirtschafts- und Finanzministerien des Bundes, die Bundesländer sowie assoziierte Mitglieder aus der Wirtschaft vertreten sind. Und seit April 2011 gibt es ein Nationales Cyberabwehrzentrum, an dem das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammenarbeiten, wobei als assoziierte Behörden das Bundeskriminalamt, der Bundesnachrichtendienst (BND), die Bundespolizei, die Bundeswehr sowie das Zollkriminalamt mitwirken. Im November 2012 wurde schließlich die *Allianz für Cybersicherheit* gegründet, in der sich das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITCOM) abstimmen. Daneben haben einige Bundesbehörden eigene Cybereinheiten. Die Strukturen sind allerdings ziemlich intransparent, und es bleibt unklar, wer diese Einrichtungen kontrolliert.

Cyberattacken sind alltäglich

Dass auf dem Feld des Cyberkriegs ein vehementes Wettrüsten stattfindet, ist auch an der Vielzahl von staatlich und militärisch motivierten und initiierten Cyberangriffen abzulesen. Öffentliche Aufmerksamkeit erregt haben beispielsweise der *Titan Rain*, eine Angriffsserie einer chinesischen Hackergruppe auf US-amerikanische Computersysteme von Rüstungskonzernen, Streitkräften, NASA u. a., und die *Olympic Games* mit dem Computerwurm *Stuxnet*, der der Störung des iranischen Atomprogramms diente. Bekannt geworden sind auch die Denial-of-Service-Attacken gegen estländische und georgische Regierungswebseiten, die wahrscheinlich von russischer Seite lahmgelegt wurden. Die Liste ließe sich noch um diverse Beispiele verlängern. In vielen Fällen ist allerdings nicht klar, was Ziel und Zweck ist und wer wirklich als Verursacher dahintersteckt. Spionage und Sabotage sind vielfach im Spiel, aber es kann sich auch um Provokation oder Warnung handeln. Es wäre in manchen Fällen durchaus denkbar, dass Cyberkriegseinheiten

solche Angriffe als Training durchführen. Auf jeden Fall zeigen diese Beispiele wie auch die jüngst bekannt gewordene massenhafte Ausspähung sozialer Netzwerke durch die US-amerikanische National Security Agency (NSA) mit Hilfe des Überwachungsprogramms PRISM, dass elektronische Medien und elektronisch gespeicherte Daten umfassend überwacht und ausgewertet und dass Industrieanlagen, Infrastruktursysteme wie Strom- und Wasserversorgung, Verwaltungseinrichtungen und das Bankwesen durch Cyberattacken vergleichsweise einfach gestört oder ausgeschaltet werden können.

Cyberkrieg scheint attraktiv

Mit der weltweit betriebenen Einrichtung von Cyberkriegseinheiten wird erheblich an der Rüstungsspirale gedreht. Das gilt als militärisch attraktiv, weil es relativ kostengünstig ist, so dass sich auch kleinere und ärmere Länder diese Art der Aufrüstung leisten können, und weil die Gefährdung eigener Soldaten geringer ist als bei herkömmlichen Formen des Krieges. Auch können Gegner durch das Ausschalten ziviler Infrastrukturen erheblich geschwächt werden. Außerdem ist eine Rückverfolgung von Angriffen schwierig, so dass die Aggressoren gar nicht immer sofort erkannt werden. Ein weiterer Umstand, der beachtet werden muss, liegt in dem Phänomen, dass es zumindest nach dem heutigen Stand der Technik wesentlich einfacher ist, Cyberangriffe durchzuführen, als sich gegen solche Attacken zu schützen. Gerade die hochentwickelten Industrieländer mit ihrem hohen Grad an Computerisierung und Vernetzung sind extrem verwundbar.[2]

Cyberkrieg tangiert zivile Freiheit

Die vielseitige Aufrüstung zum Cyberkrieg bedeutet aber nicht nur, dass zivile Einrichtungen erheblich gefährdet sind, sondern es gibt weitere Widersprüche zwischen zivilen Ansprüchen und militärischen Ambitionen. So gibt es eine Zuständigkeits- und Mittelkonkurrenz bei der Cybersicherheit zwischen Militär und Strafverfolgungsbehörden. So fehlen Energie und Geld, die in die Herstellung von Schadsoftware für Cyberangriffe fließen, beim Entwickeln von Schutzmechanismen. So werden Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoption geheim gehalten, statt sie aufzudecken und zum Schutz der eigenen Zivilgesellschaft zu beseitigen. Gleichzeitig wird dadurch Beihilfe zur Cyberkriminalität geleistet, weil weniger Schwachstellen beseitigt werden, als möglich wäre. Schließlich stehen die militärischen Ziele der Kontrolle, Überwachung und Fähigkeit zu Cyberangriffen im Widerspruch zum zivilen Anspruch auf freien Umgang mit digitalen Medien und Internet.

Cyberkrieg ist global, Cyberabwehr national

Während Angriffswerkzeuge für den Cyberkrieg teilweise im Internet zu finden und oft billiger zu haben sind als konventionelle Waffen, während ihre Handhabung vergleichsweise einfach erlernt werden kann, ist es um die Cyberabwehr – zumindest heute noch – schlecht bestellt. Ein wesentlicher Grund dafür ist, dass Bemühungen um Cybersicherheit überwiegend national organisiert sind, während der Cyberspace mit dem Internet und den Netzen internationaler Konzerne global funktioniert. Die Netze internationaler Firmen ignorieren staatliche Grenzen, die Liefer- und Wertschöpfungsketten sind weltumspannend, eine wachsende Menge relevanter Daten ist in einer „Public Cloud" gespeichert, und die Betreiber kritischer Infrastrukturen beschränken sich auch selten auf nationale Territorien. Nationale Cyberabwehr kann deshalb nicht oder nur sehr eingeschränkt funktionieren.

Cyberkrieg erhöht Kriegsgefahr

Ein besonders bedenklicher Aspekt der Aufrüstung zum Cyberkrieg ist, dass die allgemeine Kriegsgefahr und Kriegsbereitschaft dadurch steigen. Das Department of Defense der Vereinigten Staaten hat im Jahre 2011 die *Strategy for Operating in Cyberspace* herausgegeben, die von der defensiven Schwäche, der immensen Abhängigkeit von funktionierenden IKT-Systemen und die hohe Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung und Mobilität geleitet ist.[3] Statt jedoch eine weltweite Cyberabrüstung anzustreben, wird mit Gegenangriffen bei Cyberattacken gedroht. Dabei wird der Einsatz konventioneller Waffen nicht ausgeschlossen – im Gegenteil wird die Eintrittsschwelle sogar sehr niedrig gelegt. Der Begriff Cyberangriff wird sehr weit gefasst und reicht von Denial-of-Service-Attacken und Sabotage von militärischen und zivilen Systemen über die Manipulation und den Diebstahl von Informationen sowie Wirtschaftsspionage bis hin zu Diebstahl geistigen Eigentums. Hacktivismus, Cybercrime und Cyberwarefare werden undifferenziert als Bedrohung der nationalen Sicherheit der USA angesehen und können Gegenangriffe nach sich ziehen. Eine spannende Frage in diesem Zusammenhang ist, welche Auswirkungen das für den Bündnisfall in der NATO hat. Wenn die USA eine Cyberattacke mit Raketen beantworten, müssen sich dann die anderen NATO-Partner an die Seite der USA stellen?

Cyberkrieg im Lichte des Kriegsvölkerrechts

Cyberkriege sind wegen der weltweiten Aufrüstung und weitgehend fehlender Bemühungen um Cyberabrüstung eine reale Gefahr. Deshalb drängt sich die Frage auf, ob und wie das Kriegsvölkerrecht auf Cyberkriege anwendbar ist. Die Fachleute sind sich uneinig. Die einen argumentieren, dass Cyberkriege „reguläre" Kriege sind, so dass das Kriegsvölkerrecht uneingeschränkt gilt und angewendet werden kann. Ein wesentliches Problem wird in diesem Falle darin gesehen, dass der Aggressor bei Cyberattacken nicht immer feststeht und schwer ermittelbar sein kann. Die Gegenposition betont die Besonderheiten von Cyberkriegen, die im Kriegsvölkerrecht in der bisherigen Form nicht berücksichtigt sind, so dass eine Art digitaler Genfer Konvention nötig wäre. Wie Cyberkrieg im Völkerrecht reflektiert ist oder werden kann, muss dringend geklärt werden, wobei auch die Ächtung eine Option ist.[4] In diesem Zusammenhang ist vor allem auch das *Tallinn-Manual* von Bedeutung, das im Auftrag des *NATO Cooperative Cyber Defence Centre* mit Sitz in Tallinn von einem rund zwanzigköpfige Expertengremium von 2009 bis 2012 ausgearbeitet worden ist und das völkerrechtlich gebotene Verhalten von Staaten im Cyberkrieg zum Gegenstand hat.[5]

Cyberrüstung bedroht die Zivilgesellschaft

Durch die weitreichenden und hochentwickelten Möglichkeiten, Cyberangriffe durchzuführen, sind aber nicht nur militärische IKT-Systeme bedroht, sondern staatliche Einrichtungen, Unternehmen und die Bürgerinnen und Bürger insgesamt, wobei diese gezielt oder als Zufallstreffer und Kollateralschaden zu Opfern werden können. Die digitalisierte Gesellschaft als Ganzes ist hochgradig abhängig von kritischen Infrastrukturen wie der Energie- und Wasserversorgung, dem Transportwesen, den Informations- und Kommunikationskanälen und dem Gesundheitssystem. Fast alle dafür eingesetzten Computersysteme sind vernetzt und so von überall her erreichbar. Die kommerzielle Hard- und Software ist in der Regel leicht angreifbar. Die Standardisierung erleichtert und effektiviert Angriffe. Die Komponenten von IKT-Systemen kommen von vielen Herstellern und Lieferanten, so dass kaum kontrollierbar und nachvollziehbar ist, wie sicher sie sind. Mit der überdies wachsenden Komplexität der Systeme und Anwendungen wächst die Häufigkeit von Schwachstellen, Fehlkonfigurationen und unbekanntem Verhalten. Die Sicherheit von IKT-Systemen ist selten ein Designziel bei der Durchführung von Entwicklungsprojekten, der Profit steht im Vordergrund. Das Problem besteht darin, dass kritische Infrastrukturen mit dem Internet verbunden sind, dieselbe Hard- und Software, dieselben Protokolle und Dienste nutzen und dass dieselben Schwachstellen auftreten wie bei allen sonstigen Nutzerinnen und Nutzern der IKT-Technik. Zudem mangelt es den Betreibern von kritischen Infrastrukturen an Sensibilität für die Probleme. Auf der anderen Seite bergen die Versuche des Staates, die Angreifbarkeit der kritischen IKT-Systeme zu mindern, auch Gefahren und Risiken. So bedeutet eine Verschärfung von Sicherheitsgesetzen in der Regel, dass die Freiheit im Internet beeinträchtigt wird.

Cyberpeace statt Cyberwar

Der Gefahr von Cyberkrieg lässt sich nur durch eine konsequente Cyberabrüstung und durch eine Konzeption des Cyberpeace begegnen.

Auf der militärischen Ebene heißt das, Offensivwaffen für den Cyberkrieg zu verbieten und Cybersicherheit rein defensiv auszurichten. Im Sinne einer digitalen Genfer Konvention sollte ebenfalls verboten sein, Cyberangriffe auf kritische Infrastrukturen zu unternehmen. Wirtschaftliche Interessen müssen als legitimer Cyberkriegsgrund ausgeschlossen werden, ebenfalls dürfen ziviler Ungehorsam und Onlineprotest im Internet nicht dafür herhalten. Schließlich sollte es verboten sein, Cyberattacken mit dem Einsatz konventioneller Waffen zu beantworten. Außerdem sollte eine internationale unabhängige Instanz geschaffen werden, die behauptete Cyberangriffe forensisch untersucht, so dass eine verlässliche Zuordnung zu den Verursachern stattfindet und nicht die Falschen als Aggressoren beschuldigt werden können.

Auf der zivilen und politischen Ebene müssten alle staatlichen Stellen, alle Unternehmen und alle Bürgerinnen und Bürger verpflichtet werden, Schwachstellen in IKT-Systemen offenzulegen. Der Betriebserlaubnis kritischer Infrastrukturen müsste immer eine kompetente und transparente Sicherheitsprüfung vorausgehen, die Betreiber müssten die Sicherheit der IKT-Systeme garantieren. Die kritischen Infrastrukturen sollten dezentral und unvernetzt betrieben werden. Wichtig wäre auch, Cybersicherheitsstrategien unter demokratische Kontrolle und unter einen Parlamentsvorbehalt zu stellen. Speziell für Deutschland gilt, dass der Aufbau von Cyberabwehrzentren transparent und demokratisch kontrolliert vollzogen wird, dass die Zentren friedenspolitisch ausgerichtet werden und in ihnen eine strikte Trennung von Polizei, Geheimdiensten und Militär gewahrt wird. Als Unterstützung von Cyberpeace-Initiativen sollte die Bundesregierung die Friedensforschung zur Entwicklung von Strategien zur Befriedung des Cyberspace ausreichend fördern.

Statt eines Schlusses

Die Überlegungen in diesem Beitrag fassen nicht nur das entsprechende Referat des zweiten Autors auf dem Kongress *Quo vadis NATO?* zusammen, sondern sie sind auch stark angelehnt an den Vortrag der ersten Autorin über *Cyberpeace statt Cyber-*

Sylvia Johnigk, Kai Nothdurft und Hans-Jörg Kreowski

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.

Kai Nothdurft arbeitet als Information Security Officer in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung

war auf dem 29. Chaos Communication Congress 2012 (29C3) in Hamburg und folgen teilweise Ausführungen von Sylvia Johnigk und Kai Nothdurft in der FIfF-Kommunikation 1/2012.[6] Auch wenn das Thema Cyberwar nicht zuletzt wegen der immensen weltweiten Cyberaufrüstungen in letzter Zeit große öffentliche Aufmerksamkeit erregt, zeichnet sich die Problematik schon lange ab, wie der Artikel von Ute Berhardt und Ingo Ruhmann im Tagungsband der FIfF-Jahrestagung 1994 beweist.[7]

Dennoch stehen die kritische Auseinandersetzung mit dem Thema Cyberwar und die Entwicklung einer Gegenkonzeption unter dem Motto Cyberpeace noch ganz am Anfang. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) organisiert einen Arbeitskreis RUIN (RUestung und Informatik), der sich intensiv mit diesen Fragen beschäftigt. Wer interessiert ist, über die Aktivitäten des AK RUIN informiert zu werden oder mitarbeiten möchte, wende sich bitte an den zweiten Autor (siehe auch die Webseite fiff.de/themen/ruin). Darüber hinaus hat das FIfF gerade die Kampagne *Cyberpeace* gestartet, die durch die *stiftung bridge* gefördert wird. Sie hat zum Ziel, das öffentliche Bewusstsein von der gefährlichen Durchdringung des virtuellen Raumes mit militärischen Aktivitäten zu schärfen und den Widerstand dagegen zu stärken (siehe auch *http://cyberpeace.fiff.de/*).

Anmerkungen

1 *Sandro Gaycken: re:publica XI April 2011 http://re-publica.de/11/blog/panel/cyberwar-und-seine-folgen-für-die-informationsgesellschaft/*

2 *Der Cyberkrieg kann jeden treffen http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.146684 und Wirtschaftswoche: Bundeswehr anfällig für Cyber-Angriffe http://www.wiwo.de/technologie/digitale-welt/bundeswehr-bundeswehr-anfaellig-fuer-cyber-angriffe/7220 974.html*

3 *US Militärdoktrin des DoD: Strategy for Operating in Cyberspace http://www.defense.gov/news/d20110714cyber.*

4 *Spiegel Online: Der Wurm als Waffe http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html, Ein Gegenschlag ist nicht legal http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089 und Cyberwar: Die UN führen erste Gespräche über eine völkerrechtliche Ächtung http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089*

5 *Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013*

6 *Sylvia Johnigk und Kai Nothdurft: Cyberwarfare – Aufrüstung im Cyberspace als Herausforderung für die Friedensarbeit des FIfF, FIfF-Kommunikation 1/2012, S. 41–45*

7 *Ute Bernhardt und Ingo Ruhmann: Information als Waffe: Netwar und Cyberwar – Kriegsformen der Zukunft, in: Hans-Jörg Kreowski et al. (Hrsg): Realität und Utopien der Informatik, agenda-Verlag Münster 1995, S. 104–119*

Lesen & Sehen

Neues für Bücherwürmer & Cineasten

Rosemarie Will und Sven Lüders für die Redaktion der vor*gänge*

Meinungsfreiheit in Zeiten der Internetkommunikation

Editorial zu vor*gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik – Nummer #225/226

Unser Grundgesetz kennt eigentlich keine Hierarchie der Grundrechte. In ihm stehen die freie Rede wie der Schutz der Vertraulichkeit, die Religionsfreiheit und die Gleichberechtigung sowie viele andere Werte nebeneinander. [illegible] werten kommt der Meinungsäu[illegible] gende Bedeutung zu, sie ist me[illegible] ter den anderen. So betont auch [illegible] in seinen Entscheidungen immer wieder, dass die Meinungsäußerungsfreiheit für die Freiheit und die Demokratie schlechthin konstitutiv sei.

Wo und wie sich diese Freiheit jeweils verwirklichen kann, welchen potenziellen Einschränkungen und Gefährdungen sie ausgesetzt ist, unterliegt wie bei allen Grundrechten dem gesellschaftlichen Wandel – sowohl der Wertevorstellungen, Normen und politischen Gegebenheiten, aber auch ihrer technischen Bedingungen. Mit der zunehmenden Verlagerung der öffentlichen Kommunikation in den digitalen Raum stellen sich daher auch für die Meinungsfreiheit neue Fragen: Was bedeutet es, wenn Kommunikation die Flüchtigkeit des gesprochenen Wortes verliert und immer mehr digitale Spuren hinterlässt? Wie sollen wir mit der [illegible] wie lebensweltlichen Abschot[illegible] mit *Hate Speech* und *Fake News* [illegible] beeinflussen Netzwerke und ihre [illegible] Wahrnehmung und Kommunikationsbeziehungen? Mit diesen Fragen digitalisierter Kommunikation befasst sich die vorliegende Ausgabe der vorgänge. Unsere AutorInnen suchen bürgerrechtliche Antworten darauf, welche Chancen und Gefahren sich für die Meinungsfreiheit unter den Bedingungen digitaler, vernetzter Kommunikation ergeben.

Den Schwerpunkt eröffnet Patrick Donges mit einem Beitrag, der die Entwicklung der Internetkommunikation bis zur Entstehung von Social Media kommunikationswissenschaftlich einordnet. Donges macht drei Faktoren aus, die die Kommunikation und die medialen Inhalte im Netz heute prägen: Digitalisierung,

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de