Published in Zeitschrift für Außen- und Sicherheitspolitik (ZfAS) 2/2016
https://link.springer.com/article/10.1007/s12399-016-0557-1

Was macht Cyber? Epistemologie und Funktionslogik von Cyber

Ben Wagner . Kilian Vieth

Zusammenfassung Dieser Artikel untersucht die Funktionslogik des Begriffs Cyber im Spannungsfeld von Macht und Raum. Ausgehend von einer Begriffsherleitung der Wörter Cyber und Cyberspace wird die Verknüpfung von Cyber und Sicherheit in zwei Stufen aufgezeigt. Wir argumentieren, dass durch die fortgeschrittenen Versicherheitlichung des Wortes mittlerweile ein Prozess der *Cyberfizierung* an Stelle von Versicherheitlichung beobachtet werden kann. Wir sprechen uns daher für eine Erforschung von Cyber als Praxis aus, um seine praktischen Bedeutungen und Auswirkungen besser zu verstehen. Abschließend fassen wir die sprachlichen, institutionellen und praktischen Überlegungen zu Cyber in fünf Funktionen zusammen, die als Grundlage für weitere Analysen dienen können.

Schlüsselwörter Cyber . Versicherheitlichung . Epistemologie . Praxis . *Cyberifizierung*

What does Cyber do? Epistemology and Functional Logic of Cyber

Abstract This article studies the logic of operation of Cyber in the area of power and space. Based on a short explanation of the origins of cyber and cyberspace, we show in what ways cyber and security are connected. We analyse that due to the advanced securitisation of the word cyber, we can today witness a process of *cyberfication* that functions as securitisation. Therefore, we advocate a shift of research towards the practices of cyber, in order to better understand its significance and effects. In conclusion, the linguistic, institutional and practical considerations about cyber are summarised in five functions which could serve as a foundation for further analyses of cyber.

Keywords Cyber . Securitization . Epistemology . Practice . *Cyberfication*

Dr. B. Wagner
bwagner@europa-uni.de

K. Vieth
kilian@cihr.eu

Centre for Internet & Human Rights, Europa-Universität Viadrina
Große Scharrnstraße 59, 15230 Frankfurt (Oder), Deutschland

1 Einleitung: Was macht Cyber?

Das *Cyber* ist ein seltsames Gewächs. Scheinbar ohne Materialität irrt es durch den sprachlichen Raum der Begriffe über vernetzte Kommunikationstechnologie und wird dabei begleitet von ständigen Machtkämpfen. Da die Deutung von Räumen immer auch eine Machtfrage ist, sollte dies nicht verwunderlich sein. Es stellt sich allerdings die Frage nach der genauen Verortung von Machtgefügen (Ellrich 2002). Da es trotz dieser vielen Fragen ausgesprochen wird, stellen wir eine weitere: Was macht *Cyber*?

Der folgende Artikel ist auf den Spuren eines omnipräsenten Begriffs der sehr vielfältig und oft sehr vage genutzt wird. Cyber, um dessen Verortung im Kontext von Debatten über technisch-übertragene Räume etwas präziser zu fassen. Dabei soll zunächst die Geschichte des Begriffs geklärt werden. Auf dieser Grundlage wird dann der Prozess Versicherheitlichung zunächst anhand des Begriffs selbst und später über die Verwendung des Begriffs deutlich gemacht. Schließlich wird Cyber auch als Praktik verstanden und die Frage danach gestellt, wie Menschen agieren, wenn sie Cyber machen. Schließlich wird ein Fazit aus den sprachlichen, institutionellen und praxisorientierten Erwägungen gezogen, um Cyber als Gesamtkonzept besser zu verstehen.

2 Cyber und Cyberspace: Ursprünge einer Utopie

Die Ursprünge des Wortes Cyber liegen lang vor der Erfindung des Internets. Die Wortschöpfung wird oftmals William Gibson zugeschrieben, der in seinem Roman *Neuromancer* von 1984 den Begriff Cyberspace verwendete. Cyber und Cyberraum sind jedoch keine gleichzusetzenden Worte und haben unterschiedliche Bedeutungsentwicklungen erfahren. Das Wort Cyber wird bereits wesentlich früher verwendet und bezieht sich auf den Begriff der Kybernetik, der aus dem englischen *cybernetics* entlehnt wurde. Kybernetik beschreibt die Kommunikation zwischen Mensch und Maschine. Norbert Wiener gilt als Begründer der Kybernetik als Wissenschaft, die sich mit der Steuerung und Regelung dynamischer Systeme befasst.

Die Benutzung des Wortes Cyber weitete sich jedoch schnell in andere Bereiche aus. Im Zuge dieser Ausdehnung des Begriffes wurde Cyber zunehmend eine emanzipatorische Bedeutung zugeschrieben. Cyber konnte Grenzen überwinden, es wurde mit Freiheit von Zwängen und dem Aufbrechen von Einengung assoziiert. Ähnliche Eigenschaften finden sich auch in moderneren Debatten über den Cyberraum, mit dem bis heute Utopien einer herrschaftsfreien Welt verbunden werden.

Die Verbindung von Personen und Daten über Computernetzwerke wurde häufig als Raum wahrgenommen und beschrieben. Insbesondere in den frühen Jahren des Internets waren maritime Metaphern, etwas das *Surfen* im Internet, sehr beliebt, um die Beziehung zu und Interaktion mit Computern und ihren Netzwerken greifbar zu machen. Der Cyberspace wurde damit eine scheinbar endlose Weite unterstellt, ein neuer Raum, in dem es bislang Unbekanntes zu entdecken gibt (vgl. Ellrich 2002). Von John Perry Barlows (1996) Unabhängigkeitserklärung im Cyberspace bis zum MCI Kultvideo von 1997 (Lipshin o. J.), in dem die Gleichberechtigung aller Menschen durch das Internet beschworen wurde: Der Cyberraum symbolisierte die Utopie einer besseren Welt.
Seit dem Jahr 2000 zeichnet sich jedoch ein Wandel in der Verwendung und Bedeutung des Wortes Cyber ab. Anstatt um Cyberpunk und Hacker-Utopien geht es vor allem um eines: Sicherheit. In zunehmendem Maße wird Cyber zu einer Metapher für Bedrohungsszenarien und notwendige Militarisierung.[1]

Indes verschwindet die Verwendung des Begriffs Cyberraum immer weiter aus dem alltäglichen Sprachgebrauch. Die Metapher eines freien, post-territorialen Raumes, der abgekoppelt von der Offline-Welt existiert, scheint nicht mehr zu verfangen. Die künstliche Abtrennung des Cyberraumes als separater, virtueller Raum gelingt vielleicht schon deshalb immer schlechter, weil On- und Offline-Welt im Zuge technologischer Innovation immer stärker verschmelzen. Wenn wir rund um die Uhr ein Smartphone bei uns tragen, das Internet aus fast allen Arbeitsabläufen nicht mehr wegzudenken ist und auch große Teile der Freizeitgestaltung online stattfinden, dann wird digitale Kommunikation nicht mehr als getrennter Raum erfahren. Cyberraum und *reale* Welt standen dabei nie notwendigerweise in einem Abgrenzungsverhältnis. Die konstruierte Konkurrenz beider Räume hat es nie gegeben, die Unterscheidung von virtuell und real ist eher eine gesellschaftliche Konvention, keine aus Strukturen ableitbare Gegebenheit. Wir springen nicht von einem Raum in den anderen, vielmehr wird zwischen Internet und Mensch neue soziale Realität produziert (Ahrens 2003; Löw et al. 2008, S. 81). Hierzu hat Mark Graham ausgeführt:

> Such imaginations of 'cyberspace' all claim an aspatiality for the collective hallucination of Internet: a disembodied place, but a place nonetheless, paradoxically imbued with another type of spatiality allowing for a global coming-together of humanity. They give their

[1] Für eine Übersicht der Begriffe *cyberspace* und *cyber* siehe:
https://books.google.com/ngrams/interactive_chart?content=cyber%2Ccyberspace&case_insensitive=on&year_start=1948&year_end=2008&corpus=15&smoothing=3&share=&direct_url=t4%3B%2Ccyber%3B%2Cc0%3B%2Cs0%3B%3Bcyber%3B%2Cc0%3B%3BCyber%3B%2Cc0%3B%3BCYBER%3B%2Cc0%3B.t4%3B%2Ccyberspace%3B%2Cc0%3B%2Cs0%3B%3Bcyberspace%3B%2Cc0%3B%3BCyberspace%3B%2Cc0%3B%3BCYBERSPACE%3B%2Cc0

> imagined ‘cyber-’ space an ontic role. It becomes a fixed and singular, but also an ethereal and ubiquitous alternate dimension. (Graham 2013, S. 179)

Das Internet war nie ein grenzenloser Raum, der alle geographischen und sozialen Gräben zwischen den Menschen überwindet. „Die durch sie erzeugten virtuellen Räume substituieren jedoch nicht die Alltagswelt [...], sondern die moderne Gesellschaft ist durch eine *Konvergenz* realweltlicher und virtueller Räume gekennzeichnet“ (Löw et al. 2008, S. 81). Eine aktivistische Medienplattform formuliert dies in Anlehnung an George Orwell sogar etwas drastischer: „terms like [...] cyperspace are newspeak, they confuse the truth. There is no cybersphere, there is only life here“ (thejuicemedia 2015). Selbst Barlows Freiheitsmanifest hat mit dem Versuch, den Cyberraum für unabhängig zu erklären, selbst eine neue Grenzziehung vorgenommen. Vor allem aber hat die Metapher des Cyberspace dafür gesorgt, dass die Infrastruktur des Internets lange Zeit aus vielen Analysen ausgeklammert wurde, obwohl die technischen Strukturen vielfältigen rechtlichen und politischen Einflüssen unterliegen.

3 Raum der (Un-)Sicherheit: Versicherheitlichung eines Begriffs

Das Konzept Cyber hat sich weiterentwickelt, allerdings nicht in der Art und Weise wie es die utopisch-emanzipatorischen Ursprünge des Begriffs vermuten lassen. Die freiheitlichen Ideale sind zwar weiterhin vorhanden, stehen aber vermehrt in einem militärischen, anstatt einem zivilen Kontext. Der Cyberraum wird gerade wegen seiner anarchistischen VordenkerInnen als eine neue Sphäre der (Un-)Sicherheit gesehen, in der Staaten Ordnung herstellen müssen (Scott 1998). Da die Digitalisierung mittlerweile alle Gesellschaftsbereiche erfasst hat, wird Cyber zum *signifier* für eine diffuse, ubiquitäre Bedrohungslage:

> Den übergreifenden Nenner bildet die Allgegenwart der Vernetzung, die eine allgemeine Verletzlichkeit gesellschaftlicher Strukturen wie des Individuums begründen und damit die Betroffenheit eines jeden plausibel machen soll. Handlungsdruck wird erzeugt und das Diffuse der Gefahr trägt zu deren Potenzierung bei. (Thiel 2012, S. 64)

Der Cyber-Begriff weitet den Sicherheitsbegriff damit deutlich aus. Aus konkreter IT-Sicherheit eines bestimmten Systems wird die Sicherheit einer ganzen Gesellschaft über digitale Kanäle. Christopher Daase (2009) vertritt eine Erweiterung des Sicherheitsbegriffs in der Sach-, Raum-,

Gefahren- und Referenzdimension. Für die Versicherheitlichung des Cyberspace kommt natürlich zuerst die erweiterte Raumdimension in Betracht. Ein imaginierter neuer Raum wird von Sicherheitsakteuren erschlossen. Eine Trennung von äußerer und innerer Sicherheit ist nicht möglich. Cyber macht aber auch neue Vektoren in den anderen Dimensionen auf; insgesamt dient Cyber als gutes Beispiel für eine Erweiterung und Vertiefung des Sicherheitsbegriffs insgesamt. Allerdings darf eine Analyse des Begriffs nicht bei der reinen Beobachtung der Ausdehnung des Sicherheitsbegriffs stehen bleiben, sondern muss auch die Ursachen dahinter und die sozialen und politischen Auswirkungen analysieren.

4 Versicherheitlichung als *Cyberfizierung*

Durch die starke Verknüpfung von Cyber mit Sicherheit, zeichnet sich eine weitere diskursive Veränderung ab, die der *Cyberfizierung*. Der Begriff Informationssicherheit wird zunehmend durch Cybersicherheit ersetzt. Sowohl Einzelpersonen, als auch die Gesellschaft als Ganzes sind Gefahren aus dem Cyberspace ausgesetzt, die das traditionelle Konzept von Sicherheit erweitern (Daase 2009). Anstatt konkreten Bedrohungen entgegenzuwirken, geht es um Risiken, die aus der Interaktion mit dem Cyberraum entstehen. Cyber dient dabei als Container-Begriff, dessen Beliebtheit in seiner Unschärfe und Flexibilität begründet liegt. Die *Strategische Leitlinie Cyber-Verteidigung* des Bundesverteidigungsministeriums vom April 2015 schreibt etwa über den Cyberraum:

> Die Cyber-Sicherheitsstrategie für Deutschland definiert den Cyber-Raum als virtuellen Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. (BMVg 2015)

Die Leitlinie beschreibt den Cyberraum als einen neuen *Operationsraum,* der gleichberechtigt neben den klassischen Betätigungsfeldern der Bundeswehr zu Lande, zu Wasser, in der Luft und im Weltraum existiert. Warum wird der Begriff der Cybersicherheit den wesentlich genauer definierten Begriffen Computersicherheit oder IT-Sicherheit vorgezogen? Es entsteht der Eindruck, dass ein Sicherheitskonzept mit einem nur vage umrissenen Referenzobjekt politische Vorzüge mit sich bringt.

Das diskursorientierte Argument der *Cyberfizierung* lässt sich auch aus institutioneller Perspektive nachvollziehen (von Solms und van Niekerk 2013). Staatliche Akteure wie Militär, Außenministerien oder Polizeiämter haben damit begonnen, der wahrgenommenen Bedrohung des Cyber eigene institutionelle Antworten entgegenzusetzen.

Beispiel aus dem Militär: Bei der Militarisierung von Cyber spielt das amerikanische Militär eine herausragende Rolle. Die Erkenntnis, dass Cyber ein entscheidender Kriegsschauplatz werden würde, verleitete amerikanische Militärs 2009 zur Gründung eines eigenen Cyber Commands. Gleichberechtigt neben Land, Luft und See übernimmt dieses die Koordinierung von Streitkräften in einer neuen, digitalen Kampfsphäre. Cyber wird dabei als neue Querschnittsaufgabe konstruiert, wofür eine eigene räumliche Konstruktion besonders hilfreich ist. Cyber ist damit ein instrumentell besonders relevantes Konstrukt bei der Legitimierung von militärischen Einsätzen über das Internet. In Deutschland wurde diese Cyber-Logik auch auf die Bundeswehr übertragen. In der *Strategischen Leitlinie Cyber-Verteidigung* wird der Cyberraum als neue Dimension der Verteidigungspolitik dargelegt (BMVg 2015). Die Bundeswehr scheut jedoch offensichtlich davor zurück, in den Cyberraum ähnliche Ressourcen zu investieren wie das US-Militär. Gleichwohl teilt das Bundesverteidigungsministerium die amerikanische Definition von Cyber als *neuen* Ort für militärische Eingriffe, die die herkömmliche Definition von militärisch-relevanter Räumlichkeit erweitert: „Neben den klassischen Räumen Land, Luft, See und Weltraum ist auch der Cyber-Raum somit ein Operationsraum" (BMVg 2015).
Ähnlich wie in den USA erlaubt der Begriff Cyber in Deutschland die Mobilisierung von zusätzlichen Ressourcen für eine Querschnittsaufgabe, wenn auch in deutlich geringerem Umfang als in den USA. Durch die gezielte Militarisierung eines als zivil geltenden Kommunikationsnetzwerks werden die Kompetenzen des Militärs massiv ausgeweitet. Während die Aufgaben zum Schutz von IT-Infrastruktur und Systemen bisher bei zivilen Akteuren lag, wird dieser *Heimatschutz* jetzt auch von der Bundeswehr betrieben. Völkerrechtliche und politische Grundsätze der Kriegführung sowie der inneren und äußeren Sicherheit sind auf militärische Manöver im Cyberraum nicht ohne weiteres übertragbar.

Beispiel aus der Außenpolitik: Außenministerien in der ganzen Welt haben Stellen für eigene Cyber-KoordinatorInnen geschaffen und in über 50 Ländern gibt es nationale Cybersicherheitsstrategien. Bei der Entwicklung dieser Dokumente wird auch klar, wie sehr die politische Logik von Cyber über die gesamten Strategien hinweg zu einem deutlichen Sicherheitsfokus führt. Zunächst werden Cybersicherheitsstrategien entwickelt (Klimburg 2012;

Luiijf et al. 2013), aus denen dann später auch andere internationale Cyberstrategien entwickelt wurden. In diesem Kontext bleibt das Primat der Sicherheit und damit auch das Primat des Cyber in der internationalen politischen Strategie der beteiligten Außenministerien bestehen. So beschäftigt sich das Auswärtige Amt weiterhin mit *Cyber-Außenpolitik,* auch wenn darunter verstanden wird, „die wirtschaftlichen Chancen des Internets auszubauen" oder „universelle Menschenrechte wie den Schutz der Privatsphäre und Meinungs- und Pressefreiheit auch im Internet zu schützen und die freiheitsstiftenden Wirkungen des Internets verantwortungsvoll zu nutzen" (AA 2015).

Diese Debatte spielte auf europäischer Ebene ebenfalls eine gewichtige Rolle bei der Entwicklung einer europäischen Cybersicherheitsstrategie. Bei der Entwicklung dieser Strategie wurde „auf Druck Schwedens und der Niederlande eine Cyber-Strategie vereinbart, die über den Bereich Sicherheit hinausgeht" (Bendiek et al. 2012, S. 5); ein Vorstoß der bisher nur bedingt erfolgreich war. Diese Übermacht der Sicherheitspolitik im Cyberbereich war dann selbst für DiplomatInnen, die mit Sicherheitspolitik regelmäßig zu tun haben, zu viel und führte zu einer anhaltenden Debatte zwischen den Mitgliedstaaten der Europäischen Union, ob nicht aus der EU-Cybersicherheitsstrategie eine allumfassende Cyberstrategie entwickelt werden sollte.

Bemerkenswert ist auch, dass letztlich die Verbreiterung der Strategie über Sicherheit und Außenpolitik hinaus für die Bundesregierung gar nicht unter dem Begriff Cyber möglich war. So hat sich die Bundesregierung stattdessen, wie viele andere Regierungen auch, eine *Digitale Agenda 2014–2017* gegeben, auf deren Grundlage sowohl wirtschaftliche als auch gesellschaftspolitische und sogar außen- und sicherheitspolitische Dimensionen integriert werden.

Beispiel aus der Polizeiarbeit: Deutlich länger verbreitet als im Bereich der Außenpolitik sind Strategien zur Bewältigung von Cybercrime. Hier ist die Verwendung erst in den letzten Jahren historisch deutlich gewachsen, da der Begriff Cyber zunächst bis 2005 nur selten auftaucht und erst seit den 1970er Jahren als „Computerkriminalität" (Dornseif 2005, S. 37) und später als „Missbrauch der Informations- und Kommunikationstechnik" (Dornseif 2005, S. 38). Dies ist allerdings zu differenzieren von „Cybercrime im weiteren Sinne […] [, welches] alle Straftaten, bei denen mithilfe von Informations- und Kommunikationsmedien (dem Internet, Telefon usw.) Straftaten geplant, vorbereitet und ausgeführt werden [beinhaltet]" (Stammer 2014, S. 3).

Durch die oben beschriebene Konvergenz von „realweltlichen und virtuellen Räumen" (Löw et al. 2008, S. 81) bzw. durch die stetige Durchdringung aller Gesellschaftsbereiche durch die Digitalisierung ist somit jede Form von Kriminalität automatisch auch potentiell als Cybercrime deklariert. Die definitorische Unschärfe scheint für die polizeiliche Kriminalstatistik keine grundsätzlichen Probleme mit sich zu bringen, was darauf hindeutet, dass der Ermessensspielraum

der Polizei bei Cybercrime eher eng ausgelegt wird.
Auch die europäische Polizeiagentur Europol erkennt den gesellschaftlichen Wandel, geht aber davon aus, dass „the speed at which society and crime 'cyberise' exceed the speed at which law enforcement can adapt" (Europol 2015, S. 66). Durch die *Cyberfizierung* des gesellschaftlichen Wandels wird suggeriert, dass sich Kriminalität grundsätzlich ändern würde. Gleichwohl wird von Europol eingestanden, dass auch bei Verbrechen wie Mord digitale Beweismittel fast immer eine Rolle spielen (Europol 2015, S. 66). Um Probleme im Adaptionsprozess der Polizei an den digitalen Wandel zu kaschieren, muss der Begriff Cybercrime als neuartige Bedrohung herhalten um sicher zu stellen, dass entsprechende Ressourcen mobilisiert werden.

5 Cyber als Praxis: Wer macht Cyber?

Wie bereits dargestellt, unterscheidet sich der tatsächliche Umgang mit Cyber als Praxis sehr von den Diskursen über Cyber. Während in den Diskursen von einem abstrakten und *entgrenzten* virtuellen Raum gesprochen wird, werden in der Bekämpfung des Cybercrime oder bei Cyberangriffen sehr konkrete Menschen verhaftet oder Systeme zerstört. Anstatt ständig in luftigen Höhen über ein sehr praktisches Phänomen zu sprechen, wäre es daher viel sinnvoller über den praktischen Umgang mit Cyber zu sprechen, also was Menschen tatsächlich machen wenn sie Cyber sagen. Dies entspricht auch dem "practice turn" (Adler and Pouliot 2011) in den internationalen Beziehungen, der den Forschungsfokus auf *practices* und *practitioners* legt.
Viele praktische Analysen aus dieser Perspektive stehen noch aus, aber erste Versuche hierdurch Sicherheitspolitik im digitalen (Schmidt 2014) und nicht digitalen (Adler 2008) Bereich sind durchaus vielversprechend. Um Cyber zu verstehen, muss Wissenschaft viel eingehender *communities of practice* untersuchen, um deren implizites Wissen zu verstehen. Denn erst durch dieses implizite Wissen von Polizei, Bundesamt für Sicherheit in der Informationstechnik (BSI) oder Bundesnachrichtendienst (BND) von dem, was Cyber ist und sein könnte, ist es überhaupt möglich, die Kategorie Cyber zu konstruieren. Gerade weil dies nicht en détail untersucht worden ist, ist die Definition von Cyber so vage, und wird dadurch letztlich zu einer beliebig ausdehnbaren aber letztlich kaum definierten Kategorie. Neben den *communities of practice* ist noch ein anderer Aspekt extrem relevant: die Macht- und Funkionslogik von Cyber. Gerade weil so viele Machverhältnisse mit dem Begriff verknüpft sind, ist eine genauere Analyse notwendig, die im letzten Teil dieses Artikels begonnen wird.

6 Fazit: Die Macht- und Funktionslogik des Cyber

Die Debatte über technologischen Wandel wird überwiegend im Kontext eines irrealen Raums geführt. Anstatt zu fragen, was Menschen mit digitalen Technologien machen, wird primär der Wandel zu Cyber und *Cyberfizieriung* als Debatte über einen überidealisierten, virtuellen Raum geführt. Dabei geraten die tatsächlichen Praktiken von Menschen mit digitalen Technologien in den Hintergrund, was wiederum dazu führt, dass diese kaum verstanden werden.

Der Begriff des Cyber spielt hierbei eine entscheidende Rolle, da er fünf entscheidende Funktionen in einer Debatte um Technologie und Gesellschaft erfüllt, die für die Regulierung von Technologie besonders relevant sind. *Erstens* ist eine *begriffliche Expansionsfunktion* zu konstatieren; durch die außerordentlich breite Definition von Cyber werden davon so gut wie alle Gesellschaftsbereiche berührt. Selbst wenn Individuen nicht unmittelbar digitale Technologien benutzen, können sie dennoch vom Cyberspace betroffen sein, indem zum Beispiel die JournalistInnen in ihrer Zeitung über digitale Medien recherchieren. *Zweitens* hat der Begriff Cyber eine *Mobilisierungsfunktion*, in dem er etwas Neues und bisher noch nicht Dagewesenes suggeriert, wofür entsprechend auch neue Ressourcen mobilisiert werden müssen. Dadurch kann zum Beispiel die Polizei oder das BSI deutlich machen, warum diese neue Ressourcen brauchen. So wird zum Beispiel Analysten des Britischen Geheimdienst GCHQ in einem internen Handbuch dem ‚Problem Book' empfohlen den Begriff cyber besonders häufig zu benutzten, weil durch die Verwendung des Begriffs neue finanzielle Ressourcen mobilisiert werden können die sonst nicht zur Verfügung stehen würden (Doctorow 2016). Dies hängt, *drittens,* natürlich eng mit der *Versicherheitlichungsfunktion* von Cyber zusammen, denn die Mobilisierung von Ressourcen findet in der Regel im Sicherheitsbereich statt. Wie aus den oben stehenden Beispielen deutlich wird, kann Cyber nicht ohne den Bezug zu Sicherheit gedacht werden.

Gleichzeitig hat der Begriff *viertens* durch seine besondere Unschärfe eine *Verschleierungsfunktion,* da völlig unklar ist, was mit dem Begriff eigentlich gemeint ist. Ähnlich zu anderen nur schwierig zu bestimmenden Begriffen ist diese Verschleierung durchaus erwünscht, um möglichst viel Handlungsspielraum für Reaktionen auf Cyberbedrohungen zuzulassen. Dies hängt *fünftens* auch mit der *Dematerialisierungsfunktion* des Begriffs zusammen, der eine surreale *Entweltlichung* gleichkommt. Da ein selbstreferenzieller, virtueller Raum suggeriert wird, kann im Prinzip so gut wie alles in diesem Raum passieren.

Diese Funktionslogiken sollten allen bewusst sein, die den Begriff Cyber verwenden. Durch den zunehmenden Anstieg von Debatten über Digitalisierung, moderne Kommunikationstechnologie

und das Internet werden auch immer neue Begriffe und Metaphern für das Internet entwickelt. Unsere Vorstellungen der Digitalisierung bestimmen unmittelbar deren sozial Konstruktion und mittelbar auch das Internet an sich (Mansell 2012). Gerade weil die zukünftige Entwicklung digitaler Technologien weiterhin unklar ist, sind die Begriffe und Metaphern, die das Internet beschreiben, besonders wichtig. Der Begriff Cyber ist nicht alternativlos, kann aber ohne entsprechenden sozialen Kontext nicht gedacht werden.

6 Literatur

Ahrens, D. (2003). Die Ausbildung hybrider Raumstrukturen am Beispiel technosozialer Zusatzräume. In C. Funken, & M. Löw (Hrsg.), *Raum – Zeit – Medialität. Interdisziplinäre Studien zu neuen Kommunikationstechnologien* (S. 173–190). Opladen: Leske + Budrich.

AA – Auswärtiges Amt. (2015, 13. Nov.). Cyber-Außenpolitik, http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html. Zugegriffen: 21. Jan. 2016.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Humanist,56*(3), 18–19.

Bendiek, A., Dickow, M., & Meyer, J. (2012). Europäische Außenpolitik und das Netz. *SWP-Aktuell,* (60).

BMVg – Bundesministerium der Verteidigung. (2015, 16. Apr.). Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg. netzpolitik.org. https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#2-Strategischer-Kontext. Zugegriffen: 21. Jan. 2016.

Daase, C. (2009). Der erweiterte Sicherheitsbegriff. In M. A. Ferdowsi (Hrsg.), *Internationale Politik als Überlebensstrategie* (S. 137–153). München: Bayerische Landeszentrale für politische Bildungsarbeit.

Doctorow, Cory. 2016. “Exclusive: Snowden Intelligence Docs Reveal UK Spooks’ Malware Checklist / Boing Boing.” *BoingBoing*. Retrieved February 11, 2016 (https://boingboing.net/2016/02/02/doxxing-sherlock-3.html).

Dornseif, M. (2005). *Phänomenologie der IT-Delinquenz: Computerkriminalität, Datennetzkriminalität, Multimediakriminalität, Cybercrime, Cyberterror und Cyberwar in der Praxis.* Unveröffentlichte Dissertation, Universität Bonn.

Ellrich, L. (2002). Die Realität virtueller Räume: soziologische Überlegungen zur ‚Verortung‘ des

Cyberspace. In R. Maresch, & N. Werber (Hrsg.), *Raum – Wissen – Macht.* Frankfurt am Main: Suhrkamp.

Europol. (2015). The Internet Organised Crime Threat Assessment (IOCTA). https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf. Zugegriffen: 21. Jan. 2016.

Graham, M. (2013). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal, 179*(2), 177–182.

Klimburg, A. (Hrsg.). (2012). *National cyber security framework manual.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Lipshin, J. (o. J.). MCI's anthem (1997) – Freedom from the marked body. Critical Commons. http://www.criticalcommons.org/Members/JLipshin/clips/Anthem.mp4/view. Zugegriffen: 21. Jan. 2016.

Löw, M., Steets, S., & Stoetzer, S. (2008). *Einführung in die Stadt- und Raumsoziologie*. Opladen, Farmington Hills: Budrich.

Luiijf, E., Besseling, K, & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1), 3–31.

Mansell, R. (2012). *Imagining the internet: communication, innovation, and governance*. Oxford: Oxford University Press.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97–102.

Stammer, C. (2014). Einblick in die Cybercrime am Beispiel des Phishing. Hochschule für Wirtschaft und Recht Berlin. http://www.hwr-berlin.de/fileadmin/downloads_internet/publikationen/beitraege_FB4/Heft_1_2014_Fachbereich_Rechtspflege.pdf. Zugegriffen: 21. Jan. 2016.

thejuicemedia. (2015). A message from George Orwell, to everyone on the Internet. YouTube. https://www.youtube.com/watch?v=c4EEa0HAqzQ&feature=youtu.be. Zugegriffen: 21. Jan. 2016.

Thiel, T. (2012). Unendliche Weiten…? Umkämpfte Grenzen Im Internet. *Indes, 1*(4), 61–67.