Cyberwar

Zur strategischen Transformation eines umkämpften Objekts im deutschen Kriegsdiskurs

von Laurids Melbye und Julius Wörner

Der Cyberraum als Kriegsgebiet

Kriegsführung im Internet ist längst keine Fantasie düsterer Militärstrateg_innen und Sci-Fi-affiner Regisseur_innen mehr, sondern zunehmend Teil der alltäglichen medialen Berichterstattung. Die U.S.-amerikanischen Präsidentschaftskandidat_innen diskutierten noch in der Endphase des Wahlkampfes von 2016 live im Fernsehen über den Themenpunkt Cyberwarfare und die Herkunft von Hackerangriffen (vgl. CNN 2016), in deren Folge über 44.000 Seiten E-Mails des Democratic National Committee (vgl. Wikileaks.org 2016a), ebenso wie 20.000 Seiten E-Mails der Clinton-Wahlkampagne (vgl. Wikileaks.org 2016b), allgemein zugänglich gemacht wurden. Dabei stand insbesondere zur Debatte, ob es sich bei der Identität der Angreifer um staatliche Akteure anderer Nationen handelt. Im Zusammenhang mit diesen Vorkommnissen mehren sich im öffentlichen Diskurs die Sorgen um weitere mögliche digitale An- und Eingriffe sowie deren Konsequenzen, wie sich dies auch im Vorfeld der Bundestagswahl 2017 zeigte (vgl. Heise.de 2016a).

Dieser gesteigerten Aufmerksamkeit für den Cyberwar im öffentlichen Diskurs entsprechen auch aktuelle Novellierungen innerhalb der Sicherheits- und Verteidigungspolitik. So hat die NATO durch die Erklärung des Cyber- und Informationsraums zum militärischen Operationsfeld am 14. Juli 2016 (vgl. Spiegel.de 2016) die klassischen Operationsfelder (Land, Wasser, Luft, Weltraum) um ein Fünftes ergänzt. Ein Novum mit Folgen, da hiermit

im deutschen Kriegsdiskurs die Einrichtung einer neuen Teilstreitkraft neben Heer, Marine und Luftwaffe für diese neue Dimension der Kriegsführung als eine Notwendigkeit dargestellt werden konnte (vgl. Faz.net 2015). Entsprechend wurde am 5. April 2016 die fünfte Teilstreitkraft der Bundeswehr offiziell durch die Verteidigungsministerin Von der Leyen ins Leben gerufen.

Ein folgenreiches Ereignis, dessen Entstehungsprozess hier in der Betrachtung ministerialer Alltagsarbeit, respektive ihrer materiellen Zeugnisse, analysiert werden soll. Diese beträchtliche Umgestaltung der deutschen Sicherheits- und Verteidigungsarchitektur wird dabei vor dem Hintergrund des bundesdeutschen Kriegsdiskurses eingebettet, welcher in Form von öffentlichen Debattenbeiträgen und weiterer zugänglicher Regierungsdokumente eingehend untersucht wurde. Hierzu wird im Folgenden, aufbauend auf die jeweilige sequentielle Feinanalyse von insgesamt vier ministerialen Dokumenten, eine trans-sequentielle Analyse nach Scheffer (2015) unternommen, welche diese Materialien in ihrer jeweiligen situativen Entfaltung als Schritte hin zu der Einrichtung dieser neuen Teilstreitkraft, dem Kommando Cyber- und Informationsraum (KdoCIR), zusammenbindet. Auf die hierzu angewandten Methoden wird in der Darstellung der Analyseergebnisse näher eingegangen werden. Zur Erhebung des hierzu benötigten Materials wurde zu Beginn unserer Recherche eine explorative, ungerichtete Sammlung von Medienberichten angelegt, welche sich vom Jahr 2000 bis zum Februar 2017 erstreckt. Auf ihrer Basis wurde ein Netzwerk aus insgesamt 215 Zeitungsartikeln sowie 16 Publikationen der Bundesregierung generiert, in welcher die einzelnen Beiträge anhand harter Verweise, also direkter Bezüge und Quellenangaben verknüpft wurden. Mittels dieser Vorgehensweise wurden die vier sequentiell analysierten Dokumente als für den bundesdeutschen Kriegsdiskurs bedeutsam erkennbar. Dabei sollen die wiederkehrenden Motive beleuchtet werden, die in diesen und auch in weiteren Debattenbeiträgen erkennbar werden, welche diesen Prozess auszeichnen und Aufschluss bieten über mögliche zukünftige Entwicklungen.

Aus Sicht trans-sequentieller Analytik stellt sich hier zunächst die grundsätzliche Frage, wie der Cyberwar als „formatives Objekt" (Scheffer 2015: 233) dem bundesdeutschen Kriegsdiskurs überhaupt zugeführt wurde und welche Konsequenzen dies hatte. Wann also wurde der Begriff des Cyberwars innerhalb dieses Diskurses aufgenommen, mit Hilfe welcher Mittel wurde dies vollzogen, wie wurde er im Lauf der Zeit geformt und wie wirkte der Cyberwar formativ auf diesen Kriegsdiskurs zurück (vgl. ebd.: 228ff.)? Ziel dieses Artikels ist es daher, die erfolgten Umformungen des

> Wann also wurde der Begriff des **Cyberwars** innerhalb dieses Diskurses aufgenommen, [...] und wie wirkte der Cyberwar formativ auf diesen Kriegsdiskurs zurück ?

Diskursobjektes Cyberwar und seine zukünftigen, formativen Konsequenzen für das Regierungshandeln in Deutschland durch diese trans-sequentielle Analyse aufzudecken.

Dass der Cyberwar gegenwärtig eine zentrale Stellung im Kriegsdiskurs einnimmt, kann aus ethnomethodologischer Sicht als eine Leistung der im Diskurs mit diesem Objekt arbeitenden Akteure verstanden werden - als ein praktisches ‚Accomplishment' im Sinne Harold Garfinkels (1969: 1ff.), mit welchem Handlungen gegenüber Anderen sichtbar und als angemessen ausweisbar gemacht werden können. Das Funktionieren dieser ‚Accounts' (Garfinkel 1969: 1) ist für die Praxis von Regierungsmitgliedern entscheidend, da angenommen werden kann, dass politische Entscheidungen und die hierfür gewählten Verfahren in Deutschland grundsätzlich der demokratischen Legitimation durch die Öffentlichkeit bedürfen (vgl. Blatter 2007; Lucke 1996; Luhmann 1969). Außerdem ist prinzipiell auch heute noch davon auszugehen, dass Medienakteure wie jene, welche hier als Teilhaber am Diskurs betrachtet wurden, in der doppelten Funktion der Demonstration des Geschehenen und seiner kritischen Kommentierung agieren und hierdurch idealerweise eine Form kritischer Öffentlichkeit bilden, welche diese Entscheidungsprozesse aufmerksam begleiten (vgl. Wimmer 2007: 23ff.; Habermas 2015: 293ff.).

Als Ergebnis soll herausgestellt werden, dass der Cyberwar seine Karriere – abseits der aktuellen technologischen Möglichkeiten – insbesondere auch dem Umstand verdankt, dass er sich aufgrund seiner Unterbestimmtheit flexibel in bestehende Konstruktionen von Unsicherheit einbringen lässt und diese entscheidend ausweiten kann, ohne selbst an strategischer Offenheit zu verlieren. Mit diesem Objekt lassen sich also paradoxerweise Sicherheit und Unsicherheit gleichermaßen innerhalb von Regierungsdokumenten inszenieren und bearbeitbar machen. Wie sich dies auf die Antizipation kommender Gefahren auswirkt, wird ebenfalls behandelt werden.

Die Entdeckung des Cyberwars: Eine Genealogie

Was gegenwärtig unter ‚Cyberwar' gegenwärtig verstanden wird, lässt sich gut an der Definition des *Weißbuchs 2016* des Bundesministeriums der Verteidigung ablesen. Hier steht er synonym für Cyberwarfare, Informationskrieg, Cyberkrieg, Krieg im Internet und weitere Wortschöpfungen und signifiziert die digitale Kriegsführung zwischen staatlichen Akteuren, etwa militärischen oder paramilitärischen Einheiten im Auftrag von staatlichen Regierungen (BMVg 2016a). Die noch junge Geschichte dieser Thematik zeichnet sich durch mehrere Steigerungen aus, welche sich im Zusammenhang mit einzelnen, bedeutenden Ereignissen vollziehen und extensiv von den Medien behandelt wurden. So war der über das Internet geführte Krieg in den Neunzigern des letzten Jahrhunderts vor allem noch Gegenstand von Diskussionen über Formen zukünftig-möglicher Kriegsführung und warf Fragen grundsätzlicher Natur auf, etwa wie eine solche Gefahr völkerrechtlich eingeordnet und über bindende Regelungen eingehegt werden könnte (vgl. Minkwitz/Schöfbänker 2000). Diese theoretischen Fragen gewannen im Verlauf des ersten Jahrzehnts nach der Jahrtausendwende eine neue Dringlichkeit, als sich die Anzeichen für Kriegsführung im Cyberraum zu verdichten schienen, welche es ermöglichten, dass das Diskursobjekt Cyberwar aus dem Bereich des grundsätzlich Vorstellbaren in einen Bereich des praktisch Möglichen überführt wurde. Bereits in den Verteidigungspolitischen Richtlinien 2003 und im Weißbuch 2006 wird das Szenario eines solchen „Informationskrieges" (BMVg 2006: 101) bzw. einer „Informationskriegsführung" (BMVg 2003: 8) als grundsätzliche Möglichkeit dargestellt. Diese wird jedoch nicht weiter elaboriert und bleibt abseits der Aussage, man werde sich mittel- bis langfristig mit der Entwicklung von Maßnahmen beschäftigen, noch ohne erkennbare Konsequenzen.

Der für diesen Kriegsdiskurs entscheidende Wendepunkt ereignet sich im April 2007 mit einem digitalen Angriff auf estnische Regierungs- und Infrastruktureinrichtungen (vgl. Nzz.ch 2008), welcher von Medienakteuren als ein erster konkreter Fall digitaler Kriegsführung betrachtet wurde. Dieser Präzedenzfall wiederum habe, so lautet jedenfalls der Konsens im Kriegsdiskurs, zur Einführung des Cyberabwehrzentrums der NATO in Tallinn geführt (vgl. Nzz.ch 2015). Abgesehen von weiteren Fällen vermuteter Cyberkriegshandlungen war es weiterhin besonders der sogenannte Stuxnet-Angriff auf iranische Nukleareinrichtungen im Jahr 2010, welcher in den Folgemonaten seiner diskursiven Karriere als herausragendes Ereignis die Debatte im internationalen wie auch im deutschen Kriegsdiskurs nachhaltig prägte (vgl. Bundeszentrale für politische Bildung

2016; Gayken 2010). Beide Ereignisse werden als Fälle von Cyberwarfare auch heute noch häufig als Verweis auf die reale Gefahr dieser Form der Kriegsführung herangezogen.

Zu genau diesem Zeitpunkt ist das erste Dokument angesiedelt, welches im folgenden Kapitel analysiert wird. Seine Besonderheit kann vor dem Hintergrund dieser ersten Steigerung verstanden werden. Es handelt sich um die 2011 erschienene Neuauflage der Verteidigungspolitischen Richtlinien (BMVg 2011), welche angesichts dieser ersten erkannten Fälle von Kriegsführung im Internet eine neue Initiative zur Bearbeitung dieser antizipierten Bedrohung macht.

Den Cyberwar im Kriegsdiskurs verorten: Die Verteidigungspolitischen Richtlinien 2011

Das Dokument „Verteidigungspolitische Richtlinien 2011" (im Folgenden: *VPR 2011*, vgl. BMVg 2011) legt die Grundlage für ein neues Verständnis dessen, was der Cyberwar ist und sein kann. Verteidigungspolitische Richtlinien werden vom Bundesministerium der Verteidigung herausgegeben und dem Planungsstab unter der Leitung des/der zuständigen Bundesministers/-in zugeschrieben. Sie werden seit 1972 regelmäßig herausgegeben und legen nach offizieller Darstellung des BMVg die Grundsätze für die Gestaltung der Verteidigungspolitik, den Auftrag der Bundeswehr sowie ihre Aufgaben fest und setzen Vorgaben für zukünftig anzustrebende Fähigkeiten der Streitkräfte (vgl. ebd.). Diese Setzungen werden in den Kontext gesamtstaatlicher Sicherheitsvorsorge eingebettet. Die *VPR 2011* formulieren und repräsentieren dementsprechend die sicherheitspolitischen Interessen der Bundesrepublik (BMVg 2011: 1). Bis zum Erscheinen des *Weißbuches 2016* ist dies die letzte hochrangige Publikation des BMVg, welches auf dieser umfassenden Ebene die Ziele, Aufgaben und Fähigkeiten des Verteidigungsministeriums und der Bundeswehr im gesamtgesellschaftlichen Kontext formuliert. Sie ist definiert als „verbindliche Grundlage für die Konzeption der Bundeswehr und für alle weiteren Folgearbeiten im Geschäftsbereich des Bundesministeriums der Verteidigung" (ebd.: 1), produziert also eine Verpflichtung zu ihrer weiteren Beachtung für zukünftige Ausarbeitungen. Insofern ist dieses Dokument ein geeigneter Startpunkt für die vorgenommene Untersuchung.

Aus einer ethnomethodologischen Betrachtung heraus stellt sich nun zuerst die Frage, wie in diesem Account eine Sichtbarkeit und Berichtbarkeit bestimmter sicherheits- und verteidigungspolitischer Verhältnisse hergestellt wird (vgl. Garfinkel 1967: 1). Wie also generieren die mit der Politik befassten Akteure mithilfe

dieses Dokumentes ein Verständnis der sie umgebenden Welt und ihrer praktischen Notwendigkeiten füreinander, wie halten sie dieses Verständnis fest und wie können sie dadurch zu bestimmten Handlungen am Objekt Cyberwar auffordern? Die Herstellung von Analysierbarkeit in der angewandten Sprache ist hier von erheblicher Bedeutung (vgl. Hester/Eglin 1997). Der analytische Fokus liegt daher besonders auf der ordnenden Funktion und den hiermit verbundenen praktischen Konsequenzen dieser Accounts (vgl. Garfinkel 1967, Garfinkel/Sacks 1990, Rawls 2002). Im Hinblick auf das hier untersuchte Dokument, die *VPR 2011*, ist das erste Ziel der Analyse das Herausarbeiten der sprachlich entfalteten sicherheits- und verteidigungspolitischen Lage und der ihr zugrundeliegenden Rationalisierung, mit welcher diese Verhältnisse erklärt werden. Im Anschluss hieran wird in einem weiteren Schritt untersucht, wie das Objekt Cyberwar in dieses Lagebild eingebracht und strategisch zur Erreichung bestimmter Ziele genutzt wird.

Zur Offenlegung der vorausgesetzten Sicherheitslage und des gegebenen Bearbeitungsstandes des Objekts Cyberwar in dieser diskursiven Situation erscheint das Instrumentarium der sequentiellen Membership Categorization Analysis (MCA) geeignet, wie sie aus der Ethnomethodologie heraus auf der Basis der Arbeiten von Harvey Sacks entwickelt wurde (vgl. Sacks 1990, 1996; weiterführend auch Hester/Eglin 1997, Silverman 1998: 74ff.; Bergmann 2010). Sie offenbart die entfaltete sicherheits- und verteidigungspolitische Ordnung und weiterhin die praktische Handhabung mit dem Objekt Cyberwar vor Hintergrund dieses Kontextes. Dies wird in der Analyse erreicht durch die sequenzielle Betrachtung der genutzten Kategorien, der aufgeworfenen Relationen zwischen diesen und den an die Kategorien und Kategorienbünde geknüpften Aktivitäten und Prädikate. An ihrem Ende steht somit ein weitgeflochtenes Beziehungsnetz zwischen den Sicherheits- und Verteidigungspolitischen Kategorien und den ihnen zugeschriebenen Zuständen und Aktionen.

Wie also, so lässt sich mit der MCA fragen, wird innerhalb der *VPR 2011* eine solche sicherheits- und verteidigungspolitische Ordnung aufgebaut und wie wird das in den Bewertungen der vorigen Ereignisse immer gewichtiger gewordene Objekt Cyberwar in diese eingefügt? Als entscheidend hierfür stellt sich in der Analyse die im Dokument grundlegend gesetzte Unterscheidung zwischen einem *Hier* und einem *Nicht-Hier* heraus. Die Darstellung der gegenwärtigen Sicherheitslage in der *VPR 2011* lebt von der Unterscheidung bestimmter räumlicher Gebiete entlang einer nah-bis-fern reichenden Achse, ausgehend von einem an der Sprecherposition erkennbaren Zentrum „Deutschland“, über

„Europa“ reichend bis hin zur „Peripherie“ (BMVg 2011: 2). Das Ziehen dieser räumlichen Unterscheidung markiert den ersten Zug. Das “Hier” wird als Hort der Sicherheit erkennbar gemacht. Diese geographisch-definitorische Abgrenzung wird anschließend im folgenden Zug von einem einseitigen Wirkungsverhältnis unterlaufen, welches von dieser fernen Peripherie bis in das im ‚Hier‘ liegende Zentrum hineinreicht und die vorausgesetzte räumlich-gesicherte Ordnung sichtbar untergräbt. Dies zeigt sich hier:

> *Sicherheit wird nicht ausschließlich geographisch definiert. Entwicklungen in Regionen an Europas Peripherie und außerhalb des europäischen Sicherheits- und Stabilitätsraumes können unmittelbaren Einfluss auf die Sicherheit Deutschlands entfalten. Krisen und Konflikte können jederzeit kurzfristig und unvorhergesehen auftreten und ein schnelles Handeln auch über große Distanzen erforderlich machen.* (ebd.: 2)

Mittels dieser Argumentationsfigur wird das Ferne erfolgreich als Angelegenheit des Zentrums problematisiert. In dieser Ferne lauert ein diffuses, nicht weiter spezifiziertes Anderes, welches eine Bearbeitung erfordert, selbst wenn im Zentrum, wo die Leserinnen und Leser positioniert werden, Sicherheit und Stabilität herrschen. Deutlich wird hier auch die normative Hierarchisierung, welche die Trennung zwischen dem Raum der Sicherheit und demjenigen der offenbar fehlenden Sicherheit begleitet und ein Bedrohungsszenario zu untermauern hilft. Die Aufhebung einer Unterscheidungsgrenze durch eine Bedrohung findet sich nochmal in der Aussage, die „traditionelle Unterscheidung von äußerer Sicherheit und öffentlicher Sicherheit im Innern verliert […] mehr und mehr ihre Bedeutung“ (ebd.: 6). Interessanterweise wird dabei nie direkt darauf eingegangen, was dieses Andere nun genau ist, dass diese Gefahr ausstrahlt. Die Gefahr bleibt diffus und zu einem gewissen Maße flexibel einsetzbar.

Innerhalb der *VPR 2011* finden sich mehrere Spezifizierungen dafür, wie ein solches Unterlaufen der räumlich gesetzten Grenzen von außen einen Schaden im Inneren produzieren kann. Hierzu zählt unter anderem auch die Schädigung oder der Ausfall sogenannter kritischer Infrastrukturen, zu welchen auch die “Informationsinfrastrukturen” im virtuellen Informationsraum gezählt werden (vgl. ebd.: 3). Zu den positiven Nutzungsmöglichkeiten dieses Informationsraumes werden die „Mobilisierung von Demokratiebewegungen” gerechnet, zu den negativen vor allem politischer, wirtschaftlicher und krimineller Missbrauch durch fremde staatliche und nichtstaatliche Akteure; befürchtet werden vor allem „Desinformation“, „Radikalisierung“ und „Destabilisierung“ durch „Extremisten“ (vgl.

ebd.: 2). Die Informationsinfrastrukturen selbst gelten hier ebenfalls als potenzielles Ziel von „Cyber-Angriffe[n]“ (ebd.: 3). Diese Darstellung schafft grundsätzlich eine Bedrohungslage im Inneren durch äußere Gefahren, transportiert durch den Informationsraum, der wiederum selbst bedroht wird. Das Internet, so die Schlussfolgerung, untermauert das bereits oben angesprochene Bild einer Auflösung der räumlichen Trennung zwischen nah und fern und wird für diese Auflösung mitverantwortlich gemacht. Der Schutz der kritischen Infrastrukturen wird im Dokument insgesamt als eine der „subsidiären Aufgaben der Bundeswehr im Inland“ (ebd.: 15) verstanden und dem Heimatschutz zugeordnet (vgl. ebd.). Dieser dritte Zug öffnet den Cyberraum dem Zugriff verteidigungspolitischer Akteure, etwa den Einsatz der Bundeswehr, legitimiert über ihren Auftrag zum Heimatschutz.

Verstanden als Bedrohung staatlicher Stabilität und nationaler Sicherheit werden Cyberangriffe selbst mit den Attributen hoher „Geschwindigkeit und Nichtvorhersehbarkeit“ (ebd.: 3) versehen und in den Rahmen von „neuen, computergestützten Auseinandersetzung auch zwischen Staaten“ (ebd.: 3) gestellt. Diese werden zu diesem Zeitpunkt als „asymmetrische Bedrohungen“ (ebd.: 3) *in Entwicklung* bewertet. Die *VPR 2011* antizipiert hier einen Trend hin zu einer zukünftigen Kriegsbedrohung und macht diesen Trend und die eigene Antizipationsleistung sichtbar. Ein Angriff erscheint unausweichlich. Unter Referenz auf die Schwierigkeiten gegenwärtiger Präventionen wird im Dokument die Herstellung von zukünftiger Bearbeitbarkeit als Auftrag klar gesetzt. Dies wird reflexiv verstanden als ein erster Schritt der Vorsorge in Vorbereitung späterer Anpassungshandlungen (vgl. ebd.: 3). Entsprechend dieser Inszenierung des Cyberangriffes als antizipiertes Mittel zukünftiger, asymmetrischer Kriegsführung von staatlichen Akteuren besteht die Reaktion des BMVg zu diesem Zeitpunkt in dessen Übernahme in das eigene Vokabular von Kriegen, Konflikten und ihrer möglichen Handhabe durch die Bundeswehr. Diese Übernahme wird innerhalb dieses Dokuments geleistet.

Da bereits im Vorhinein der Informationskrieg als eine zukünftige Möglichkeit erwähnt wurde, ist dieser Schritt nicht aus dem Nichts gegriffen. Im Verhältnis zu früheren Veröffentlichungen ist neu, dass der Raum, der diesem Objekt Cyberwar im Dokument eingeräumt wurde, als Anerkennung seiner Existenz und der gesteigerten Relevanz seiner Bearbeitung gelesen werden kann. Interessanter aber ist, dass hier zum ersten Mal im Rahmen einer hochrangigen Veröffentlichung des BMVg eine systematische Einordung dieses Objektes erkennbar angeboten wird. Mit ihrer Hilfe lässt sich digitale Kriegsführung über den Heimatschutz zu einem Teil

der Sicherheits- und Verteidigungspolitik machen. Der Cyberwar findet Einzug in die Darstellung der allgemeinen Sicherheitslage mit ihrer räumlichen Unterscheidung von Zentrum und Peripherie und hilft, diese Darstellung erfolgreich argumentativ infrage zu stellen, was die Notwendigkeit einer zukünftigen Bearbeitung hervorhebt. Der Informationskrieg wird so in das bestehende Erklärungsmodell des BMVg eingebaut und bietet hier die Möglichkeit, die Verbindung von einem gefährlichen Äußeren mit einem zu schützenden Inneren zu untermauern; eine Verbundenheit, die durch verteidigungspolitische Akteure versichert werden soll. Insofern schafft dieses Dokument eine doppelte Relevanzmachung: ein Hervorheben des Cyberwars für die Sicherheits- und Verteidigungspolitik einerseits und des BMVg's durch den antizipierten Informationskrieg andererseits. Die *VPR 2011* erkennt sich selbst als eine Basis für derartige zukünftige Unternehmungen, und scheint die kommenden Maßnahmen bereits zu ahnen.

Ein eigenes Erklärungsmodell: Die Cyber-Sicherheitsstrategie für Deutschland 2011

In demselben Jahr, in welchem die Verteidigungspolitischen Richtlinien erschienen sind, wurde auch ein weiteres entscheidendes Dokument veröffentlicht. Bei dieser „Cyber-Sicherheitsstrategie für Deutschland" (im Folgenden: *CSS 2011*, vgl. BMI 2011) handelt es sich um eine Veröffentlichung durch das Bundesministerium des Innern vom Februar 2011. Sie bewegt sich damit, wie auch die *VPR 2011*, vor dem Hintergrund der gesteigerten Bedeutung des Objekts Cyberwar im Kriegsdiskurs. Sie wurde durch das Bundeskabinett beschlossen und zielt auf die Herstellung von allgemeiner Cyber-Sicherheit auf einem „der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau" ab (BMI 2011: 4). Um dieses nicht weiter spezifizierte "Niveau" im Zuge gesamtstaatlicher Sicherheitsvorsorge zu erreichen, werden in diesem Dokument die informationstechnologische Gefährdungslage und die Rahmenbedingungen einer solchen Cyber-Sicherheit dargestellt, um anschließend eine Leitlinie und die angestrebten Ziele und Maßnahmen zu beschreiben. Darüber hinaus werden hier wichtige Kernbegriffe für diese Arbeit definiert. Insgesamt lassen sich mit erneutem Blick auf die Kategorienbildung und -verknüpfung mehrere grundlegende Bewegungen innerhalb dieses Dokuments erkennen, welche das Objekt Cyberwar einfassen und in den späteren Dokumenten des BMVg wiederkehren. Weit mehr als nur die Integration des Cyberwars in ein bestehendes Schema wird hier die Ausarbeitung eines ganz eigenen Erklärungsmodells unternommen, welches Geltung für alle Formen informationstechnologischer Gefährdungen beansprucht.

> Die Cyber-Sicherheitsstrategie entwickelt im ersten Zug eine **Trennung zweier Räume**: einem territorial bestimmten, erkennbar **physischem Raum** und einem **Cyberraum**.

Wie wird dieses Modell sequentiell im Text erkennbar? Die Cyber-Sicherheitsstrategie entwickelt im ersten Zug eine Trennung zweier Räume: einem territorial bestimmten, erkennbar physischem Raum und einem Cyberraum. Während Ersterer in einzelne Nationalstaaten und ihre jeweils dazugehörenden „Lebensbereiche" (Staat, kritische Infrastrukturen, Wirtschaft, Bevölkerung, Gesellschaft (vgl. BMI 2011: 1)) unterteilt wird, wobei auch dieser Text von dem Betrachtungspunkt *Deutschland* aus aufbaut, umfasst der *Cyber-Raum* als zweiter Raum alle im globalen Maßstab über das Internet und mittels Datenaustausch vernetzten IT-Systeme. Definiert werden hierunter sowohl große Informationsinfrastrukturen wie auch alle vorstellbaren IT-Produkte und einzelnen Komponenten, egal ob Soft- oder Hardware; ausgenommen werden lediglich isolierte virtuelle Räume (vgl. ebd.: 14).

Dieses Nebeneinander der Räume, des physischen und des digitalen, wird im nächsten Zug durch eine Form einseitiger Abhängigkeit erweitert. Die Bewegungen im Cyberraum seien demnach gänzlich unabhängig vom physischen Raum, während die gesellschaftlichen Lebensbereiche den Zugang zum Cyberraum und seinen verschiedenen Komponenten unmittelbar benötigen. Die Prosperität dieser Lebensbereiche und damit diejenige des Landes ist hierdurch bedingt, andernfalls drohen für das kollektive Ganze „erhebliche[n] Beeinträchtigungen der […] Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen (Deutschlands)" (ebd.: 2). Entsprechend dieser Verwendung des Begriffs des Lebens steigern sich die möglichen Einwirkungen des Cyberraums auf den territorialen Raum und seinen Entitäten zwangsläufig zu einem „existenziellen" (ebd.: 2) Risiko, womit die Notwendigkeit einer Cyber-Sicherheitsstrategie zu dessen Bearbeitung begründet wird. Tatsächlich ist es aber nicht angestrebt, die einseitige Abhängigkeit aufzulösen oder eine andere Form des Verhältnisses beider Räume zu begründen, vielmehr soll die bisherige Form beibehalten und versichert werden.

Aufbauend auf dieses riskante Verhältnis beider Räume werden Gefährdungen entfaltet und relevante Akteure benannt. Unterschieden wird hinsichtlich der Angriffe aus dem Cyberraum grundsätzlich zwischen „Cyber-Ausspähung", „Cyber-Spionage" und „Cyber-Sabotage" je nachdem, ob der Erhalt von Daten oder die

Schädigung von Informationsinfrastrukturen das Ziel des Angriffs sind (ebd.: 14f.). Dargestellt wird ein qualitativer sowie quantitativer Anstieg der Angriffe, die sowohl „zahlreicher" als auch „komplexer" geworden seien (vgl. ebd.: 3). Das Dokument verlässt sich hier auf das kursorische Vorwissen von Leserinnen und Lesern, mit welchen die passenden Inferenzen gebildet werden können; es verweist nur oberflächlich auf reale Vorkommnisse und baut so eine weltgebundene Dringlichkeit auf, ohne sich auf die Diskussion einzelner Vorkommnisse einzulassen.

Wichtig ist hierbei, dass die Angriffe an die besonderen Eigenschaften des Cyberraum gebunden werden. Aufgrund dieser können sie „verschleiert" werden und „Opfersysteme" zu Angriffswerkzeugen umfunktionieren (vgl. BMI 2011: 3), während Herkunftsort, Identität und die Motive von Angriffen in der Regel nicht nachvollziehbar und offen für viele verschiedene Besetzungen sind („kriminelle, terroristische und nachrichtendienstliche Akteure", „militärische Operationen" (ebd.: 3). Diese Unterbestimmtheit wurde bereits beschrieben, wird hier aber als unauflösbar naturalisiert. Die Gefahr des Angriffs kann weder vom Cyberraum getrennt, noch kann die Bindung zu diesem aufgegeben werden, will man nicht die Lebensgrundlage der Gesellschaft schädigen. Durch diese Bearbeitung der Angriffe demonstrieren die Autorinnen und Autoren, dass es keine abschließende Sicherheit geben kann und es gerade daher einer fortwährenden Versicherheitlichung bedarf. Das Risiko einer existenziellen Gefährdung der Lebensbereiche bleibt bestehen. Das einzig Mögliche ist die Reduktion des Risikos auf ein "tragbare[s] Maß" an „Cyber-Sicherheit" (ebd.: 15). Das in der *CSS 2011* entfaltete Erklärungsmodell für den Cyberwar und das Bild einer unauflöslichen existenziellen Abhängigkeit des physischen vom digitalen Cyberraum und der hierdurch nicht abschließend herstellbaren Sicherheit werden im folgenden Dokument, der *Strategischen Leitlinie Cyber-Sicherheit 2015* des BMVg, sichtbar aufgegriffen und mit dem bereits herausgestellten Auftrag zum Schutz der Informationsinfrastruktur kombiniert.

Eine Möglichkeit zum Angriff: Die Strategische Leitlinie Cyber-Sicherheit

Die "Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" (im Folgenden: *SL 2015*, vgl. BMVg 2015a) wurde am 16. Mai 2015 durch die Verteidigungsministerin Ursula von der Leyen erlassen und zirkulierte bis zu ihrer unautorisierten Veröffentlichung durch das Nachrichtenportal Netzpolitik.org im Juli 2015 lediglich innerhalb des Bundesministeriums für Verteidigung. Da die "Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" nur als Leak im

Volltext auf dem Portal Netzpolitik.org vorliegt, können für diese Quelle leider keine Seitenzahlen zu den Zitaten ausgewiesen werden. Dieses Dokument greift beide bereits analysierten Dokumente namentlich auf, um auf deren Basis Relevanzen und Handlungsräume für das BMVg und damit für die Bundeswehr neu zu formen. Das erklärte Ziel besteht darin, die Cyber-Sicherheit als neuen Teil der gesamtgesellschaftlichen Sicherheitsvorsorge zu bearbeiten und die damit verbundenen zukünftig möglichen Beiträge des BMVg zu erschließen (vgl. BMVg 2015a).

Um nun zu analysieren, wie in diesem Dokument als ein neuer Schritt die beiden bisher produzierten und hier analysierten Positionen *VPR 2011* und *CSS 2011* verarbeitet werden, wird über die einzelne sequentielle Analyse hinaus eine trans-sequentielle Analyse notwendig, welche auf die Membership-Categorization-Analysis der einzelnen Dokumente aufsetzt und beobachtbare Bewegungen zwischen diesen Bearbeitungsschritten erkennbar macht. Die trans-sequentielle Analyse (TSA) nach Scheffer (vgl. Scheffer 2015, auch: 2008, 2012, 2017) unternimmt unter Einbezug des soziologischen "Verfahrens"-Begriff, wie er von Niklas Luhmann geprägt wurde (vgl. Scheffer et al. 2008, zum „Verfahrens"-Begriff auch Luhmann 1969, Lucke 1996, Stollberg-Rilinger 2001, Sikora 2001), eine Zusammenführung der empirischen Untersuchung einzelner Situationen bzw. Arbeitsepisoden im Rahmen mikrosoziologischer Analysen. Sie strebt damit nach einer sinnvollen Vereinigung von a) sequentiellen Analysen situativer Entfaltung und gemeinsamer Handlungskoordination von Akteuren im Moment und b) der Untersuchung des Ablaufs einer Prozessstrecke über einen situationsübergreifenden Zeitraum (vgl. Scheffer 2015). Auf diese Weise gelingt es etwa, das Wissen der Akteure um die vergangenen und zukünftigen Arbeitsabläufe und Aushandlungen in Rechnung zu stellen, ohne aber die Ungewissheiten und konkreten Probleme im situierten Jetzt zu unterschlagen (vgl. ebd.). Die beiden entscheidenden Begriffe *Prozess* und *Ereignis* sind in der TSA bereits immer auch aufeinander bezogen und erhellen sich wechselseitig (vgl. Scheffer 2008: 371ff., 2017: 99).

Im Zentrum der Analyse steht das formative Objekt, welches im Fokus der Bearbeitung der Akteure steht und von einer Episode in die nächste trägt und getragen wird. Die Arbeit der Akteure am Objekt ist es, welche die Prozesshaftigkeit der einzelnen Aushandlungen erkennen und die Situationen sinnvoll verknüpft erscheinen lässt. Die zentrale Stellung des Objekts ist dabei vielfältiger Natur: Es ist zu formen und bildet so den Fokuspunkt der Handlungen, wird selbst durch die einzelnen Bearbeitungen aus- und umgeformt, wie es auch bestimmte Forderungen an die Arbeitsschritte stellt und wirkt wiederum

formierend auf den Gesamtprozess zurück (vgl. Scheffer 2015: 233f.; 2017: 101). Dies bedeutet insgesamt, dass wir uns genau der einzelnen Situationen dieses Gegenstands-im-Werden annehmen mit ihren Bearbeitungen, Prüfungen und Passagepunkten, inklusive aller Anknüpfungen an frühere oder kommende Situationen (vgl. Scheffer 2015: 238ff.).

Wie also zeigt sich die Prozesshaftigkeit der Bearbeitung des Cyberwars in diesem Dokument, der *Strategischen Leitlinie Cyber-Verteidigung (SL) 2015*? Zunächst wird der in der *VPR 2011* enthaltenen Möglichkeit einer zukünftigen weiteren Bearbeitung des Cyberwars sichtbar entsprochen. Sie füllt somit nach eigener Aussage die dort vorbereitete Position möglicher weiterer Anpassung und markiert dies als ein Regelfall ministerialer Arbeit (BMVg 2015). Doch zu dieser weiterführenden Bearbeitung der inzwischen (an-)erkannten Gefährdung wird die in der *Cyber-Sicherheitsstrategie 2011* des BMI unternommene Entwicklung eines "vollständigen Instrumentariums" (BMI 2011: 12) herangezogen. Der dort in der *CSS 2011* artikulierte Regierungsauftrag zur „Gewährleistung von Sicherheit im Cyber-Raum" (BMI 2011: 4) wird in der *SL 2015* mit direktem Verweis hervorgehoben und explizit angenommen (BMVg 2015), also als Ziel eigener neuerlicher Ausarbeitung gesetzt. Die *SL 2015* übernimmt auch das in der *CSS 2011* erarbeitete Modell dessen, was der Cyberraum und die mit ihm verbundenen Risiken, Bedrohungen und Verwundbarkeiten sind und in welchem Verhältnis diese zum territorialen Raum Deutschlands stehen. Durch diese Übernahme des Erklärungsmodells des BMI durch das BMVg kann eine entsprechende eigene Definitionsarbeit verhindert und die Weiterbearbeitung als unproblematische Übernahme außerministerialer Wissensbestände dargestellt werden. In diesen beiden Zügen wird im Dokument also bereits sehr viel trans-sequentielle Arbeit mit Blick auf die weitere Formung des Cyberwars geleistet.

Das BMVg definiert sich und die Bundeswehr in einem weiteren Zug als einen der durch den Cyberraum existenziell bedrohten Lebensbereiche ähnlich dem Staat, der Wirtschaft und der Bevölkerung, wie sie in der *CSS 2011* genannt werden (vgl. BMI 2011: 2). Dies hat zur Folge, dass alle damit gültigen definitorischen Konsequenzen, also auch die Abhängigkeiten und Verwundbarkeiten, auf sie übertragen werden.

Hierdurch wird nicht allein eine eigene Betroffenheit evoziert, vielmehr wird hieraus auch weiter geschlussfolgert, dass auch andere Mitglieder der Kategorie Militär als Lebensbereich anderer Staaten an diese Konsequenzen gebunden sind (vgl. ebd.). Somit erwächst der Bundeswehr hieraus die Chance, andere militärische

Akteure über "Angriffsvektoren" (ebd.: 347), im Cyberraum angreifen zu können. Entsprechend wird gefordert, dass Handlungssicherheit für die Institution Bundeswehr geschaffen wird, mit welcher diese Möglichkeit ausgeschöpft werden kann. Das bezieht sich auf die Mittel und den rechtlichen Rahmen, mit welchen sie entsprechend ihres verfassungsmäßigen Auftrags operieren kann. Diese Argumentation wurde im weiteren Verlauf des Diskurses als Militarisierung des Internets skandalisiert (vgl. Sowa 2016, Netzpolitik.org 2016b). Sie lässt sich erkennen in der Definition des Cyberraums zum genuin militärischen Handlungsfeld:

> *Diese Voraussetzungen gelten für eigene wie gegnerische Streitkräfte als auch für nicht staatlich legitimierte bzw. nicht als militärisch klassifizierte Gegner gleichermaßen und bieten daher auch Ansatzpunkte für eigene Operationen. Neben den klassischen Räumen Land, Luft, See und Weltraum ist auch der Cyber-Raum* **somit ein Operationsraum**. *[...] Dies erfordert auch die Bereitstellung von adäquaten Strukturen und Ressourcen.* (BMVg 2015, Hervorheb. im Orig.)

Die grundlegende Problematik eines Angriffs aus dem Cyberraum bezüglich der (kaum vorhandenen) Erkennbarkeit der Identität und der Motive der Angreifer bleibt dabei, wie auch die Definition von

> Der Cyberwar ist [...] nicht länger nur eine Gefahr, sondern neuerdings auch eine Machtoption für das eigene Arsenal.

Cyber-Angriffen und ihren Wirkungen, unverändert von der *CSS 2011* zu *SL 2015* bestehen. Doch konnte das bereits in der *VPR 2011* erkannte militärische Objekt Cyberwar im Anschluss dieser neuerlichen Bearbeitung überraschenderweise dazu genutzt werden, eine entscheidende Neuformung dieses Objekts dahingehend zu erreichen, dass nun auch die Bundeswehr dazu befähigt werden soll, Kapazitäten zum Cyberangriff aufzubauen. Der Cyberwar ist dieser begrifflichen Wendung nach nicht länger nur eine Gefahr, sondern neuerdings auch eine Machtoption für das eigene Arsenal. Dabei besteht der Erfolg dieser Neuformung darin, als Regelfall ministerialer Folgearbeit an vorhandenen Dokumenten darstellbar zu sein.

Die Autorinnen und Autoren dieses Dokumentes *SL 2015* scheinen sich der Brisanz dieser Novelle im Vorwege bereits im Klaren gewesen zu sein. Hierauf schließen lässt einerseits die heimliche Weitergabe und andererseits die Notwendigkeit äußerer Legitimation für die eigene

Weiterbearbeitung des Objektes Cyberwar. Entsprechend scheint es, dass das BMVg die hier in diesem Dokument unternommene Formung als eine Reaktion auf eine Aufforderung des BMI, artikuliert als Auftrag in der *CSS 2011*, verstanden wissen möchte. Insofern bewegt sie sich auch bezüglich der Objektformung scheinbar in den Grenzen des vom BMI kommenden Definitionsrahmens, den sie selbst nicht bilden muss. Andererseits zielt der direkte Verweis auf die *VPR 2011* darauf, deutlich zu machen, dass es sich bei dieser Formung insgesamt lediglich um eine Erfüllung eines selbst gesetzten Auftrags handelt. Beides zusammen kann als eine doppelte Strategie der Rechtfertigung für das eigene Handeln am Objekt gelesen werden. Der Impuls für das Handeln wird in der ministerialen Umwelt verortet, ebenso sein Ziel und die zu nutzenden Erkenntnismittel - die Rechtmäßigkeit dieses Vorgehens selbst findet das BMVg in den früher gesetzten und anerkannten Richtlinien.

Die anschließende Skandalisierung dieses Dokumentes im öffentlichen, deutschen Kriegsdiskurs durch das Medienorgan Netzpolitik.de machen entsprechend deutlich, dass diese neue Formung des Cyberwar durch das BMVg nicht ohne Kritik von allen Teilhabern des Kriegsdiskurses als legitimer Schritt erachtet wird. Im Gegenteil: Im Anschluss der Veröffentlichung zeigt sich im Diskurs eine starke Häufung von Beiträgen, welche die Legitimität dieser Entscheidung grundsätzlich in Frage stellen.

Diese Ausgestaltung der Vorgaben "zur Entwicklung und Umsetzung von Grundsätzen für die Cyber-Verteidigung" (BMVg 2015) durch die *Strategische Leitlinie* werden explizit in Hinblick auf das *Weißbuch 2016* vorgenommen. Die Analyse der dortigen Präsentation des Cyberwars und der nun in das Handlungsfeld des BMVg und der Bundeswehr eingebundenen Cyber-Verteidigung folgt abschließend.

In Vorbereitung auf den Krieg der Zukunft: Das Weißbuch 2016

Abseits der Grenzen ministerialer Dokumente ist in den Jahren zwischen der *VPR 2011* und dem *Weißbuch 2016* (vgl. BMVg 2016a) viel geschehen. Wie vom BMVg selbst beschrieben handelt es sich bei einem Weißbuch um das "oberste sicherheits- und verteidigungspolitische Grundlagendokument der Bundesregierung" (Bundesregierung.de 2015). Entsprechend wird innerhalb des *Weißbuchs 2016* die sicherheitspolitische Agenda für die nächsten Jahre, wenn nicht Jahrzehnte, formuliert. Dargestellt werden die Grundzüge, Ziele und Rahmenbedingungen deutscher Sicherheitspolitik sowie die Lage der Bundeswehr und die Vorgaben für die Streitkräfte: "Das Weißbuch steht in der Hierarchie sicherheitspolitischer Grundlagendokumente an oberster Stelle,

gefolgt von den Verteidigungspolitischen Richtlinien (VPR)" (BMVg.de 2015b).
Die deutsche Bundesregierung begann offenbar spätestens 2015 mit dem Aufbau eines eigenen "*militärischen Organisationsbereiches*" der Bundeswehr, welcher den "*Cyber- und Informationsraum*" entsprechend abdecken soll (vgl. BMVg 2016b: 1; vgl. auch Deutschlandfunk.de 2015). Der definitorische Wandel, wie er im vorherigen Kapitel dargelegt wurde, schlägt sich somit auch praktisch in der Struktur des BMVg und der Bundeswehr nieder. Zwar bestanden bereits vorher einzelne Cyber-Einheiten innerhalb der bereits bestehenden Teilstreitkräfte (vgl. Zeit.de 2015, Heise.de 2014, Spiegel.de 2009), doch mit der bereits in der Einleitung beschriebenen offiziellen Verkündung der neuen, fünften Teilstreitkraft durch das Bundesministerium für Verteidigung im April 2016 wurde die Bearbeitung dieser neuen Bedrohungslage organisatorisch auf das höchstmögliche Niveau gehoben. Die Bearbeitung des Cyberwars wird hierdurch zum wichtigen Bestandteil der Neugestaltung der gesamten deutschen Sicherheits- und Verteidigungspolitik. Eine steile Karriere, schließlich hat sich der öffentliche Diskurs um den sogenannten Cyberwar erst seit der großflächigen Verbreitung des Internets in den 1990ern entwickelt.

Das *Weißbuch 2016* ist von Beginn an geprägt durch das Bild eines unberechenbaren, dynamischen Weltgefüges, worauf bereits der erste Satz der Einleitung von Bundeskanzlerin Angela Merkel hinweist:

> *Die Welt im Jahr 2016 ist eine Welt in Unruhe. Auch in Deutschland und Europa spüren wir die Folgen von Unfreiheit, Krisen und Konflikten in der unmittelbaren Nachbarschaft unseres Kontinents. Wir erleben zudem, dass selbst in Europa Frieden und Stabilität keine Selbstverständlichkeit sind.* (BMVg 2016: 6)

Die Verortung dieser "Unruhe der Welt" entlang einer *Nah-bis-fern-Achse* ist bereits aus der *VPR 2011* bekannt, ebenso auch die kreisförmig verlaufende Unterteilung der territorialen Gebiete von der Kategorie 'Deutschland' aus über 'Europa' bis in die sogenannte unmittelbare 'Nachbarschaft' als Stellvertreter für das nicht spezifizierte Andere, welches dem "Wir" gegenübersteht. Die Darstellung der sicherheitspolitischen Weltordnung erweist sich hier als überaus konsistent im Zeitverlauf. Entlang dieser Zuschreibungen wird ein Wirkungsverhältnis zwischen dem Wir und der Nachbarschaft aufgespannt, welches über die Grenzen des Wir in dessen Raum hineinwirkt (vgl. ebd.: 6). Der „Konflikt im Cyberraum" (ebd.: 6) dient im Weißbuch als nützliches Kategorisierungsinstrument, um die Zustände aus der Peripherie in den Raum des *Wir* hineinzutragen, ist er doch selbst „grenzenlos" (ebd.: 37). Dabei wird erklärt, dass es sich bei Angriffen aus und im Cyberraum

„schon lange" nicht mehr um „Fiktion" handelt, sondern um „Realität" (ebd.: 37). Dies macht erneut die Karriere des Cyberwars im Diskurs, von einer bloßen Potentialität zur längst erkannten Realität, offensichtlich. Mit Bezug auf das Objekt Cyberwar wird deutlich, wie groß der Unterschied in der Bedeutung, die ihm zugeschrieben wird, geworden ist: Innerhalb der *VPR 2011* war der Cyberwar bereits als eine von vielen möglichen Gefahren, welche die Infrastruktur Deutschlands schädigen können, anerkannt und die Informationsinfrastruktur als kritische Infrastruktur eingeordnet worden, wodurch eine allgemeine Zuständigkeit konstruiert wurde. Doch im *Weißbuch 2016* ist die Stellung des Themenfeldes Cyberwar wesentlich prominenter. Das zeigt sich darin, dass die Digitalisierung mitsamt der Globalisierung als entscheidender „Treiber des Umbruchs" (ebd.: 28) kategorisiert wird, also als einer von insgesamt nur zwei Faktoren, welche die eingangs eingeführte Unruhe der Welt überhaupt erst hervorgebracht haben (vgl. ebd.: 28ff.). Verstanden als „politische[n], ökonomische[n] und technologische[n] Verflechtung" (ebd.) auf der Ebene der „Lebensbereiche" werden beide zur Ursache von „gesellschaftlichen und sozialen Wandlungsprozessen" (ebd.) ausgearbeitet. Das Verständnis vom Cyberraum und seinen Gefahren, wie es erstmalig in der *CSS 2011* formuliert und von der *SL 2015* sichtbar übernommen wurde, wird hier erneut eingesetzt:

> *Die sichere und gesicherte sowie freie Nutzung des Cyber- und Informationsraums ist elementare Voraussetzung staatlichen und privaten Handelns in unserer globalisierten Welt. Die wachsende und sämtliche* Lebensbereiche *durchdringende Digitalisierung mit ihrer fortschreitenden Vernetzung von Individuen, Organisationen und Staaten prägt in einzigartiger Weise die Chancen unserer Gegenwart und Zukunft. Sie macht Staat, Gesellschaft und Wirtschaft jedoch zugleich besonders verwundbar für Cyberangriffe und erfordert unmittelbare Gefahrenabwehr.* (ebd.: 36, Herv. durch die Autor_innen)

Das Bild der gesellschaftlichen Lebensbereiche, die durch Cyberangriffe existenziell bedroht werden, setzt sich erkennbar fort. Es ist beachtenswert, dass mit dem Begriff Informations- und Cyberraum sowohl der Formulierung der *VPR 2011* als auch der *CSS 2011*, und damit der *SL 2015*, Rechnung getragen wird. Die dabei bereits in der *CSS 2011* eingebrachte Figur der einseitigen Abhängigkeit bleibt dabei in der Verknüpfung der Kategorien sichtbar erhalten:

> *Eine Unterbrechung des Zugangs zu [...] globalen öffentlichen Gütern zu Lande, zur See, in der Luft sowie im Cyber-, Informations- und Weltraum birgt erhebliche Risiken für die*

Funktionsfähigkeit unseres Staates und den Wohlstand unserer Bevölkerung. (BMVg 2016: 41)

Dies markiert die zukünftige Relevanz der sicherheits- und verteidigungspolitischen Arbeit an diesem Objekt, welches wohl scheinbar nicht mehr aus der Sicherheits- und Verteidigungspolitik weggedacht werden kann. Der Cyberraum wird dementsprechend im *Weißbuch 2016* in einer Reihe mit den bis dato existierenden Dimensionen des Krieges genannt.

Das Dokument leistet also in Bezug auf den Cyberwar und das ihn tragende Wirklichkeitsbild einiges. Der Cyberraum tritt als militärisches Operationsfeld zu denjenigen im physischen Raum hinzu, was bedeutet, ihn zum legitimen Einsatzgebiet der Bundeswehr zu erklären. Und tatsächlich findet sich im *Weißbuch* eine breite Darstellung von hierfür zukünftig bereitgestellten Personal- und Sachmitteln (vgl. ebd.: 118ff.). Diese Bewegung hatte sich auch bereits in der *SL 2015* und in ihrer Diskussion im Kriegsdiskurs angekündigt. Der Cyberraum als Ort zukünftiger Entwicklung birgt, so beschreibt es das *Weißbuch 2016,* neben den bisher bekannten noch vielerlei unbekannte Gefahren, welche gegenwärtig noch nicht antizipiert werden können. Sicherheits- und Verteidigungspolitik ist und wird somit auf lange Sicht "komplexer, volatiler sowie dynamischer und damit immer schwieriger vorhersehbar" (ebd.: 28). Die hier über den Kategoriengebrauch produzierte Norm offenbart sich in der Erwartung an die eigene Institution, weiter aufmerksam und gestaltend tätig zu sein, enthält aber ebenso auch eine indirekte Aufforderung an den deutschen Staat, diese Anpassungsmaßnahmen zu finanzieren. Das Bild eines zukünftigen Krieges im Internet mit bisher noch nicht vorstellbaren Technologien ist im Jetzt strategisches Mittel den Modus Operandi am Laufen zu halten oder auszuweiten. Dies wiederum steht im breiteren Kontext der Herstellung von Legitimation und Akzeptabilität für die getroffenen und noch zu treffenden politischen Entscheidungen (vgl. Lucke 1996). Es bleibt also zu erwarten, dass der hier formulierte Anspruch an die eigene Institution auch in Zukunft zur Legitimation weiterer Aus- und Umformungen genutzt wird.

Die unsichtbare Gefahr als Quelle unendlicher Formung: Eine Diskussion

In nur knapp einem Jahrzehnt (2007-2016) ist der Cyberwar zu einer ernstzunehmenden Bedrohung geworden, welche über ihre eigene Wirklichkeitsdimension verfügt, abgedeckt durch eine sich gegenwärtig im Aufbau befindliche Teilstreitkraft der Bundeswehr. Und all dies konnte erreicht werden, ohne dass die tatsächlichen technischen Möglichkeiten, politischen Ziele

> In der gegenwärtigen Darstellung des Cyberwars wird eine auffällige **Unterbestimmtheit** dieses Themenkomplexes erkennbar.

und entstehenden Kosten dieser neuen Kriegsführung bis heute wirklich klar ersichtlich scheinen. Diese Erkenntnisse sollen im Folgenden diskutiert werden.

Die nützliche Unterbestimmtheit des Cyberwars

In der gegenwärtigen Darstellung des Cyberwars wird eine auffällige Unterbestimmtheit dieses Themenkomplexes erkennbar. Diese Unterbestimmtheit lässt sich entlang zweier Bedingungen erklären: Erstens scheint es, dass aufgrund der potentiellen Geheimhaltung von Informationen nicht alle am Diskurs beteiligten Akteure über den gleichen Wissensstand verfügen beziehungsweise den gleichen Zugang zu Informationen haben (vgl. Heise.de 2015). Viele Beiträge im öffentliche Diskurs bewegen sich aufgrund dieser Einschränkungen partiell im Raum von Spekulationen. Dies trifft auch auf diesen Artikel zu. Die im Diskurs hervorgebrachten Aussagen konnten bislang in ihrem Wahrheitsgehalt immer nur nachträglich durch die Teilnehmerinnen und Teilnehmer validiert werden, wenn überhaupt. Beispielhaft hierfür sind die streitbaren Aushandlungen um die öffentliche Zuschreibung und administrative Selbstzuschreibung von Operationen im Cyberraum. Ein prominenter Fall hiervon ist die Auseinandersetzung mit dem Fall Stuxnet (vgl. z.B. Nzz.ch 2010, Zeit.de 2010, Gayken 2010, Zeit.de 2011, Deutschlandradio.de 2012). Diese Kämpfe und ihre Folgen sind potenziell brisant, da durchaus davon ausgegangen wird, dass auch im neuen Operationsfeld Cyberraum der NATO-Bündnisfall eintreten kann (vgl. Heise.de 2016b, Zeit.de 2016, Deutschlandfunk.de 2016, Spiegel.de 2016).

Zweitens scheint es, dass die grundlegenden Eigenschaften des diskursiven Objektes Cyberwar in den aktuell hervorgebrachten Definitionsversuchen, etwa durch die Bundesregierung, ganz bewusst nicht abschließend definiert werden, fehlt es doch nicht allein an Wissenzugängen, sondern auch an Wissen überhaupt. Was also genau der Cyberwar ist, scheint bis dato aus gutem Grund nicht geklärt. Dies zeigt sich in der aktuellsten Darstellung der Cyberbedrohungslage durch das Bundesinnenministerium:

> *Die Folgen von Cyber-Angriffen beschränken sich nicht auf den*

> *Cyber-Raum. Erfolgreiche Angriffe können gesellschaftliche, wirtschaftliche, politische und auch persönliche Schäden verursachen. [...] Die Angreifer haben vielfach einen kriminellen, extremistischen/terroristischen, militärischen oder nachrichtendienstlichen Hintergrund. Die quantitative und qualitative Vielfalt der potenziellen Akteure aus dem In- und Ausland und der technischen Möglichkeiten zur Verschleierung erschweren die Erkennung, Zuordnung, Abwehr und Verfolgung von Cyber-Angriffen. [...] Dies erschwert die politische Bewertung von Cyber-Angriffen und die Entscheidung über die gebotenen Gegenmaßnahmen*. (Bundesministerium des Inneren 2016: 7)

Im Kriegsdiskurs gilt es, Kriegshandlungen als solche zu erkennen, adäquat zuzuordnen, ihr Schadenspotenzial abzuschätzen, sie abzuwehren und sie von anderen Handlungsformen wie etwa Kriminalität, Terrorismus oder auch Aktivismus abzugrenzen. Dass diese Schritte mit Erfolg vollzogen werden, ist jedoch aufgrund der technischen Eigenschaften des Cyberwars als informations-technologisch geführter Krieg offenbar nicht abschließend zu gewährleisten, wie obiges Zitat verdeutlicht. Weiterhin ist bislang in der juristischen Behandlung des Objektes Cyberwar nicht ausreichend definiert, was in diesem Kontext überhaupt eine Waffe, ein Akteur, ein staatliches Hoheitsgebiet oder eine kriegerische Handlung sein kann (vgl. Netzpolitik.org 2015, Netzpolitik.org 2016a, Heise.de 2015, Nzz.ch 2014, Gayken 2011, Chiesa 2010, Wegener 2009). Wie in einigen Diskursbeiträgen offensichtlich wird, steht zudem nicht fest, ob hier abschließende Definitionen überhaupt realisierbar sind (vgl. Netzpolitik.org 2015, Chiesa 2010). Was sich hier im Diskurs darstellt, ist das Fehlen angemessener epistemischer Mittel, mit welchen für den praktischen Gebrauch haltbares Wissen generiert und einem Katalog juristischer Definitionen zugeordnet werden kann. Der Leserin drängt sich hier das Bild des "unbekannten Unbekannten" auf, welches der ehemalige U.S.-amerikanische Verteidigungsminister Donald Rumsfeld im Vorfeld der völkerrechtswidrigen Invasion des Irak prominent geprägt hat (vgl. Rumsfeld 2009). Dass ein solch fragiles diskursives Objekt inzwischen zum festen Bestandteil sicherheits- und verteidigungspolitischer Diskussionen und zum Beweggrund für die Einrichtung einer neuen Teilstreitkraft geworden sind, ist somit keineswegs selbstverständlich.

Die Karriere des Cyberwars hin zur „existenziellen" Bedrohung

Dennoch scheint es offensichtlich, dass der Cyberwar auch jenseits endgültiger Definitionen sinnvoll innerhalb des Kriegsdiskurses eingesetzt werden kann. Es ist

zu vermuten, dass ein wichtiger Grund hierfür in seiner Nutzung zum Legitimationsgewinn zu finden ist. Harvey Sacks (1996: 205ff.) hat mehrfach illustriert, wie Normen im Sprachgebrauch zu wichtigen Operateuren für das unmerkliche Verstehen von Aussagen werden können, und umgekehrt, wie bestimmte Normen über Aussagen eingesetzt werden können. Die "moralische Ordnung" (Bergmann 2010: 160) des Kriegsdiskurses, welche über das Bild des Cyberwars aufgeworfen und erneuert wird, mit ihrer ganz eigenen Logik von Freund und Feind, Sicherheit und Gefahr, zeigt sich hier als wichtiges Mittel in der Umgestaltung der deutschen Bundeswehr. Diese ist hierdurch zwar nicht vollständig unabhängig, aber doch zum gewissen Grade befreit von den einzelnen Präzedenzfällen und der faktischen Wahrscheinlichkeit seines wirklichen Eintretens. Die Unabschätzbarkeit des Angriffs und seiner Wirkung ermöglicht hier den Aufbau von wirkmächtigen Bedrohungsszenarien. In der Einzelanalyse der Dokumente sind die vielen Verbindungspunkte zwischen den vier gewählten Materialstücken ersichtlich geworden. Der inzwischen erreichte Stand seiner Zuwendung, also das Einrichten einer fünften Teilstreitkraft der Bundeswehr und die inzwischen offen geführte Diskussion um den Aufbau eigener offensiver Fähigkeiten erscheint als Ergebnis einer außergewöhnlich kreativen Kombinationsarbeit von ministerial hervorgebrachtem Wissen am Objekt Cyberwar. Die *CSS 2011* und die *SL 2015* können hier als entscheidende Zwischenschritte verstanden werden auf dem Weg des Objekts von seiner initialen Anerkennung als sicherheits- und verteidigungspolitisch relevanter Gefahrenquelle in der *VPR 2011* bis zu seinem institutionellen Niederschlag als Teilstreitkraft in der Organisationsstruktur der Bundeswehr, dargestellt im *Weißbuch 2016*. Anhand der als Präzedenzfälle anerkannten Ereignisse, dem Angriff auf Estland 2007 und der Stuxnet-Attacke 2010, konnte der Cyberwar zu einer realen und vor allem existenziellen Bedrohung moderner Gesellschaften gemacht werden, als deren bedrohter Teil und deren Schützer zugleich sich das BMVg und die Bundeswehr verstehen.

Der Cyberwar als „unkalkulierbares Risiko" moderner Kriegsführung

Diese Karriere des Objekts Cyberwar ist eng verknüpft mit der dargestellten Notwendigkeit zur Antizipation bisher unbekannter Gefahren und ihrer Umwandlung in ein im Jetzt zu bearbeitenden Risiko als institutionelle Reaktion zur Schaffung von Ordnung beziehungsweise Sicherheit. Einerseits bleibt festzuhalten, dass die spezifischen Eigenschaften des Cyberwars, wie sie bis hierhin behandelt wurden, die sicherheitspolitischen Akteure auf der Seite von Staaten offensichtlich vor

erhebliche operative und kommunikative Schwierigkeiten stellen. Der Cyberwar kann theoretisch den „new wars" (Broska 2004: 107), dem „asymmetrischen Krieg" (Winter 2011: 1) oder dem „hybriden Krieg" (Münkler 2015: 1) zugeordnet werden. Zu diesen Kategorien werden Konflikte gerechnet, welche im Zusammenspiel von Globalisierung, Staatenverfall, neuen Technologien und der teilweisen Privatisierung von Gewalt entstehen können. Die Grenzen der klassischen Kriegsführung zwischen Staaten verwischen und verlaufen parallel oft unterhalb der Schwelle dessen, was definitorisch international als Krieg bezeichnet wird (vgl. Broska 2004: 107ff.). Herfried Münkler (2015: 4) sieht dabei besonders den Begriff des hybriden Kriegs, zu welchem er auch Angriffe aus dem Cyberraum rechnet, als „semantischen Stempel [...] sicherheitspolitischen 'Durchwurstelns'", als Anzeichen für das Fehlen einer adäquaten Terminologie, mit welcher moderne Kriege klassifiziert werden können. Trotz derartiger Probleme sind Staaten, wie Ulrich Beck (2007: 32, 63) herausstellt, verpflichtet im Angesicht neuer Bedrohungen Sicherheit herzustellen und zu gewährleisten. Die Herausbildung adäquater Ankerpunkte für ihre Maßnahmen zur gesamtstaatlichen Sicherheitsvorsorge ist somit von hoher Relevanz für die Praxis des Regierens. Benötigt werden Mechanismen der kommunikativen Handhabung, welche Gefahren bearbeitbar machen, die sich dadurch auszeichnen, dass sie in erster Linie unsichtbar bzw. nicht auf allen erforderlichen Ebenen (er)fassbar sind.

Mit Becks Risikotheorie wird erkennbar, dass nicht mehr die akute Gefahr das alleinige Paradigma des sicherheitspolitischen Regierens ist, sondern die Antizipation der Ausnahme bzw. des Risikos - also von unbekannten oder unkalkulierbaren Bedrohungen (vgl. ebd.: 81ff., 211ff.). Dies scheint augenscheinlich für den Cyberwar im Besonderen zu gelten, da dieser sowohl reale, definitorische als auch legale Unbestimmtheiten aufweist. Als scheinbare Lösung wird nach Beck sicherheitspolitisch das Prinzip der akuten Gefahrenabwehr und Kompensation um das Prinzip der Vorsorge erweitert (vgl. ebd.: 217f.). Beck unterscheidet den Diskurs über basale Bedrohungen und Unsicherheiten von einer "Semantik des Risikos", die sich durch eine „gegenwärtig[e] Thematisierung zukünftige[r] Gefahren" auszeichnet, welche in Folge der Erfolge der Zivilisation selbst entstehen und durch die Modernisierung zunehmend an Bedeutung gewinnen (ebd.: 19). Im Denkmodell des Risikos werden Chance und Gefahr als untrennbare Begleiterscheinungen von technischer Entwicklung, als unabschätzbare Nebenfolgerisiken, in die Welt gebracht, welche weitere technologische Entwicklungen notwendig machen um diese zu bearbeiten (vgl. ebd.: 19ff.). Treten Risiken ein, werden sie zur (gesellschaftlichen) Katastrophe: „[S]ie vergegenwärtigen einen Weltzustand, den

es (noch) nicht gibt." (Beck 2007: 29) Ein besonderes Moment des Risikos besteht dabei darin, dass Unsicherheit nicht nur über die Antizipation der Katastrophe selbst, sondern parallel auch durch das Nicht-Wissen bezüglich der Validität des Risikos selbst hervorgerufen wird. Wissen und Nicht-Wissen können somit nicht klar getrennt werden (vgl. ebd.: 21f.). Es bedarf daher der „inszenierte[n] Antizipation" als psychologischer Notwendigkeit, durch welche eine antizipierte Katastrophe als Risiko in der Gegenwart als bearbeitbar dargestellt werden kann (ebd.: 32). Die „Definitionsverhältnisse" von Risiken können daher bei Beck als "Herrschaftsverhältnisse der Risikoinszenierung" begriffen werden (ebd.: 55).

Der Cyberwar als Mittel zum „Undoing" klarer Grenzziehungen

Diese Betrachtungsweise lässt sich auch mit den vielbeachteten Analysen Giorgio Agambens (2014) zum Ausnahmezustand verknüpfen. Agamben geht hier von der Annahme einer qualitativen Steigerung des Ausnahmezustands zu einem "herrschende[n] Paradigma des Regierens" in der Gegenwart aus (Agamben 2014: 9). Dieses ermöglicht das Handeln von sicherheitspolitischen Akteuren in der Abwesenheit klarer Rechtsdefinitionen, welches mit dem Schutz einer gegebenen "gültigen Ordnung" (ebd.: 41) gerechtfertigt und ausgeformt wird (vgl. ebd.: 11ff.). Dass der Ausnahmezustand potentiell zum Paradigma des Regierens werden kann, erklärt Agamben über die Annahme einer Transzendierung des Ausnahmezustands in einen Modus des zukünftigen "weltweite[n] Brügerkrieg[s]" (ebd.: 9), was klare Ähnlichkeiten zu dem in den Dokumenten sichtbaren Undoing von Grenzen aufweist und Ähnlichkeiten mit Münklers (2015: 1) Gegenwartsdiagnose einer Auflösung der Trennlinie zwischen Krieg und Frieden birgt. Dies bedeutet, dass sich die auf Dauer gestellte Antizipation des Ausnahmezustands bei Agamben als ein konstitutives Moment für die Rechtsordnung selbst gerieren kann (vgl. Agamben 2014: 13). Folglich ist es möglich, dass Maßnahmen von Regierungen getroffen werden, welche auf die Abwehr von Gefahren zielen, die im Falle des erhofften Funktionierens der Maßnahmen gar nicht erst eintreten, wobei die Beweisführung des Erfolgs besagter Maßnahmen sich in der Regel als unmöglich darstellt. Parallel erkannte Agamben, dass in dieser Antizipation des zukünftigen Ausnahmezustands eine Handlungsaufforderung an entsprechende exekutive Sicherheitsorgane eingebettet ist, derer diese sich nicht entziehen können. Was Agamben (2014: 41) als den "Notstand als Lücke" beschreibt, ist die Trajektorie der präventiven Risikoabwehr und der Antizipation von Risiken als Paradigma für sicherheitspolitisches Handeln. Diese Umstände zeigen sich auch in den

Dokumenten durch die aktive Darstellung der Gefahren als beinahe unmöglich absehbar und die dennoch vertretene Aufforderung ständiger Wachsamkeit und Entwicklung. Doris Lucke beschreibt diese Inszenierung mit Bezug auf die hier angesprochene Herstellung von Legitimität als ein Dilemma, insofern:

> *Entscheidungen über Akzeptierbarkeit und faktische Akzeptanz, z.B. bei neuen Technologien oder Bundeswehreinsätzen, immer kurzfristiger und im konkreten Fall schneller getroffen werden [müssen]. Dies kann oft nur unter Akzeptanz des Negativ-Ziels „akzeptabilisierter" (Rest-)Risiken oder über Verträglichkeitsanalysen als erträglich definierter Grade an Bedrohung und Unsicherheit geschehen.* (Lucke 1996: 475)

Der Cyberwar als „Call for Action"

Yves Winter (2011) hat sich in einer ethnomethodologischen Untersuchung der Kommunikationspraktiken von Regierungen mit dem diskursiven Umgang mit dieser Kriegsform auseinandergesetzt. Winters besonderer Fokus liegt dabei auf den Möglichkeiten bzw. Richtungen der Transformation des Objektes *asymmetrischer Krieg* sowie den daran anknüpfenden politischen Handlungen, welche durch die Bearbeitung des Objektes ermöglicht bzw. erschlossen werden. Das Besondere des asymmetrischen Krieges, so zeigt Winter auf, liegt in der Vielzahl von Unterkategorien von Konflikten, welche über ihren Sammelbegriff in einer singulären diskursiven Konstellation bearbeitbar gemacht werden (vgl. ebd.: 488ff.). Die offensichtliche Unschärfe des Begriffs des asymmetrischen Kriegs erweist sich nach seiner Betrachtung als ein Vorteil für sicherheitspolitische Akteure zur Einordnung und Handbarmachung dieser Konflikte. Ähnlich ließe sich auch für das Objekt Cyberwar argumentieren, dass es in der Weise seiner Formung viele Vorteile birgt. Es besticht in ähnlicher Weise durch einen fließenden Übergang von Devianz im Cyberraum, über Cyber-Kriminalität, -Spionage, -Terrorismus bis hin zu -Krieg. Winter zeigt auf, wie die Kategorisierung des asymmetrischen Kriegs eine Re-Interpretation von bestehenden Definitionen ermöglicht, welche von Sicherheitsakteuren geleistet werden kann, um die Grundlage für die Ausführung von sicherheitspolitischen Operationen zu schaffen (vgl. ebd.: 492ff.). In gleicher Weise lässt sich argumentieren, dass die besondere Kategorisierung des Cyberwar, welcher dem asymmetrischen Krieg untergeordnet werden kann, es zulässt, ein breites Maß an Handlungen aus seinem Bestehen folgern zu können. Die Breite dieses kategorialen Möglichkeitsraums zeigt sich in der Einführung der fünften Teilstreitkraft der Bundeswehr. Eine weitere zentrale Praxis, die Winter aufdeckt,

ist das Phänomen der "asymmetric moral economy" (Winter 2011: 490):

> *I use this term to designate a peculiar feature of the asymmetric war discourse, the tendency to portray powerful states as weak and vulnerable victims of dangerous non-state actors.* (ebd.: 490)

Diese von Winter herausgestellten Tendenzen innerhalb der Bearbeitung des asymmetrischen Krieges spielen wie in der Dokumentenanalyse herausgearbeiteten Verletzbarkeit der Gesellschaft offensichtlich auch innerhalb des deutschen Kriegsdiskurses eine bedeutsame Rolle. Diese Verletzlichkeit kann als moralischer Auftrag zur Bearbeitung des Cyberwar interpretiert werden, welcher über den Einsatz der Kategorien gefertigt wird. Entsprechend findet der Cyberwar im untersuchten Prozess nicht nur eine bis dahin nicht gekannte institutionelle Anerkennung, sondern wird innerhalb des *Weißbuchs 2016* zu einem der wichtigsten Argumente für den Umbruch von der bisherigen Nachkriegsordnung hin zu einer neuen, ungewissen Sicherheitslage, welche einer gut gerüsteten Bundeswehr bedarf (vgl. BMVg 2016a: 6). Das BMVg inszeniert sich und die Bundeswehr als notwendige Größe und sieht sich doch gleichzeitig in seiner Selbstzuschreibung als verletzbaren gesellschaftlichen Lebensbereich. Die Rahmung der eigenen Verwundbarkeit stellt somit eine Praxis dar, welche notwendige Ankerpunkte für Bedrohungen schafft, um anschließend über die Antizipation des möglichen Schadens eine sicherheitspolitische Bearbeitung zu ermöglichen bzw. eine Eskalation bereits bestehender sicherheitspolitischer Maßnahmen zu fordern, wie Winter nahelegt (vgl. Winter 2011: 490).

Fazit

Die Entwicklung des hier untersuchten Objektes Cyberwar ist mit Blick auf die diskutierten Theorien als ein Fall moderner Regierungsarbeit erkennbar geworden und lässt sich im Rahmen des gegenwärtigen sozialwissenschaftlichen Diskurses einfassen. Der Cyberraum, welcher nicht von den für die Herstellung von Sicherheit relevanten Grenzen abhängt, wird ein Konfliktgebiet, in welchem Unterscheidungen zwischen Kombattant und Zivilist, innerer und äußerer Sicherheit, Kriegsakt und krimineller Handlung, abseits klassischer Definitionen aus der Rechtspraxis, potenziell verhandelbar gemacht werden können. Da die Informationsinfrastrukturen und der sich zwischen diesen aufspannende Cyberraum als für die gesellschaftlichen Lebensbereiche inzwischen existenziell notwendig befunden werden, wird diese Quelle verteidigungspolitischer Bearbeitung auf absehbare Zeit nicht versiegen.

> Im Fall Cyberwar konnte beobachtet werden, wie **Sicherheit und Unsicherheit** im politischen Verfahren der Positionserarbeitung über die kategoriale Arbeit an Definitionen gleichzeitig kommunikativ hergestellt werden.

Generell wird die wichtigste Arbeit in den strategischen Positionspapieren der Bundesregierung zum Cyberwar zu großen Teilen über Erweiterungen und Ausdifferenzierung bereits veröffentlichter legitimer Definitionen und Perspektiven geleistet. Diese Interpretationsarbeit und ihre Sichtbarmachung für beobachtende Akteure stellen somit eine zentrale Praxis von Sicherheitsakteuren da, um das Durchsetzen von Neuerungen innerhalb der politischen Sphäre überhaupt erst legitimierbar zu machen. Im Fall Cyberwar konnte beobachtet werden, wie Sicherheit und Unsicherheit im politischen Verfahren der Positionserarbeitung über die kategoriale Arbeit an Definitionen gleichzeitig kommunikativ hergestellt werden. Paradoxerweise scheint es, als könnte Sicherheit nicht abschließend erreicht werden ohne die kategoriale Konstruktion von Risiken, durch welche eine Notwendigkeit zur Bearbeitung durch Sicherheitsakteure konstant hergestellt und somit das Erreichen von Sicherheit verunmöglicht wird.

LITERATUR

Agamben, Giorgio (2014): Ausnahmezustand: Homo sacer II.1. Frankfurt am Main: Suhrkamp.

Beck, Ulrich (2007): Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit. Frankfurt am Main: Suhrkamp.

Bergmann, Jörg (2010): Die kategoriale Herstellung von Ethnizität - Ethnomethodologische Überlegungen zur Ethnizitätsforschung. In: Müller, Marion/Zifonun, Darius (Hrsg.), Ethnowissen: Soziologische Beiträge zu ethnischer Differenzierung und Migration. Wiesbaden: Springer VS, S. 155-169.

Blatter, Joachim (2007): Demokratie und Legitimation. In: Benz, Arthur/Lütz, Susanne/Schimank, Uwe/Simonis, Georg (Hrsg.): Handbuch Governance. Theoretische Grundlagen und empirische Anwendungsfelder. Wiesbaden: Springer VS, S. 271-284.

Bundesministerium der Verteidigung (BMVg.de) (2003), Mai 2003: Verteidigungspolitische Richtlinien für den Geschäftsbereich des Bundesministeriums der Verteidigung. URL: http://www.ndh.net/home/kuvoss/mi_vpr-2003.pdf (15.11.2018).

BMVg.de (2006), Oktober 2006: Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr. Online verfügbar unter: http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/weissbuch_2006.pdf (14.11.2018).

BMVg.de (2015b), 18.12.2015: FAQ. Weißbuch 2016, Online verfügbar unter: https://www.bmvg.de/de/themen/weissbuch/faq (14.11.2018).

BMVg.de (2016b) April 2016: Abschlussbericht Aufbaustab Cyber- und Informationsraum. Online verfügbar unter: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf (14.11.2018).

Bundesministerium des Inneren (BMI) (2016), November 2016: Cyber-Sicherheitsstrategie für Deutschland 2016. Online verfügbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (14.11.2018).

Bundesregierung.de (2015), 18.02.2015: Deutsche Sicherheitspolitik neu definieren. Weißbuch 2016. Online verfügbar unter: https://www.bundesregierung.de/Content/DE/Artikel/2015/02/2015-02-17-weissbuch-2016.html (15.11.2018).

Bundeszentrale für politische Bildung (2016), 21.10.2016: Sicherheit im Cyberspace. Online verfügbar unter: http://www.bpb.de/apuz/235533/sicherheit-im-cyberspace?p=all. (15.11.2018).

Broska, Michael (2004): 'New Wars' Discourse in Germany. In: Journal of Peace Research, Jg. 41/1, 2004, S. 107-117.

Chiesa, Roul (2010), 06.12.2010: Katz und Maus. Online verfügbar unter: http://www.theeuropean.de/raoul-chiesa/4879-kriegsfuehrung-im-internet (15.11.2018).

CNN (2016): Donald Trump vs Hillary Clinton full Hofstra debate. In: CNN.com, 26.09.2016. Online verfügbar unter: http://edition.cnn.com/videos/politics/2016/09/27/clinton-trump-hofstra-entire-first-presidential-debate-sot.cnn (15.11.2018).

Deutschlandfunk.de (2015), 11.11.2015: Bundeswehr: Aufrüsten für den digitalen Krieg. Online verfügbar unter: http://www.deutschlandfunk.de/bundeswehr-aufruesten-fuer-den-digitalen-krieg.676.de.html?dram:article_id=336566 (15.11.2018).

Deutschlandfunk.de (2016), 15.06.2016: NATO-Verteidigungsministertreffen: NATO erklärt Cyberspace zum Einsatzgebiet. Online verfügbar unter: http://www.deutschlandfunk.de/nato-verteidigungsministertreffen-nato-erklaert-cyberspace.1818.de.html?dram:article_id=357274 (15.11.2018).

Deutschlandradio.de (2012), 01.06.2012: Obama soll Stuxnet-Attacke befohlen haben. Online verfügbar unter: http://www.deutschlandradio.de/obama-soll-stuxnet-attacke-befohlen-haben.331.de.html?dram:article_id=207687 (15.11.2018).

Faz.net (2015), 17.09.2015: Verteidigungspolitik: Von der Leyen rüstet Bundeswehr für den Cyber-Krieg. Online verfügbar unter: http://www.faz.net/aktuell/bundeswehr-von-der-leyen-plant-cybereinheit-13808851.html (15.11.2018).

Garfinkel, Harold (1967): Studies in Ethnomethodology. Englewood Cliffs: Prentice-Hall.

Garfinkel, Harold/Sacks, Harvey (1990): On formal structures of practical action. In: McKinney, John/Tiryakian,

Edward (Hrsg.): Theoretical Sociology. New York: Appleton-Century-Crofts, S. 338-366.

Gayken, Sandro (2010), 26.11.2010: Stuxnet: Wer war's? Und wozu?. Online verfügbar unter: http://www.zeit.de/2010/48/Computerwurm-Stuxnet/komplettansicht (15.11.2018).

Gayken, Sandro (2011): Krieg der Rechner: Warum es so schwierig ist, sich vor militärischen Cyberangriffen zu schützen. In: Internationale Politik 2, S. 88-95.

Habermas, Jürgen (2015): Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Frankfurt am Main: Suhrkamp.

Heise.de (2014), 20.06.2014: Die deutschen Cyber-Krieger. Online verfügbar unter: https://www.heise.de/tr/artikel/Die-deutschen-Cyber-Krieger-2192518.html (15.11.2018).

Heise.de (2015), 17.12.2015: Beim Cyberwar-Wettrüsten herrscht gefährliche Geheimhaltung. Online verfügbar unter: https://www.heise.de/tp/features/Beim-Cyberwar-Wettruesten-herrscht-gefaehrliche-Geheimhaltung-3377215.html (15.11.2018).

Heise.de (2016a), 08.12.2016a: Cyberangriffe auf Parteien sollen sich zur Wahl 2017 häufen. Online verfügbar unter: https://m.heise.de/newsticker/meldung/Cyberangriffe-auf-Parteien-sollen-sich-zur-Wahl-2017-haeufen-3566172.html (15.11.2018).

Heise.de (2016b), 15.06.2016b: NATO: Cyberraum wird offiziell zum Operationsfeld. Online verfügbar unter: http://www.heise.de/newsticker/meldung/Nato-Cyberraum-wird-offiziell-zum-Operationsfeld-3238719.html?wt_mc=rss.ho.beitrag.atom (15.11.2018).

Hester, Stephen/Eglin, Peter (1997): Membership Categorization Analysis. An Introduction. In: Hester, Stephen/Eglin, Peter (Hrsg.): Culture in Action. Studies in Membership Categorization Analysis. Lanham: University Press of America Inc., S. 1-24.

Lucke, Doris (1996): Grenzen der Legitimation: zum Strukturwandel der Akzeptanz. In: Clausen, Lars (Hrsg.): Gesellschaften im Umbruch: Verhandlungen des 27. Kongresses der Deutschen Gesellschaft für Soziologie in Halle an der Saale 1995. Frankfurt am Main: Campus, S. 473-483.

Luhmann, Niklas (1969): Legitimation durch Verfahren. Neuwied am Rhein: Hermann Luchterhand.

Minkwitz, Olivier/Schöfbänker, Georg (2000), 31.05.2000: Information Warfare: Die neue Herausforderung für die Rüstungskontrolle. Online verfügbar unter: https://www.heise.de/tp/features/Information-Warfare-Die-neue-Herausforderung-fuer-die-Ruestungskontrolle-3447223.html (15.11.2018).

Münkler, Herfried (2015): Hybride Kriege: Die Auflösung der binären Ordnung von Krieg und Frieden und deren Folgen. Ethik und Militär 2015 (2). Online verfügbar unter: http://www.ethikundmilitaer.de/de/themenueberblick/20152-hybride-kriege/muenkler-hybride-kriege-die-aufloesung-der-binaeren-ordnung-von-krieg-und-frieden-und-deren-folgen/ (15.11.2018).

Netzpolitik.org (2015), 16.12.2015: Im Cyber-Raum gibt es keine Uniform: Bundesregierung ignoriert völkerrechtliche Probleme des Cyber-Krieges. Online verfügbar unter: https://netzpolitik.org/2015/im-cyber-raum-gibt-es-keine-uniform-bundesregierung-ignoriert-voelkerrechtliche-probleme-zum-cyber-krieg/ (15.11.2018).

Netzpolitik.org (2016a), 02.03.2016: Aktiv, passiv, responsiv: Cyberangriffe durch die Bundeswehr? Definitionssache. Online verfügbar unter: https://netzpolitik.org/2016/aktiv-passiv-responsiv-cyberangriffe-durch-die-bundeswehr-definitionssache/ (15.11.2018).

Netzpoltik.org (2016b), 02.09.2016: Schwarzbuch zur Bundeswehr kritisiert Militarisierung des Cyberraums und Drohnenaufrüstung. Online verfügbar unter: https://netzpolitik.org/2016/schwarzbuch-zur-bundeswehr-kritisiert-militarisierung-des-cyberraums-und-drohnenaufruestung/ (15.11.2018)

Nzz.ch (2008), 06.07.2008: Die Nato rüstet sich für den Krieg im Internet. Online verfügbar unter: https://www.nzz.ch/die-nato-ruestet-sich-fuer-den-krieg-im-internet-1.777626 (15.11.2018).

Nzz.ch (2010), 26.09.2010: Hier war ein Expertenteam am Werk. Online verfügbar unter: https://www.nzz.ch/hier_war_ein_expertenteam_am_werk-1.7689061 (15.11.2018)

Nzz.ch (2014), 12.12.2014: Krieg mit virtuellen Waffen: Geheimes Wettrüsten im Cyberspace. Online verfügbar unter: https://www.nzz.ch/meinung/kommentare/geheimes-wettruesten-im-cyberspace-1.18443493 (15.11.2018).

Nzz.ch (2015), 09.09.2015: Krieg in der fünften Dimension. Online verfügbar unter: https://www.nzz.ch/internatio-

nal/europa/krieg-in-der-fuenften-dimension-1.18609905 (15.11.2018).

Rawls, Anne (2002): Editors Introduction. In: Garfinkel, Harold (Hrsg.): Ethnomethodology's Program. Working out Durkheims Aphorism. Lanham: Rowman and Littlefield, S.1-64.

Rumsfeld, Donald (2009): Donald Rumsfeld Unknown Unknowns! In: Youtube, 07.08.2009. Online verfügbar unter: https://www.youtube.com/watch?v=GiPe1OiKQuk (26.02.2017).

Sacks, Harvey (1990): On the Analysability of Stories by Children. In: Gumperz, John/Hymes, Dell (Hrsg.): Directions in Sociolinguistics. The Ethnography of Communication. New York: Holt, Rinehart and Winston, S. 329-345.

Sacks, Harvey (1996): Lectures in Conversation. Volumes I & II. Oxford: Blackwell.

Scheffer, Thomas (2008): Zug um Zug und Schritt für Schritt. Annäherungen an eine transsequentielle Analytik. In: Kalthoff, Herbert/Hirschauer, Stefan/Lindemann, Gesa (Hrsg.): Theoretische Empirie. Frankfurt am Main: Suhrkamp.

Scheffer, Thomas (2012): Die trans-sequentielle Analyse – und ihre formativen Objekte. In: Hörster, Reinhard/Köngeter, Stefan/Müller, Burkhard (Hrsg.): Grenzobjekte. Soziale Welten und ihre Übergänge. Wiesbaden: Springer VS, S. 89-114.

Scheffer, Thomas (2015): Diskurspraxis in Recht und Politik. Trans-Sequentialität und die Analyse rechtsförmiger Verfahren. In: Zeitschrift für Rechtssoziologie, Jg. 35/2, S. 223-244.

Scheffer, Thomas (2017): Neuer Materialismus, praxeologisch – New Materialism, praxeologically. In: Behemoth – A Journal for Civilisation, Jg. 10/1, S. 92-106.

Scheffer, Thomas/Michaeler, Matthias/Schank, Jan (2008): Starke und Schwache Verfahren. Zur unterschiedlichen Funktionsweise politischer Untersuchungen am Beispiel der englischen „Hutton Inquiry" und des „CIA Ausschusses" der EU. In: Zeitschrift für Soziologie, Jg. 37/5, S. 423-444.

Sikora, Michael (2001): Der Sinn des Verfahrens. Soziologische Deutungsangebote. In: Zeitschrift für Historische Forschung, Beiheft 25, S. 25-51.

Silverman, David (1998): Harvey Sacks. Social Science and Conversation Analysis. Oxford: Polity Press.

Sowa, Aleksandra (2016), 11.08.2016: Der Kalte Krieg ist vorbei - es lebe der Kalte Cyber-Krieg! Online verfügbar unter: http://www.theeuropean.de/aleksandra-sowa--2/11205-die-us-wahl-die-cia-und-russland (15.11.2018).

Spiegel.de (2009), 07.02.2009: Bundeswehr baut geheime Cyberwar-Truppe auf. URL: http://www.spiegel.de/spiegel/vorab/a-606095.html (15.11.2018).

Spiegel.de (2016), 14.06.2016: Ministertreffen in Brüssel: NATO erklärt Cyberraum zum Kriegsschauplatz. Online verfügbar unter: http://www.spiegel.de/politik/ausland/nato-erklaert-cyberraum-zum-kriegsschauplatz-a-1097686.html (15.11.2018).

Stollberg-Rilinger, Barbara (2001): Einleitung. In: Zeitschrift für Historische Forschung, Beiheft 25, S. 9-24.

Wegener, Henning (2009): Der unsichtbare Feind. Im digitalen Raum sind die Angreifer den Verteidigern immer einen Schritt voraus. In: Internationale Politik, Jg. 9/10, S. 48-57.

Wikileaks.org (2016a), 22.07.2016a: Search the DNC email database. Online verfügbar unter: https://wikileaks.org/dnc-emails/ (15.11.2018).

Wikileaks.org (2016b), Oktober 2016b: The Podesta Emails. Online verfügbar unter: https://wikileaks.org/podesta-emails/ (15.11.2018).

Wimmer, Jeffrey (2007): (Gegen-)Öffentlichkeit in der Mediengesellschaft. Analyse eines medialen Spannungsverhältnisses. Wiesbaden: Springer VS.

Winter, Yves (2011): The asymmetric war discourse and its moral economies: a critique. In: International Theory, Jg. 3/3, S. 488-514.

Zeit.de (2010), 26.09.2010: Trojanerangriff: Hackerprogram Stuxnet attackiert Irans Atomanlage. URL: http://www.zeit.de/digital/2010-09/iran-stuxnet-trojaner (15.11.2018).

Zeit.de (2011), 18.01.2011: Cyberattacke: Israel und USA sollen Stuxnet entwickelt haben. Online verfügbar unter: http://www.zeit.de/digital/internet/2011-01/israel-usa-computerwurm (15.11.2018).

Zeit.de (2015), 16.09.2015: Bundeswehr: Die Cyberkrieger ordnen sich neu. Online verfügbar unter: http://www.zeit.de/politik/2015-09/cyberkrieg-bundeswehr-cyberkommando (15.11.2018).

Zeit.de (2016), 15.06.2016: Cyberwar: NATO erklärt virtuellen Raum zu Kriegsgebiet. Online verfügbar unter: http://www.zeit.de/politik/ausland/2016-06/cyberwar-nato-jens-stoltenberg-operationsgebiet (15.11.2018).

ANALYSEMATERIAL

Bundesministerium des Inneren (BMI) (2011): Cyber-Sicherheitsstrategie für Deutschland. In: bmi.bund.de, 02.2011. Online verfügbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (15.11.2018).

Bundesministerium der Verteidigung (BMVg) (2011): Verteidigungspolitische Richtlinien. In: bundesregierung.de, 27.05.2011. Online verfügbar unter: https://www.bmvg.de/resource/blob/13568/28163bcaed9f30b27f7e3756d812c280/g-03-download-die-verteidigungspolitische-richtlinien-2011-data.pdf (14.11.2018).

BMVg (2015a): Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg. In: netzpolitik.org, 16.04.2015. Online verfügbar unter: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/ (15.11.2018).

BMVg (2016a): Weißbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. In: bmvg.de, 13.07.2016. Online verfügbar unter: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (15.11.2018).

ZU DEN AUTOR_INNEN

Laurids Melbye hat Soziologie in Hamburg und Frankfurt am Main studiert. Seine Interessen zielen auf die Verbindung von Politik und Kunst in ethnographischer Forschung.

Julius Wörner hat an der Goethe-Universität in Frankfurt Soziologie/Politikwissenschaften (B.A.) und Soziologie (M.A.) studiert. Seine Interessen liegen insbesondere in Arbeits- und Organisationssoziologie, Sozialpsychologie und Ökonomie. Zum Thema Cyberwar ist er insbesondere durch seine BA-Arbeit: „Auf dem Weg zum western failed state? Überwachung vor dem Hintergrund der Weltrisikogesellschaft“ gekommen.

Der Beitrag wurde von **Maik Krüger**, **Ágnes Molnár** und **Claas Pollmanns** gereviewt und von **Tanja Strukelj** lektoriert.