# I. Einführung

## 1. Problemstellung und Erkenntnisinteresse

Als die damalige Verteidigungsministerin Ursula von der Leyen im April 2016 offiziell die Aufstellung eines militärischen Organisationsbereiches »Cyber- und Informationsraum« ankündigte, überschlugen sich die Meldungen in den deutschen Medien und reichten von der Aufstellung einer »Cyberarmee« für den »Cyberwar« bis zu Plänen zur »digitalen Kriegsführung«. Gleichzeitig machten sie deutlich, dass Deutschland unter europäischen und transatlantischen Partnern eher als Nachzügler angesehen werden konnte.[1] Die Erhebung des Cyberraumes zu einem eigenen militärischen Handlungsraum auf dem NATO-Gipfel von Warschau im Juli 2016 könnte auf den ersten Blick höchstens im Falle Deutschlands in einem zeitlichen Zusammenhang mit dem beginnenden Aufbau militärischer Fähigkeiten gesehen werden. Während die deutsche Verteidigungsministerin die Aufstellung eines eigenen Kommandos ankündigte, hatte ihr US-amerikanischer Amtskollege Ashton Carter bereits Anfang 2016 dem sogenannten Islamischen Staat den »Cyberwar« erklärt und konnte dazu auf das im Jahre 2009 aufgestellte U.S. Cyber Command zurückgreifen.[2]

Die Beschreibungen des Cyberraumes als zukünftiges Handlungsfeld blieben auf deutscher Seite bisweilen interpretationsbedürftig. Dem fast zeitgleich erschienenen Weißbuch 2016 zufolge ist der Cyberraum »der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme«, dem »als öffentlich zugängliches Verbindungsnetz das Internet zugrunde« liegt.[3] Die Verortung des Cyberraumes zwischen einer diffusen Virtualität und dem globalen Internet ging einher mit Prognosen, dass zukünftige Konflikte im Cyberraum und damit nicht mehr »ganz konkret auf dem Boden« stattfinden.[4]

Neben den zeitlichen und qualitativen Unterschieden zwischen den deutschen und US-amerikanischen Streitkräften im Cyberraum hatten sich bereits drei Jahre zuvor Differenzen bei der Kontrolle des Internets gezeigt: Die Enthüllungen von Edward Snowden zur umfangreichen Überwachung von Datenströmen durch die

1 Vgl. Hemicker, Von der Leyens später Eintritt in den Cyberwar.
2 Vgl. Stewart/Alexander, U.S. Waging Cyber War on Islamic State.
3 BMVg, Weißbuch 2016, S. 36.
4 Bundesverteidigungsministerin Ursula von der Leyen, zit. nach Von der Leyen sieht Schlachtfeld der Zukunft im Cyberraum.

US-amerikanische National Security Agency (NSA) im Jahre 2013 führte zu einer enormen Belastung der Beziehungen zwischen Deutschland und den USA. Das gezielte Abhören des Mobiltelefons der deutschen Bundeskanzlerin Angela Merkel sowie weiterer Ziele im politischen und wirtschaftlichen Bereich führte zum diplomatischen Protest und zu einer öffentlichen Kontroverse. Die systematische und umfangreiche Durchdringung der Datenströme des Internets und das lückenlose Datensammeln (Full Take) ungeachtet nationaler Jurisdiktion durch einen militärischen Nachrichtendienst lösten in der deutschen politischen und gesellschaftlichen Debatte eine Mischung aus Erstaunen und Entsetzen aus. Das Scheitern eines No-Spy-Abkommens mit Washington und das US-amerikanische Unverständnis gegenüber den deutschen Forderungen offenbarten, dass die Vorstellungen zu Umfang und Reichweite der staatlichen Kontrolle von Datenströmen weit auseinanderlagen. Als schrittweise das Ausmaß der Überwachungsmaßnahmen immer sichtbarer und die Distanz zwischen deutschen und US-amerikanischen Perspektiven deutlicher wurden, betonte Bundeskanzlerin Merkel im Beisein des US-Präsidenten Barack Obama, das Internet sei »für uns alle Neuland«.[5] Dass diese Beschreibung wohl auf den transatlantischen Partner nicht zutraf, zeigte die wenig später in deutschen Medien veröffentlichte Systematik der globalen Überwachung. Neben dem größten europäischen Internetknoten, dem Deutschen Commercial Internet Exchange (DE-CIX) in Frankfurt am Main,[6] hatte die NSA bereits über Jahre mit dem Programm »XKeyscore« an Hunderten Standorten weltweit das Internet überwacht.[7] Die ständige Betonung von »Recht und Gesetz« auf deutschem Boden durch die Bundesregierung[8] stand der Durchdringung des Internets durch die befreundeten USA gegenüber.

Die zeitlichen und qualitativen Unterschiede in der Entdeckung von Internet und Cyberraum als sicherheitspolitische Handlungsfelder zwischen seit Jahrzehnten sicherheitspolitisch fest verbündeten und in der NATO integrierten Staaten sind erklärungsbedürftig. Das Erkenntnisinteresse der Arbeit liegt daher in den Gründen für die Unterschiede im Denken und Handeln Deutschlands und der USA im Cyberraum.

Als erste Erklärung für das unterschiedliche Handeln Deutschlands und der USA mag das »technologische Argument« auf der Hand liegen. Beide Staaten verfügen über weit unterschiedliche staatliche und wirtschaftliche Ressourcen. Die USA gelten als Ursprungsland des Internets und verfügen seither über marktbe-

5 Beuth, Die Kanzlerin von Neuland.
6 Poitras/Rosenbach/Stark, NSA überwacht 500 Millionen Verbindungen in Deutschland.
7 Vgl. Lischka/Stöcker, Die Infrastruktur der totalen Überwachung.
8 Schulze, Patterns of Surveillance Legitimization, S. 205.

herrschende Unternehmen in der Informations- und Kommunikationstechnologie. Mit Blick auf das ebenfalls von Edward Snowden teilweise enthüllte Handeln Großbritanniens in der Massenüberwachung wirft das technologische Argument aber bereits Fragen auf: Das Denken und Handeln Großbritanniens scheint den USA ähnlicher, obwohl die staatlichen und wirtschaftlichen Ressourcen eher denen Deutschlands entsprechen.

Auch wenn das Internet als bedeutender Teil des Cyberraumes für alle Staaten zu einem bestimmten Zeitpunkt »Neuland« war oder ist, liegt die Vermutung nahe, dass Staaten dem Cyberraum vor dem Hintergrund unterschiedlicher Erfahrungen teils gleiche, teils unterschiedliche Bedeutungen beimessen und dabei eine weite Spanne an zentralen Elementen hervorheben, die von der Gleichsetzung mit dem Internet bis hin zur Virtualität reicht.

Diese sozialen Konstruktionen des Cyberraumes wären dann für die eine Seite selbstverständlich, für die andere Seite aber unverständlich. Bislang ist aber unklar, wie genau sich diese Konstruktionen unterscheiden und woraus sie resultieren.

## 2. Forschungsfrage und Thesen

Der Fokus der Arbeit liegt auf der Beantwortung folgender Forschungsfrage: Welche Gemeinsamkeiten und Unterschiede zeigen sich in deutschen und US-amerikanischen Konstruktionen des Cyberraumes und woraus generieren sich deren strukturierende Elemente?

Die Betonung der territorialen Souveränität Deutschlands und der Verweis auf Recht und Gesetz auf deutschem Boden, aber auch die Beschreibung des Internets als »Neuland« (Merkel) oder von Auseinandersetzungen im Cyberraum als nicht mehr »ganz konkret auf dem Boden« (von der Leyen) erscheinen als Versuch der Übertragung einer territorialen Logik auf den Cyberraum als neues Phänomen. Die Beschreibungen und Metaphern legen nahe, dass das deutsche Unverständnis gegenüber der US-amerikanischen Konstruktion einer territorialen Prägung unterliegt und inkompatibel mit dem Internet und dem Cyberraum als vermeintlich nichtterritorialen »Phänomenen« ist. Für deren Nichtterritorialität spricht die maritime Metaphorik aus der frühen Phase des Internets, die bereits an verschiedenen Stellen Gegenstand philosophischer und raumsoziologischer Betrachtungen war: Hier wurden Metaphern aus der Schifffahrt als besonders geeignet zur Beschreibung des Internets dargestellt oder die maritime Metapher des »Surfens« in den Vordergrund gestellt.[9] Auch bezüglich des Begriffes »Cyberraum« zur Beschreibung eines exterri-

9 Vgl. Jones, Kommunikation, S. 132.

torialen Raumes wurde auf die Wirkmächtigkeit des maritimen Raumes als ebenso exterritorialem Raum verwiesen. Diese zeige sich in der eigentlichen Abstammung des Wortes »Cyber« von der »Kybernetik« (griechischer Ursprung: Kybernētikḗ téchnē) als Navigations- oder Steuermannskunst.[10] Der Vorwurf, die Deutschen in ihrer Mentalität oder Deutschland als sicherheitspolitischer Akteur hätten ein zu schwach ausgeprägtes maritimes Bewusstsein, scheint gleichzeitig so alt zu sein wie die deutschsprachige Literatur zum maritimen Raum selbst. Von Alfred von Tirpitz' verbittertem Vorwurf nach dem Ersten Weltkrieg, die Deutschen hätten »die See nicht verstanden«,[11] über die Feststellung in der Einleitung zur deutschen Übersetzung von Alfred Thayer Mahans Standardwerk »Der Einfluß der Seemacht auf die Geschichte 1660–1812«, den Deutschen sei »die See fremd geblieben« und sogar »unheimlich«,[12] bis hin zum Bedauern einer mangelhaften deutschen wissenschaftlichen[13] oder politischen und gesellschaftlichen Beschäftigung[14] mit dem maritimen Raum in neueren Werken zur »maritimen Sicherheit« gehört diese Diagnose schließlich zum Standardrepertoire. Steht also einerseits eine für Deutschland konstatierte »Sea Blindness«[15] im Zusammenhang mit einer deutschen »Cyber Blindness« und prägt andererseits der US-amerikanische Blick auf den maritimen Raum die US-Wahrnehmung des Cyberraumes? Anders formuliert: Wo gibt es Parallelen oder gar Schnittpunkte zwischen US-amerikanischen Konstruktionen des maritimen Raumes und des Cyberraumes, die es in deutschen Konstruktionen dieser Räume nicht gibt?

Diese Überlegungen verweisen darauf, dass unterschiedliche Wahrnehmungen des Cyberraumes weit über das technologische Argument hinausgehen müssten. Dem britischen Admiral Chris Parry zufolge war ähnlich dem heutigen Cyberraum auch der maritime Raum jahrhundertelang »a place apart – a virtual world that had its ›geeks‹ and specialists who understood the mysteries of the medium and how best to exploit it«.[16] Nach dieser Logik müsste es maritim geprägten Nationen auch leichter fallen, in den Cyberraum »aufzubrechen«.

Wenn der Aufbruch in den weiten maritimen Raum bereits vor Jahrhunderten neben den Schiffen als entscheidender technologischer Bedingung auch Navigation und geografisches Wissen erforderte,[17] würde nicht nur technisches, sondern

10 Vgl. Schroer, Räume, Orte, Grenzen, S. 258.
11 Tirpitz, Erinnerungen, S. 387.
12 Einführung von Gustav-Adolf Wolter zu Mahan, Der Einfluß der Seemacht, S. 11.
13 Vgl. Bruns/Petretto/Petrovic, Zum Geleit, S. 15.
14 Vgl. Jopp, Einführung in die Problemstellung, S. 11 f.
15 Vgl. z.B. Feldt, Sea Blindness.
16 Parry, Super Highway, S. 35.
17 Vgl. Elvert, Europa, das Meer und die Welt, S. 15.

auch unterschiedliches geografisches Wissen über den Cyberraum in der US-amerikanischen und deutschen Sicherheitspolitik zu den genannten Unterschieden und Verwerfungen führen.

Offen bleibt zunächst, worin diese »Geografie« des maritimen Raumes und des Cyberraumes liegt. Die erste Annäherung anhand der erwähnten Beispiele legt nahe, dass für die deutsche Seite die Staatsgrenzen im Vordergrund stehen. Hier wären die Abgrenzungen beziehungsweise der abgegrenzte Raum die strukturierenden Elemente der Konstruktion des Cyberraumes. Für die US-amerikanische Seite scheinen diese Elemente in den Hintergrund getreten zu sein und von der globalen Vernetzung überlagert zu werden. Die strukturierenden Elemente wären folglich weniger die überlagerten (Staats-)Räume, sondern vielmehr die dominierenden Datenströme des globalen Internets. Eine solche Ordnung lässt sich zweifelsohne auch im maritimen Raum finden. Auch hier lassen sich auf den ersten Blick keine festen Grenzen erkennen, wenn man von der natürlichen Begrenzung des maritimen Raumes an den Küsten der Kontinente absieht. Eine globale und stetige Stromstruktur ist ebenfalls auszumachen, wobei nicht Daten, sondern Handelsgüter und in geringerem Maße Personen transportiert werden. Eine mögliche Strukturierung des maritimen Raumes und des Cyberraumes könnte also jeweils in einer eigenen, aber vergleichbaren Struktur globaler Ströme liegen. Im Sinne eines »maritimen Gedächtnisses« wäre diese für die USA omnipräsent und würde vom maritimen Raum auf den Cyberraum übertragen werden. Auf der deutschen Seite hingegen gäbe es im Sinne eines »territorialen Gedächtnisses« im maritimen Raum keine Stromstrukturen, die auf den Cyberraum übertragen werden könnten.

Die Forschungsfrage soll daher anhand eines Vergleiches der deutschen und US-amerikanischen Konstruktionen des Cyberraumes und des maritimen Raumes untersucht und beantwortet werden. Dazu werden folgende Thesen aufgestellt:

1. Die Bundesrepublik Deutschland hat sich sicherheitspolitisch bislang auf das Denken in territorialen und abgrenzbaren Räumen konzentriert. Diese territoriale »Raumlogik« prägt die Konstruktion des Cyberraumes. Hieraus resultieren strukturell ähnliche Denk- und Handlungsmuster im maritimen Raum und im Cyberraum.
2. Die USA haben sich sicherheitspolitisch neben der Kontrolle von territorialen und abgrenzbaren Räumen auch auf die Kontrolle von maritimen Strömen konzentriert. Diese maritime »Stromlogik« prägt die Konstruktion des Cyberraumes. Hieraus resultieren strukturell ähnliche Denk- und Handlungsmuster im maritimen Raum und im Cyberraum.

## 3. Einordnung in die Forschung

### a) Perspektiven auf den Cyberraum

Der erste Blick auf die deutsch- und englischsprachigen Veröffentlichungen zum Thema Cyberraum eröffnet ein weites Feld scheinbar unzähliger Sammelbände, Monografien und Aufsätze. Die Spanne der erschienenen Werke reicht von populärwissenschaftlicher Literatur zu möglichen Cyberkriegen bis zu wissenschaftlich fundierten Analysen sicherheitspolitischer Problemstellungen im Cyberraum. Die Relevanz dieser Literatur lässt sich aber mit Blick auf die Forschungsfrage und die aufgestellten Thesen schnell eingrenzen.

Der Blick auf die wichtigsten Sammelbände offenbart zunächst die Dominanz US-amerikanischer, ferner britischer Autorinnen und Autoren. Hierzu zählen Werke, die verschiedene Aspekte von der technischen Infrastruktur und der Systematisierung von Gefahren bis zu staatlichen Instrumenten beleuchten,[18] aber auch solche, die Implikationen für (völker)rechtliche und politische Ordnungen des internationalen Systems problematisieren.[19] Einflussreich sind ebenso Werke, die den Cyberraum bewusst aus US-amerikanischer Sicht beleuchten und die wissenschaftliche Erschließung der Grundlagen des Cyberraumes als Ausgangspunkt für die Entwicklung US-amerikanischer Strategien sehen und so eine starke normative Ausrichtung erkennen lassen.[20]

Besonders bei den Monografien reichen die Werke in einer weiten Spanne von gut begründenden, sachlichen Veröffentlichungen bis zu populärwissenschaftlichen Werken, die teils von Fantasien zu künftigen Cyberkriegen geleitet sind.[21] Diesen gegenüber stehen andere Werke, die sich um eine Versachlichung von Cyberkriegsszenarien bemühen.[22] Ergänzt werden diese Ansätze durch ebenfalls nüchterner argumentierende Monografien, die sich Fragen zu staatlichen Strategiefindungsprozessen widmen.[23] Selten sind insbesondere in der deutschsprachi-

---

18 Z.B. Routledge Handbook of Internet Politics.

19 Z.B. Cyber-Development sowie Power and Security.

20 Hier sticht besonders hervor: Cyberpower and National Security. Der Band ist das Ergebnis einer Studie des Center for Technology and National Security Policy an der National Defense University im Auftrag des Pentagons und beinhaltet explizit Empfehlungen für politische Entscheidungsträger; vgl. Vorwort des Bandes und Kramer/Starr/Wentz, Introduction.

21 Stellvertretend für die US-amerikanischen Werke steht hier die Publikation des ehemaligen Cybersicherheitsberaters im Weißen Haus, Richard A. Clarke: Clarke/Knake, Cyber War; sowie für den deutschsprachigen Raum das eher für den nichtwissenschaftlichen Markt verfasste Buch Gaycken, Cyberwar.

22 Stellvertretend Rid, Cyber War Will not Take Place.

23 Z.B. Betz/Stevens, Cyberspace and the State.

gen Forschungslandschaft Publikationen, die technisches Wissen und politisches Denken gleichermaßen betrachten und Formen strategischen Denkens im Cyberraum umreißen.[24]

Eine andere Form der Dekonstruktion der Vorstellungen zu Cyberkriegen liegt in der Analyse der Diskurse und der Narrative sicherheitspolitischer Berater und Entscheidungsträger im Prozess der Versicherheitlichung des Cyberraums. Myriam Dunn Cavelty beschreibt unter dem bezeichnenden Titel »Der Cyber-Krieg, der (so) nicht kommt«, wie die »erzählten Katastrophen« vor dem Hintergrund des tatsächlichen »Nichtwissens« entstehen.[25] Zu US-amerikanischen Diskursen in den 1990er- und frühen 2000er-Jahren über Gefahren und Bedrohungen im Cyberraum bietet neben Myriam Dunn Cavelty auch Ralf Bendrath kritische, anschlussfähige Analysen.[26] Eine weitere Gruppe stellen Werke dar, die sich den Möglichkeiten der Verregelung des Handelns von Staaten aus der Perspektive des geltenden internationalen Rechts, insbesondere des Völkerrechts, widmen[27] oder die versuchen, die Entwicklung von Normen und Regeln für neue Waffensysteme auf die Normentwicklung im Cyberraum zu übertragen.[28]

### b) Unzureichende Dekonstruktion des Cyberraumes als »Idee«

Gemein ist diesen Publikationen zumeist, dass der Cyberraum als sicherheitspolitisches Handlungsfeld zugrunde gelegt wird, ohne dass dessen Genese und Strukturen ausreichend diskutiert werden. Selbst bei Werken, deren Titel die Befassung mit dem Raum suggerieren, finden sich hauptsächlich Zusammenstellungen der eindrucksvollsten Cyberangriffe aus einer deutlich US-amerikanisch geprägten Perspektive.[29] Die bislang überzeugendste Rekonstruktion der Entwicklung des Cyberraumes unter besonderer Berücksichtigung militärischer, nachrichtendienstlicher, ökonomischer und zivilgesellschaftlicher Perspektiven bietet das International Institute for Strategic Studies (IISS) mit dem Dossier »Evolution of the Cyber Domain: The Implications for National and Global Security«.[30] Der Fokus auf informationstechnologische Entwicklungen und die Rolle der USA so-

24 Gaycken, Cyberwar, aber auch Einzelbeiträge wie Gaycken, Cybersecurity.
25 Dunn Cavelty, Der Cyber-Krieg.
26 Bendrath, The Cyberwar Debate; Bendrath, The American Cyber-Angst; Bendrath/Eriksson/Giacomello, From »Cyberterrorism« to »Cyberwar«.
27 Harrison Dinniss, Cyber Warfare and the Laws of War; als jüngere deutsche Veröffentlichung Dornbusch, Das Kampfführungsrecht im internationalen Cyberkrieg.
28 Mazanec, The Evolution of Cyber War.
29 Z.B. A Fierce Domain.
30 IISS/Tikk-Ringas, Evolution of the Cyber Domain.

wie das Erscheinungsjahr 2015 bedingen aber, dass geografische Konstruktionen sowie deutsche Perspektiven auf den Cyberraum keine relevante Rolle spielen.

Dass der Cyberraum der eigenen Analyse ohne kritische Diskussion zugrunde gelegt und als gegeben vorausgesetzt wird, betrifft auch und insbesondere Veröffentlichungen zur deutschen Cybersicherheitspolitik. Im Zuge des Bedeutungsgewinns des Internets in Deutschland und Europa ab Mitte der 1990er-Jahre waren zwar in der deutschsprachigen Forschungslandschaft raumphilosophische und raumsoziologische Monografien und Sammelbände erschienen, die sich dem Internet sowie dem »Cyberraum« als virtuellem Raum und gesellschaftlichem Phänomen widmeten.[31] Vergleiche des Cyberraumes mit dem maritimen Raum wurden etwa dann gezogen, wenn es um die Entdeckung »neuer Welten« als Erschließung und Erklärung des Unbekannten[32] oder um andere Beispiele von Raumverkürzung oder Beschleunigung ging, wobei zumindest partielle Bezüge zu geopolitischem Denken hergestellt wurden.[33] Erst als der Begriff Cyberraum in den 2010er-Jahren in der deutschen Sicherheitspolitik übernommen wurde, widmeten sich kleinere Beiträge der Genese des Präfixes »Cyber«[34] und dessen Verwendung oder Instrumentalisierung in Prozessen der Versicherheitlichung.[35]

In deutschsprachigen politikwissenschaftlichen Studien zur Sicherheitspolitik im Cyberraum nimmt die Möglichkeit unterschiedlicher Vorstellungen und Konstruktionen des Cyberraumes aber keine relevante Rolle ein. Die überzeugendste deutsche Monografie zur Sicherheitspolitik im Cyberraum liefert aus politikwissenschaftlicher Perspektive Mischa Hansel mit seiner Studie »Internationale Beziehungen im Cyberspace«, in der er die mangelnde zwischenstaatliche Kooperation bei Herausforderungen im Cyberraum problematisiert.[36] Hansel verweist zwar knapp darauf, dass es kein einheitliches Verständnis des Cyberraumes gibt, und bietet eine ausführliche Beschreibung des Cyberraumes, bedient sich aber an entscheidenden Stellen US-amerikanisch geprägter Konstruktionen aus Veröffentlichungen der National Defense University[37] und der RAND Corpo-

31 Z.B. Bredekamp, Politische Theorien des Cyberspace; Münker, Was heißt eigentlich: »Virtuelle Realität«?; Rötzer, Virtueller Raum oder Weltraum?; Krämer, Verschwindet der Körper?; Ellrich, Die Realität virtueller Räume; Pott/Budke/Kanwischer, Internet, Raum und Gesellschaft.

32 Z.B. Schroer, Räume, Orte, Grenzen, S. 254–264; oder Jones, Kommunikation.

33 Z.B. Werber, Von der Bagatellisierung des Raums.

34 Z.B. Wagner/Vieth, Was macht Cyber?

35 Z.B. Schulze, (Un)Sicherheit hinter dem Bildschirm.

36 Hansel, Internationale Beziehungen im Cyberspace.

37 Bei der Definition des Cyberraumes orientiert sich Hansel an der Definition des Cyberspace von Daniel T. Kuehl (ehemals Professor an der School of Informations Warfare and Strategy) im bereits genannten Sammelband Cyberpower and National Security;

ration.[38] Jakob Kullik geht in seiner Studie »Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik« mit einer Politikfeldanalyse der Frage nach, ob »Deutschland eine eigene, konsistente Cybersicherheitspolitik« verfolgt.[39] Er beklagt, dass es in der Debatte um die Cybersicherheit »an wissenschaftlich sauberen Begrifflichkeiten« fehlt,[40] kündigt dann aber die synonyme Verwendung der Begriffe Internet, virtueller Raum, digitaler Raum sowie Cyberspace und Cyberraum an[41] und übernimmt die Definition des Cyberspace von Mischa Hansel, die dieser wie beschrieben in Anlehnung an Daniel T. Kuehl formuliert hatte.[42] Dominika Zedler untersucht in ihrer ausführlichen Studie »Zur Strategischen Planung von Cyber Security in Deutschland« die politische und institutionelle Organisation der Cybersicherheit in Deutschland.[43] Sie rückt die Fragmentierung und dezentrale Organisation sowie die damit verbundene Unklarheit bezüglich der Verantwortlichkeiten und Zuständigkeiten in den Vordergrund ihrer Kritik am Umgang Deutschlands mit den Bedrohungen im Cyberraum.[44] Sie hinterfragt aber ebenfalls nicht die Idee des Cyberraumes selbst. Zedler nimmt für ihre Analyse der deutschen Politik vielmehr als Grundlage, dass vom Cyberraum »Cyberkrieg, Cyberkriminalität oder Cyberterrorismus« ausgehen, sodass der Cyberraum wie auch die Bedrohungen als Tatsachen vorausgesetzt werden.[45] Der Schwerpunkt liegt bei Kullik und Zedler jeweils auf der politischen und

---

vgl. Hansel, Internationale Beziehungen im Cyberspace, S. 33 f. Bei der Benennung von Fähigkeiten der Akteure im Cyberraum verweist Hansel auf die vagen Prognosen des ehemaligen Cybersicherheitsberaters Richard A. Clarke; vgl. Hansel, Internationale Beziehungen im Cyberspace, S. 35.

38 Vgl. die zahlreichen Verweise auf die RAND-Studie Libicki, Cyberdeterrence and Cyberwar; vgl. Hansel, Internationale Beziehungen im Cyberspace, S. 38 f.

39 Kullik, Vernetzte (Un-)Sicherheit?, S. 21.

40 Vgl. ebd., S. 22.

41 Vgl. ebd., S. 18.

42 Vgl. ebd., S. 35.

43 Zedler, Zur strategischen Planung von Cyber Security (2016); vgl. auch den gleichnamigen Aufsatz (2017).

44 Zedler fundiert diese Kritik mit einer umfangreichen Analyse der deutschen Institutionen und ihrer Zuständigkeiten und Kooperationsformen im Cyberraum. Mithilfe einer SWOT-Analyse (Strengths, Weaknesses, Opportunities, Threats) stellt sie klar strukturiert die Stärken, Schwächen, Möglichkeiten und Gefahren der Organisation der Cybersicherheit in Deutschland dar.

45 Vgl. Zedler, Zur strategischen Planung von Cyber Security (2016), S. 12. Hier scheint weiterhin bedenklich, dass Zedler etwa zu Cyberkriminalität und Cyberspionage sowie Cybersabotage die jeweiligen Definitionen von Bundeskriminalamt oder Bundesministerium des Innern nutzt, um auf dieser Grundlage anschließend das Handeln dieser Akteure zu bewerten; vgl. ebd., S. 15 f. Für Zeidlers Erkenntnisinteresse ist das Vorgehen zielführend, für das Thema an sich ist die unkritische Übernahme aber bedenklich.

institutionellen Organisation, die Wahrnehmung und semantische Konstruktion des Cyberraumes als sicherheitspolitisches Denk- und Handlungsfeld spielt hier allenfalls eine Nebenrolle.

Die Übernahme von Definitionen schmälert nicht zwangsläufig die wissenschaftliche Qualität dieser Studien. Liegt das Erkenntnisinteresse in einer anderen Frage, kann nicht jeder Begriff einer umfangreichen Untersuchung unterzogen werden. Insbesondere Mischa Hansels Werk bleibt ein in der deutschsprachigen Forschungslandschaft herausragendes Werk zu den Grundlagen von Kooperation im Cyberraum. Die Übernahme von Definitionen und Beschreibungen verweist aber auf die Möglichkeit der globalen Übertragung von Raumvorstellungen des US-Militärs auf wissenschaftliche Studien und die Notwendigkeit der kritischen Dekonstruktion dieser Vorstellungen als Forschungsbeitrag.

### c) Anschlussfähige Beiträge und Perspektiven

Über die Wahrnehmung des Cyberraumes in der US-amerikanischen und deutschen Sicherheitspolitik sind allenfalls einige Einzelbeiträge erschienen, die für die vorliegende Arbeit hilfreiche Impulse geben, insgesamt aber nur Teilbereiche berühren. Zu nennen ist hier abermals Myriam Dunn Cavelty, die den Prozess der Versicherheitlichung in den USA zur Cybersicherheit und den Schutz Kritischer Infrastrukturen untersucht. Dabei geht sie bereits umfangreich auf die sicherheitspolitischen Grundlagendokumente seit den 1990er-Jahren und die Rolle des Militärs ein.[46] Hier wird die jeweilige Konstruktionslogik zumindest bis zum Jahr 2008 beleuchtet, es fehlt freilich die vergleichende Perspektive.

Direkte Vergleiche zwischen der deutschen und US-amerikanischen Sicherheitspolitik im Cyberraum sind vornehmlich in der deutschen Forschungslandschaft und in der Form von Aufsätzen zu finden. Hier scheinen die Enthüllungen durch Edward Snowden zu den Aktivitäten der NSA auch das wissenschaftliche Interesse geweckt zu haben. Hervorzuheben sind einige Arbeiten der Stiftung Wissenschaft und Politik, etwa von Annegret Bendiek, die beispielsweise unter dem Titel »Umstrittene Partnerschaft« die transatlantischen Initiativen zur Cybersicherheitspolitik kritisch beleuchtet und Perspektiven für deren Weiterentwicklung aufzeigt.[47] In »Sorgfaltsverantwortung im Cyberraum« entwickelt sie Grundsätze für eine deutsche Cyber-Außen- und Sicherheitspolitik und weist da-

46 Dunn Cavelty, Cyber-Security and Threat Politics. Dunn Cavelty zeigt sich als erstklassige Expertin für Kritische Infrastrukturen. Zum Versicherheitlichungsprozess im Spiegel der Grundlagendokumente vgl. S. 94–107, zur Rolle des Militärs vgl. S. 80–90.

47 Bendiek, Umstrittene Partnerschaft. Diese Studien, die eine starke deutsche Perspektive einnehmen und auch Handlungsempfehlungen enthalten, werden in der empirischen

bei deutlich auf die Notwendigkeit einer europäischen Koordinierung hin.[48] Einen ebenfalls interessanten Ansatz bietet Kathrin Ulmer, die mit einer wissenssoziologischen Diskursanalyse die Risikokommunikation und die Strategien zur Bearbeitung und Regulierung von Risiken in den USA und Deutschland untersucht.[49] Matthias Schulze analysiert die Reaktion der Bundesregierung auf die Enthüllungen zur Überwachungspraxis der NSA durch Edward Snowden bezüglich der rhetorischen Strategien zur Legitimierung dieser Praktiken, zum Herunterspielen von Vorwürfen sowie zur Deeskalation des Skandals.[50]

In diesen Studien steht die politische Annäherung zwischen den beiden Staaten durch Strategiefindungs- und Verregelungsprozesse im Vordergrund. Unterschiedliche Konstruktionen des Cyberraumes spielen höchstens am Rande eine Rolle. Der Idee der vorliegenden Arbeit nahe kommen Marcel Dickow und Nawid Bashir, die untersuchen, ob die nationalen Cyberstrategien Deutschlands, der USA und Russlands die konzeptionellen Besonderheiten des Cyberraums ausreichend berücksichtigen.[51] Hier bleibt der Vergleich, insbesondere aber die theoretische Erarbeitung der Besonderheiten des Cyberraumes aufgrund der Breite des Vergleiches und der Kürze des Beitrages zwangsläufig kursorisch. All diese Arbeiten konzentrieren sich auf eine politische Bewertung des Handelns der USA sowie die Bedeutung für die Beziehungen zwischen Deutschland und den USA, betrachten aber mögliche Unterschiede anhand verschiedener Wahrnehmungen und Konstruktionen des Cyberraums als sicherheitspolitisches Handlungsfeld nur am Rande.

### d) Zur Dekonstruktion von »Raumstrukturen«

Die Suche nach einer Raum- oder Stromlogik in globalen Räumen weitet den Blick über Ansätze der Internationalen Beziehungen hinaus. Seit den 1990er-Jahren sind einige Beiträge erschienen, die eine Konkurrenz zwischen Räumen und Strömen aufgriffen und in eine geografische oder geopolitische Perspektive einbetteten. Mittlerweile inhaltlich nicht mehr aktuelle, aber dennoch anschlussfähige Werke wie der 1998 erschienene Sammelband »An Unruly World? Globalization, Governance and Geography« von Andrew Herod, Gearóid Ó Tuathail

---

Betrachtung der deutschen Konstruktionen des Cyberraumes in Kapitel VII näher beleuchtet.

48 Bendiek, Sorgfaltsverantwortung im Cyberraum. Bendiek schließt u.a. an eine 2012 verfasste Studie zur europäischen Dimension an: Bendiek, Europäische Cybersicherheitspolitik.

49 Eine Darstellung über ihren Forschungsansatz bietet Ulmer in: Ulmer, Cyber Risks and Cyber Security.

50 Schulze, Patterns of Surveillance Legitimization.

51 Dickow/Bashir, Sicherheit im Cyberspace.

und Susan M. Roberts hinterfragen die Konstruktion globaler Räume unter sich verändernden Bedingungen.[52] Dass diese Überlegungen nicht Teil der Internationalen Beziehungen, sondern der »Kritischen Geopolitik« sind, verweist auf die Notwendigkeit eines erweiterten Forschungsansatzes für die vorliegende Arbeit. Diese Feststellung wird verstärkt durch die Beobachtung, dass die in der englischsprachigen Forschungslandschaft sehr präsente Unterscheidung zwischen kontinental und maritim geprägten Strategien in Deutschland kaum rezipiert wird.[53] Diese Unterscheidung spielt vornehmlich eine Rolle, wenn der Blick auf die Seemacht USA gerichtet wird. Die Beiträge von Sebastian Bruns stechen hierbei besonders hervor und verdienen bei der späteren Betrachtung US-amerikanischer Konstruktionen des maritimen Raumes eine breitere Diskussion.[54]

In jüngerer Zeit mehren sich zwar in der englischsprachigen Literatur Stimmen, die mit einem stark normativen Anspruch zu einer stärkeren Berücksichtigung globaler Ströme in der sicherheitspolitischen Praxis aufrufen. Hierzu zählen eher populärwissenschaftliche Werke wie Parag Khannas »Connectography«,[55] der darauf hinweist, dass globale Raumstrukturen einer Stromstruktur weichen, aber auch theoretisch fundiertere Veröffentlichungen wie die Studie »Towards the Geopolitics of Flows«, die den Wandel von der territorialen Geopolitik zur Geopolitik der globalen Ströme analysiert, dessen Bedeutung für Finnland darlegt und explizit das Ziel verfolgt, die Wahrnehmung globaler Ströme im sicherheitspolitischen Denken Finnlands zu stärken.[56] Dem Forschungsinteresse der vorliegenden Arbeit nahe scheint die Monografie »The Challenge of Global Commons and Flows for US Power« zu kommen, welche die US-Perspektive auf globale Ströme beleuchtet und den USA einen grundlegenden Wandel von der Kontrolle der Räume zur Kontrolle globaler Ströme attestiert, jedoch auf die maritimen Handelsströme und

52 An Unruly World?, hier besonders der Beitrag Herod, Of Blocks, Flows and Networks; vgl. Ó Tuathail/Herod/Roberts, Negotiating Unruly Problematics.

53 Z.B. Barnett, Maritime and Continental Strategies.

54 Bruns, U.S. Navy Strategy; sowie in Kurzform: Bruns, US-Marinestrategie; für die maritime Prägung des US-amerikanischen strategischen Denkens und die Auswirkungen auf Europa: Bruns, Seemacht und Geopolitik.

55 Khanna, Connectography. Khanna vertritt die These, dass die globalen Verbindungslinien in Zukunft weitaus wichtiger sein werden als die Trennlinien (Grenzen). Wenn so die klassische Geografie durch eine Connectografie abgelöst werde, entwickle sich die geopolitische Konkurrenz »from war over territory to war over connectivity«; ebd., S. XVII.

56 Aaltola [u.a.], Towards the Geopolitics of Flows. In der Studie bildet der umfangreiche Theorieteil die Basis zur empirischen Diskussion der Implikationen für Finnland, wenn es zukünftig aufgrund einer eisarmen Arktis neue »arctic global flows« gibt.

den Luftverkehr in der Zeit nach dem 11. September 2001 fokussiert und Aspekte des Cyberraumes nur partiell aufnimmt.[57]

In Deutschland treten derartige Ansätze zum Verhalten von Staaten zu globalen Strömen insbesondere in Verbindung mit einer geopolitischen Perspektive aber nur als Randerscheinung auf. Zu nennen ist allenfalls Herfried Münkler, der eine Bedeutungsverschiebung von der Kontrolle geografischer Räume zu globalen Strömen nachzeichnet. Diesen Wandel würden die USA wesentlich besser verstehen als die europäischen Staaten, was sich unter anderem im Insistieren Deutschlands auf das eigene Territorium im Zuge der Enthüllungen zur Überwachung globaler Kommunikationsräume zeige.[58] Münkler schreibt hier von der »Raumrevolution des 21. Jahrhunderts«[59] und bietet somit im Sinne der vorliegenden Arbeit einen anschlussfähigen Gedanken zur Konkurrenz zwischen Räumen und Strömen, geht aber in seiner überblicksartigen Darstellung auf die konkrete Genese und Strukturierung des Cyberraumes nicht ausführlich ein. Mit Blick auf die US-amerikanisch geprägten Forschungsansätze zu globalen Raumstrukturen stellt er aber eine deutliche Ausnahme in der deutschen Forschungslandschaft dar. Münklers beiläufige Kritik am Sammelband »Raumwissenschaften« von Stephan Günzel, in dem zwar die Erziehungs- und Musikwissenschaften, nicht aber die Politikwissenschaften vertreten seien,[60] kann mit Blick auf die bereits dargestellte raumsoziologisch und raumphilosophisch geprägte Perzeption des Cyberraumes nur bestätigt werden.

Zusammenfassend lässt sich sagen, dass der im Forschungsinteresse der Arbeit liegende Vergleich zwischen Konstruktionen des Cyberraumes aus deutscher und US-amerikanischer Perspektive in einigen anschlussfähigen Beiträgen zumindest in Teilbereichen angeschnitten wird. Eine ausführlichere Arbeit, die insbesondere die deutschen Konstruktionen des Cyberraumes tiefergehend aufarbeitet, in eine historische Perspektive einbettet sowie einen umfassenden Vergleich zwischen Deutschland und den USA schafft, fehlt bislang.

57 Aaltola/Käpylä/Vuorisalo, The Challenge of Global Commons.
58 Münkler, Kriegssplitter, insbesondere S. 262, 275 f., 295, 323.
59 Ebd., S. 323.
60 Vgl. ebd., S. 371.