Jenseits der Versicherheitlichung
Zu Stand und Aussichten der Cybersicherheitsforschung

Wolf J. Schünemann und Stefan Steiger

1. Einleitung

Der Begriff Cybersicherheit hat in den letzten 20 Jahren eine bemerkenswerte Entwicklung durchlaufen. Noch Ende der 1990er Jahre wurde kaum über Cybersicherheit gesprochen, stattdessen wurde in Fachkreisen zumeist der aus der Informatik stammende Ausdruck IT-Sicherheit verwendet. IT-Sicherheit umfasst aus dieser technischen Perspektive im Kern drei Schutzziele für Daten bzw. datenverarbeitende Systeme: die Gewährleistung der Vertraulichkeit, der Integrität und der Verfügbarkeit (sog. CIA-Triade, Andress 2015). Heute werden unter dem Rubrum Cybersicherheit aber verschiedene, sehr unterschiedliche Phänomene debattiert, wobei nicht alle die Schutzziele der IT-Sicherheit verletzen. Das Spektrum der Themen reicht dabei von Datendiebstählen über folgenschwere Cyberangriffe auf kritische Infrastrukturen mit potenziell kaskadierenden physischen Effekten bis zu der Verbreitung falscher Nachrichten (Desinformation) und terroristischer Botschaften.

Diese extensionale Begriffserweiterung können Sozial- und insbesondere PolitikwissenschaftlerInnen – womöglich im Unterschied zu den technischen Disziplinen, die sich mit der Sicherheit von vernetzten IT-Systemen und den darin gespeicherten und verarbeiteten Daten befassen – nicht unberücksichtigt lassen und sich auf das technische Kernverständnis von IT-Sicherheit (CIA-Triade, siehe oben) zurückziehen. Vielmehr müssen sie die vielfältigen gesellschaftspolitischen Aufladungen des Problemfelds mit in den Blick nehmen, wollen sie dem Gegenstand gerecht werden. Dennoch oder gerade deshalb ist auch für sozialwissenschaftliche Forschung konzeptionelle und begriffliche Klarheit gefragt, wenn der Untersuchungsgegenstand Cybersicherheit systematisch erfasst und von anderen politischen Regulierungsfeldern (etwa Medienregulierung) konzeptionell unterscheidbar sein soll, insbesondere dann, wenn die Frage behandelt wird, welche politischen Maßnahmen und Ansätze für die Herausforderungen der Digitalisierung angemessen sind. Konkret erwächst der politikwissenschaftlichen Forschung neben den Anforderungen an eine differenzierte Analyse damit auch eine (Teil-)Verantwortung, zur Ernüchterung einer gelegentlich aufgeheizten öffentli-

chen und politischen Debatte beizutragen. Dies ist gerade aktuell zu betonen, in einer Zeit, in der Sicherheitsgesetze zunehmend die Freiheit der Internetkommunikation einschränken und auch liberale Demokratien ihre diesbezügliche Zurückhaltung allmählich aufgeben (BfDI 2019; Freedom House 2018).

Doch auch mit Blick auf die gesamte Entwicklung sozialwissenschaftlicher Cybersicherheitsforschung lässt sich feststellen, dass diese sich seit ihren Anfängen zwischen der Affirmation der sicherheitspolitischen Relevanz von Cyberangriffen (und deren Analyse) und der kritischen Reflexion, die eine substanzielle Lücke zwischen Vokabular und empirischen Phänomenen (Cyberangriffen) aufzeigt und die Implikationen des Sprachgebrauchs problematisiert, bewegt. Während die Arbeiten auf jener Seite oftmals von alarmistischen Untertönen begleitet werden, tendieren diese mitunter zu elfenbeinturmhafter Selbstbeschäftigung. Der Raum für die nüchterne empirische Analyse und vergleichende Arbeiten dazwischen ist noch nicht vollends erschlossen. Dies liegt freilich auch daran, dass die empirische Forschung sowohl durch technische (Detektion von Angriffen, Attributionsproblem) als auch sicherheitspolitische Hindernisse (Geheimhaltung) erschwert wird.

Dieser programmatische Beitrag verfolgt zwei Ziele: Erstens soll er einen orientierenden Überblick über die bestehende sozialwissenschaftliche Forschungslandschaft zum Thema Cybersicherheit geben und zweitens am Ende kurz aktuelle Tendenzen zur Begriffsexpansion kritisch beleuchten und zu mehr konzeptioneller Klarheit aufrufen. Hierzu stellt er zunächst die Forschungsstränge vor, die sich (überwiegend affirmativ) mit den neuen Gefahren aus dem Cyberspace sowie deren potenziellen Folgen befasst haben (Teil 2). Im Anschluss daran diskutiert er einen Strang aus dem Feld der kritischen Sicherheitsstudien, die sowohl den politischen als auch wissenschaftlichen Sprachgebrauch kritisch reflektiert haben (Teil 3). Anschließend betrachtet er das ausbaufähige Feld der empirisch-vergleichenden Cybersicherheits- und -konfliktforschung (Teil 4). Für die internationale Ebene nimmt er die internationale Normenforschung in den Blick (Teil 5). Im letzten Abschnitt behandelt der Beitrag neue Sekuritisierungstendenzen in Politik und Wissenschaft und leitet daraus ein Plädoyer für eine stärkere Differenzierung zwischen den beobachteten Phänomenen und für eine zumindest partielle Reorientierung des Feldes ab.

2. Cyberwar is (still) coming

Es ist mittlerweile über 25 Jahre her, dass die US-amerikanischen Autoren John Arquilla und David Ronfeldt vom Rand National Defense Research Institute aufziehende Konfliktformen im Zeitalter der Digitalisierung unter dem Titel »Cyberwar is coming« beschrieben (Arquilla/Ronfeldt 1993). In dieser Frühphase befassten Studien sich zunächst überwiegend mit den neuen militärischen Möglichkeiten, die

durch eine zunehmende Vernetzung entstanden waren. Konzepte wie »network-centric warfare« zielten darauf, Informationen schnell und effizient zu nutzen, um so Vorteile auf dem Gefechtsfeld zu erlangen. Aus diesem Kontext wurden in den 1990er Jahren auch Ansätze eines »Information Warfare« geboren, die verschiedene (militärische) Möglichkeiten in den Blick nahmen, Informationen in Konflikten zu nutzen oder zu manipulieren (Libicki 2017).

Mit der zunehmenden Vernetzung entstanden in der Folgezeit neue Verwundbarkeiten sowohl der Streitkräfte als auch der Gesellschaften. Spätestens seitdem sich das Internet zum Massenkommunikationsmittel entwickelt hatte und immer mehr soziale und auch individuelle Akteure sich den Sicherheitsgefährdungen im Cyberspace durch Vernetzung aussetzten, kann eine umfassendere Erschließung des Internets als militärischem Handlungsraum beobachtet werden. Staaten bauten eigene offensive und defensive Kapazitäten auf (Lewis/Neuneck 2013). Besonders eindrückliche Fälle von Cyberangriffen, wie bspw. im Frühjahr 2007 gegen Estland, führten dazu, dass im politischen Diskurs, aber auch der öffentlichen Debatte immer häufiger von Cyberkrieg gesprochen wurde (Arquilla 2013).

WissenschaftlerInnen und PolitikerInnen entwarfen anknüpfend an die genannten Entwicklungen und Ereignisse Szenarien katastrophaler Cyberangriffe. Besonders prominent wurden diese unter anderem von Richard A. Clarke skizziert, einem früheren Cybersicherheitsberater der Administration von George W. Bush (Clarke/Knake 2010). Die Rede vom Cyberkrieg riss in den Folgejahren nicht ab (Stone 2013; Stiennon 2015). Im Gegenteil: Die Bedrohungsperzeptionen im Hinblick auf den Cyberspace sind in den vergangenen Jahren immer deutlicher geworden, haben Strategiepapiere und Aktionspläne erreicht, stehen dort vielfach an führender Stelle, wenn es um die größten Bedrohungen unserer Zeit geht, und haben institutionelle Reformen begründet. Trotz aller Forderungen nach kritischer Reflexion, die die wissenschaftliche Bearbeitung des Themas auszeichnen (siehe Abschnitt 3), scheint der martialische Kriegsbegriff auch bei AutorInnen wie Verlagen jenseits des militärisch-sicherheitspolitischen Komplexes regelmäßig zu verfangen, gerade wenn es darum geht, auflagenstarke Sachbücher für eine breitere Öffentlichkeit zu produzieren (Gaycken 2011, 2012; Jamieson 2018; Kurz/Rieger 2018; Sanger 2018; Singer/Friedman 2014).[1]

Gerade die teils populärwissenschaftlich ausgerichteten Beiträge dieses Stranges weisen Ähnlichkeiten in Struktur und Inhalten auf. Zunächst führen sie in die soziotechnischen Zusammenhänge der Sicherheit von Informationssystemen ein. Dazu erläutern sie die zum Verständnis notwendigen technischen Grundlagen und stellen das in den technischen Sphären der IT-Administration sowie der Strafverfolgung etablierte und bewährte Vokabular vor. Zur Illustration von Angriffen erheblicher Reichweite wird im Regelfall eine überschaubare Anzahl bekannter Cy-

1 Die Begriffswahl wird dabei von den AutorInnen in unterschiedlichem Maße kritisch reflektiert.

bersicherheitsvorfälle angeführt. Zentrale Abschnitte sind zudem im grammatikalischen Modus des Potentialis gehalten, soll heißen: Es wird geschildert, was passieren könnte oder was nach derzeitigem Kenntnisstand als wahrscheinlich gelten darf, ggf. mit den daraus gefolgerten katastrophalen Konsequenzen für die Gesellschaft. Damit weisen diese Werke auf einflussreiche Diskurse der vergangenen Jahre hin, deren Teil sie sind und die das technisch-administrative Umfeld sowie die Ebene der politischen Entscheidungsfindung augenscheinlich geprägt haben. So zeigt die für die derzeitige IT-Sicherheitsgesetzgebung (IT-Sicherheitsgesetz – (Bundesgesetzblatt 2015), NIS-Richtlinie – (EU 2016) grundlegende Klassifikation der kritischen Infrastrukturen erkennbare Spuren des Diskurses über mögliche Cybersicherheitsbedrohungen, einschließlich katastrophenförmiger Szenarienbildung. Freilich finden sich daneben auch empirisch-vergleichende Arbeiten, die Ansätze zum Schutz kritischer Infrastrukturen untersuchen (siehe Abschnitt 4).

In diesem Beitrag sollen die realen Sicherheitsbedrohungen durch und in vernetzten IT-Systemen und Digitalisierung nicht bagatellisiert werden. Vielmehr dient die Betonung der gemeinsam und fortwährend prozessierten Erzählung, wonach der Cyberkrieg komme, dem Zweck, einen sichtbaren Strang wissenschaftlicher, einschließlich populärwissenschaftlicher, Literatur zusammenfassend zu überschauen und auf den unterschiedlich motivierten Alarmismus dieser Werke hinzuweisen. Angesichts der Bedeutung der genannten Titel für die gegenstandsbezogene Propädeutik und potentielle gesellschaftliche Aufklärung (nicht zuletzt aufgrund ihrer Alleinstellung), stellt sich die Frage, ob diese grundlegenden Felder nicht einer komplementären Anreicherung durch empirisch fundierte und in der Szenarienbildung zurückhaltendere Einführungstexte bedürfen. Eben hierfür möchten wir an dieser Stelle plädieren.

3. Kritische Sicherheitsstudien

Jede kritische Reflexion setzt konzeptionell-definitorische Vorarbeiten voraus. Dabei müssen SozialwissenschaftlerInnen die Vielschichtigkeit des Begriffs in ein kritisches Verständnis aufnehmen. In diesem Sinne findet sich eine Reihe von Beiträgen, die auf Basis sozialkonstruktivistischer Theorie in das Begriffsfeld Cybersicherheit einführen (Dunn Cavelty 2010; Nissenbaum 2005; Schünemann 2019a i.E.; Schünemann/Harnisch 2015). In darüberhinausgehenden konzeptionellen und begriffskritischen Arbeiten hat insbesondere der leichtfertige Gebrauch des Worts »Cyberkrieg« Anstoß erregt. In der Folge haben sich kritische WissenschaftlerInnen mit den Risiken einer diskursgetriebenen Versicherheitlichung und Militarisierung des Internets auseinandergesetzt (Dunn Cavelty 2012; Guitton 2013; Leisegang 2015). Auch wurden der Begriff Cyberkrieg und die damit verbundenen Szenarien angesichts zumindest nach klassischen Maßstäben überwiegend harmlo-

ser Cyberangriffe (insbesondere mit Blick auf Schäden im materiellen Raum, kinetische Effekte) als konzeptionell unangemessen abgelehnt. Stattdessen ist die Eintrittswahrscheinlichkeit eines kriegsähnlichen, ausschließlich auf Cyberangriffe beschränkten, zwischenstaatlichen Konfliktaustrags als gering eingestuft worden. So hat Thomas Rid in einer vielbeachteten Studie Cyberangriffe an der tradierten Kriegsdefinition von Carl von Clausewitz gemessen, wonach sich ein kriegerischer Akt erstens durch einen gewaltsamen Charakter, zweitens durch seine Zweckdienlichkeit zur Unterwerfung des Gegners und drittens durch seine politische Natur auszeichnet. Anhand dieser Kriterien zeigt Rid, dass es noch keine Cyberangriffe gab, die diese Anforderungen erfüllt haben, und dass der »reine« Cyberkrieg, der nur auf digitalen Angriffen beruht, zur Erreichung militärischer Ziele kaum geeignet ist. Vielmehr dienen Cyberangriffe laut Rid der Spionage, Sabotage oder Subversion und sind damit keine genuin neuen Phänomene (Rid 2012, 2013). Ähnlich argumentiert Erik Gartzke, der ebenfalls davon ausgeht, dass Cyberangriffe zur Eroberung von Territorium und Anwendung von Zwang nur eingeschränkt militärisch nützlich sind (Gartzke 2013). Vor diesem Hintergrund kritisierte Myriam Dunn Cavelty, dass sich die Forschung zu sehr den extremen Erscheinungsformen – wie dem Cyberkrieg – und den damit verbundenen Katastrophenerzählungen zugewendet habe, da dies zu einer verzerrten Gefahrenwahrnehmung beitrage. Stattdessen sollten Untersuchungen stärker die empirisch prävalenten Erscheinungsformen von Cyberangriffen in den Blick nehmen (Dunn Cavelty 2013).

Gerade der in der IB-Theorie verbreitete sozialkonstruktivistisch-kritische Ansatz der Versicherheitlichung hat die Forschung zur Cybersicherheitspolitik über lange Zeit stark geprägt. Davon zeugen die zahlreichen Studien, die dem im Kontext der Kopenhagener Schule entwickelten Ansatz (Sekuritisierung) folgen, um die soziale Konstruktion von Cybersicherheit und die Ausgestaltung zugehöriger Politiken vor allem in den USA, aber auch anderen u.a. europäischen Fallstudien zu analysieren (Bendrath et al. 2007; Dunn Cavelty 2008, 2013; Gorr/Schünemann 2013; Hansen/Nissenbaum 2009; Schulze 2016). Diese Untersuchungen konnten unter anderem zeigen, wie Regierungen ihre Kompetenzen unter Verweis auf Bedrohungen wie Cyberterrorismus oder Cyberkriege signifikant erweitern konnten.[2] Dies lässt sich in verschiedenen Sphären der Sicherheitspolitik beobachten. Erstens haben zahlreiche Staaten damit begonnen, militärische Cyberkommandos zu etablieren, angefangen 2009 mit dem United States Cyber Command. Auf internationaler Ebene wurde der Cyberspace 2016 durch die NATO beim Gipfel von Warschau als neue Domäne zur Kriegsführung anerkannt. Zweitens wurde insbesondere durch die Snowden-Enthüllungen von 2013 offenbar, wie staatliche Ge-

2 Ähnliche kritische Analysen der Diskurse gibt es dementsprechend auch zu Cyberterrorismus und zu anderen nichtstaatlichen Akteuren (Dunn Cavelty und Jaeger 2015; Dunn Cavelty 2008; Gilbert Ramsay 2016; Jarvis et al. 2017).

heimdienste den Cyberspace zur Überwachung (Signals Intelligence) nutzen, insbesondere die US-amerikanische NSA und die Geheimdienste verbündeter Staaten. Drittens haben die Regierungen auch in der Strafverfolgung neue Befugnisse (etwa zur Überwachung digitaler Endgeräte) geschaffen.

Erst in der jüngeren Vergangenheit wurde Cybersicherheitspolitik vermehrt auch auf Basis anderer theoretischer Zugänge analysiert. Immer häufiger greifen ForscherInnen dabei bspw. Ansätze der Science and Technology Studies (STS) auf. In diesen Studien wird das (Wechsel)Verhältnis zwischen technischer Infrastruktur und Gesellschaft näher beleuchtet und Perspektiven problematisiert, die einen einseitigen technischen Determinismus vertreten. Daniel McCarthy (2015) verbindet in seiner Analyse der amerikanischen Außenpolitik bspw. etablierte (marxistische) Theorien mit Ansätzen der STS. Empirisch erörtert er in seiner Studie, die durch ökonomische Motive geprägte US-amerikanische Internetpolitik, in der Kommunikationstechnologien maßgeblich als Machtressourcen genutzt werden. Dies hat unmittelbar Folgen für die Gestaltung des Netzes (bspw. den Imperativ freier Informationsverbreitung). Madeline Carr (2016a) hat für ihre Studie zu den USA ebenfalls auf die STS zurückgegriffen. Neben der Internet Governance und Netzneutralität widmet sie einen Teil der empirischen Analyse der Cybersicherheitspolitik. Sie arbeitet in diesem Kontext unterschiedliche Auffassungen von Macht heraus und verdeutlicht, wie diese die US-amerikanische Politik geprägt und auf die technische Infrastruktur gewirkt haben.

Nazli Choucri (2012) vergleicht Politiken verschiedener Staaten unter Rückgriff auf die »lateral pressure theory«. Dieser Ansatz geht davon aus, dass staatliches (Außen)Verhalten maßgeblich von der relativen Ausprägung von drei Mastervariablen abhängt: der Verteilung von Ressourcen, Bevölkerung und technologischen Kapazitäten. Anhand der Ausprägung dieser Faktoren teilt Choucri Staaten in sechs Gruppen ein, die sich in ihren Politiken aufgrund der verschiedenen Konfigurationen der Mastervariablen unterscheiden. Nach Choucri gehört bspw. Deutschland zur Profilgruppe 6, diese zeichnet sich durch ein hohes technologisches Niveau, eine relativ dazu geringere Bevölkerungszahl und wenige Ressourcen aus. Für diese Konstellation erwartet die Theorie, dass Staaten ihre Ressourcenschwäche durch eine Ausdehnung im Cyberspace kompensieren, die durch die technologischen Fähigkeiten ermöglicht wird. Staaten aus diesen Gruppen sollten daher zur Führungsgruppe im Cyberspace zählen. Ausgehend hiervon skizziert Choucri ferner verschiedene idealtypische Entwicklungspfade für den Cyberspace, die durch unterschiedliche Konfliktträchtigkeit und einen varianten Einfluss privater Akteure gekennzeichnet sind.

4. Vergleichende Sicherheitspolitik- und Konfliktforschung

Theoriegeleitete und zugleich empirisch gesättigte Forschung zu staatlichen Cybersicherheitspolitiken ist rar. Die meisten empirischen Studien zu Cybersicherheitspolitiken befassen sich mit den USA, China oder Russland (Sliwinski 2014, 468; Christou 2017, 3). Vor diesem Hintergrund ist auch eine dominant militaristische Ausdeutung von Cybersicherheit und cyber power (siehe oben) erklärlich, die sich vielfach mit alarmistischem Unterton mit der veränderten Bedrohungslage sowie mit dem Ausbau offensiver und defensiver Kapazitäten im Cyberraum befasst hat (siehe Abschnitt 2) und mitverantwortlich ist für die konzeptuelle Aufladung, die sich etwa in der Rede vom Cyberkrieg niederschlägt (Dunn Cavelty 2018).

Empirische Analysen von politischen Cyberangriffen beschränken sich zumeist auf Einzelfallstudien besonders prominenter Vorfälle. ForscherInnen haben sich in diesem Kontext mit den Angriffen gegen Estland 2007 (Herzog 2011; Ottis 2008), Stuxnet (Farwell/Rohozinski 2011; Jenkins 2013; Zetter 2014; Lindsay 2013), dem Sony- (Sharp 2017; Shaw/Jenkins 2017; Sullivan 2016) oder DNC-Hack (Lam 2018; Jamieson 2018) befasst. Darüber hinaus gibt es vergleichende Studien mit begrenzten Fallzahlen (Blank 2017; Boyte 2017; Tikk et al. 2010), die aber den Kreis der untersuchten Fälle kaum erweitern, sondern meist den bereits erwähnten Vorfällen verhaftet bleiben. Einer fundierten quantitativen Analyse des Cyberkonfliktgeschehens fehlt nach wie vor eine systematische Datengrundlage, wie sie zur strukturierten Analyse konventioneller Konflikte in Form verschiedener Datensätze besteht (bspw. im Projekt Correlates of War). Zwar haben unterschiedliche Organisationen begonnen, Listen mit politischen Cyberangriffen anzulegen (CSIS 2019; Council on Foreign Relations 2019), sie sind aufgrund ihrer Struktur aber kaum quantitativ auswertbar. Eine Ausnahme bildet der Dyadic Cyber Incident and Dispute Datensatz von Brandon Valeriano und Ryan Maness (2014, 2015). Dieser verzeichnet in der aktuellen Version (1.5) 266 Cyberangriffe mit staatlicher Beteiligung die zwischen 2000 und 2014 ausgeführt wurden. Empirische Analysen auf dieser Grundlage haben gezeigt, dass das Konfliktverhalten im Cyberspace durch staatliche Zurückhaltung geprägt ist. Die niedrige Konfliktintensität führen die Autoren dabei unter anderem darauf zurück, dass die Regierungen eine eskalative Dynamik (ggf. auch offline) fürchten und keine Präzedenzfälle schaffen wollen (Valeriano/Maness 2014). Auch wenn mit diesen Datensätzen erste empirische Analysen möglich geworden sind, bestehen in diesem Kontext immer noch Desiderate etwa zum Konfliktverhalten nichtstaatlicher Akteure. Weitere Datensätze zur Erfassung politischer Cyberangriffe befinden sich derzeit im Aufbau (Steiger et al. 2018) und könnten ebenfalls dazu beitragen, den militärischen Fokus empirisch infrage zu stellen und weitere empirische Blindstellen auszuleuchten.

Passend zu den verbreiteten Katastrophenerzählungen, doch im Kern aufgrund der Verwundbarkeit in diesen sensiblen Bereichen nicht unbegründet, hat gerade

der Schutz kritischer Infrastrukturen einen zentralen Platz in den Cybersicherheitsstrategien der Staaten, von inter- und supranationalen Institutionen eingenommen. Infrastrukturen, wie die Energie- und Wasserversorgung, sind mittlerweile von funktionierender IT derart abhängig, dass durch Cyberangriffe auch die Versorgung mit diesen Gütern beeinträchtigt werden kann. Zahlreiche Studien haben sich daher mit diesen neuen gesellschaftlichen Verwundbarkeiten befasst (Assaf 2008; Brem 2015; Brunner/Suter 2009; Chung 2018). Die Forschung hat dabei untersucht, wie Kooperationen zum Schutz kritischer Infrastrukturen – Public-Private-Partnerships – gestaltet sind (Bossong/Wagner 2016; Carr 2016b; Christensen/Petersen 2017; Freiberg 2015). Aber auch eine internationale Kooperation ist aufgrund der zunehmenden Vernetzung angebracht, da der nationale Handlungsrahmen kaum angemessene Reaktionen erlaubt. Dies gilt sowohl für transnational agierende Kriminelle als auch für die Regulierung kritischer Infrastrukturen, die über nationalstaatliche Grenzen hinweg verbunden sind, so dass durch die Vernetzung die (Un)Sicherheit der Nachbarländer schnell zum Problem für andere werden kann.

Doch nicht nur im Hinblick auf Schutz und Verteidigung werden die Rolle des Staates und seine Handlungsspielräume relativiert. Auch auf der Angreiferseite wird längst nicht ausschließlich das Handeln staatlicher Akteure untersucht. Der Perspektivwechsel, hin zu nichtstaatlichen Akteuren, geht dabei auch auf die staatliche Zurückhaltung beim Einsatz ihrer Cyberkapazitäten zurück. In diesem Kontext stehen nicht nur nichtstaatliche Akteure allein im Mittelpunkt akademischer Aufmerksamkeit, vielmehr haben WissenschaftlerInnen begonnen das Verhältnis zwischen Staaten und solchen nichtstaatlichen Akteuren zu beleuchten, die entweder direkt in staatlichem Auftrag agieren oder von diesen zumindest geduldet werden (Proxies, siehe Maurer 2016, 2018; Borghard/Lonergan 2016).

Die nichtstaatlichen Akteure, die den Cyberspace zu ihren Zwecken nutzen und dabei IT-Sicherheit unterminieren, beschränken sich aber nicht auf staatlich beauftragte »proxies«, sondern umfassen bspw. auch etablierte Terrororganisationen und sogenannte Hacktivists. Die Praktiken und Cyberkapazitäten dieser Akteursgruppierungen wurden ebenfalls von der Forschung analysiert. ForscherInnen haben hierbei unter anderem herausgearbeitet, dass der Cyberspace Machtgefälle einebnen kann und somit nichtstaatliche Akteure gegenüber Staaten an Einfluss gewinnen (Colarik/Ball 2016). Wie im Bereich des militärischen Cyberkrieges divergieren aber auch in diesem Kontext die Gefahreneinschätzungen, die mit dieser Verschiebung einhergehen (Heickerö 2014). Während Untersuchungen einerseits vor einer wachsenden Wahrscheinlichkeit folgenreicher terroristischer Angriffe warnen (Albahar 2017), haben andere empirische Studien betont, dass die Gefahr eines substanziellen Cyberangriffs bspw. durch den IS aufgrund begrenzter Fähigkeiten derzeit gering ist (Bernard 2017).

Nicht zuletzt durch das Attributionsproblem (siehe unten) begünstigt, verschwimmen im Cyberspace die Differenzen zwischen staatlichem und nichtstaatlichem Handeln im Bereich der Cybersicherheit. Das entsprechende Konfliktgeschehen zeichnet sich durch besonders heterogene Akteurskonstellationen aus. Auch diese verändern die Handlungsspielräume nationalstaatlicher Sicherheitspolitik (Schmitt/Watts 2016; Egloff 2017). Die dadurch hervorgerufenen Ungewissheiten beeinflussen das Sicherheitsempfinden und verändern die Grundlagen für staatliche Verantwortungsübernahme und sicherheitspolitisches Handeln. Passend zur zunehmend diskutierten Hybridität von Cyberkonflikten, hat sich in den vergangenen Jahren parallel zur gesellschaftspolitischen Debatte in vielen Ländern, darunter auch demokratischen Staaten, ein Forschungsstrang entwickelt, der zunehmend auch propagandistische und sog. Desinformationskampagnen als Bedrohungen der Cybersicherheit und Elemente hybrider Kriegführung aufgreift. Diese jüngste Tendenz, welche auch bei ausbleibender Zunahme der Konfliktintensität im Cyberspace eine kontinuierliche Bedrohungswahrnehmung erlaubt, soll im letzten Abschnitt dieses Beitrags kritisch diskutiert werden.

5. Internationale Normenforschung

Angesichts der begrenzten staatlichen Steuerungsspielräume in diesem Bereich haben sich die internationale Normenforschung und das internationale Recht ebenfalls der Cybersicherheit als Gegenstand zugewandt. Dabei stellen Internet und Digitalisierung die genannten Disziplinen vor besondere Herausforderungen, denn zum einen stellt der potentiell transnational verlaufende Datenverkehr den territorialen Bezug staatlicher (Sicherheits-)Politik grundlegend infrage (s. auch den Beitrag von Pfetsch et al. 2019 in diesem Band). Tradierte Struktur- und Politikdifferenzen, hier insbesondere zwischen innerer und äußerer Sicherheit, sind stärker noch als auf anderen globalisierten Feldern herausgefordert. Cyber(un)sicherheit beschreibt einen transnationalen Phänomenbereich, in dem geografische Distanzen und territoriale Grenzen weniger bedeutsam sind (Cairncross 2001; Tabansky 2011; Kello 2013).

Aus der technischen Architektur sowie aus den transnationalen Konnektivitätsansprüchen der Internetnutzung resultiert auch das sog. Attributionsproblem, mit dem sich zahlreiche Untersuchungen im Feld befassen (Rid/Buchanan 2014; Canfil 2016; Guitton 2017). Demnach ist es technisch schwer nachvollziehbar, wo, etwa in welchem Land, im In- oder Ausland, Cyberangriffe ihren Ursprung haben.

Relativ frühe Bestrebungen zur internationalen Normsetzung sind auf dem Feld internationaler Verbrechensbekämpfung sichtbar geworden, so wie bspw. die 2001 verabschiedete Convention on Cybercrime. Entstehungsprozess und Inhalte des Abkommens wurden verschiedentlich wissenschaftlich untersucht (Clough

2012; Kierkegaard 2008; Marion 2010). Demgegenüber bestehen derzeit keine verbindlichen Regeln zur Regulation staatlichen Konfliktverhaltens im Cyberspace. Die sog. Tallinn Manuals stellen bis heute die umfassendsten völkerrechtlichen Entwürfe dar, sie entstammen allerdings einem wissenschaftlichen Entstehungskontext und sind nicht verbindlich. In ihrem Anspruch, ein ius ad bellum und in bello (also Recht zum Krieg und Recht im Krieg) zu entwerfen, ist insbesondere die erste Fassung (Schmitt 2013) zudem nicht geeignet, die konzeptionelle Fixierung auf das Kriegsgeschehen (siehe oben) zu überwinden. Weiterhin wurde (auch im Rahmen des Tallinn Manual 2.0) der Frage nachgegangen, welche Sorgfaltsverantwortung (due diligence) den Staaten in diesem neuen Handlungsraum obliegt (Buchan 2016; Couzigou 2018; Liu 2017; Schmitt 2017). Ein starker militärischer Fokus findet sich daneben auch in Publikationen, die aus (völker-)rechtlicher oder ethischer Perspektive bspw. die Zulässigkeit von Cyberangriffen evaluieren oder die Übertragbarkeit des Konzepts des Gerechten Krieges auf den Cyberspace prüfen und Cyberangriffe mit kinetischen Angriffen vergleichen (Barrett 2015; Finlay 2018; Durante 2015; Goldsmith 2013).

Innerhalb der Vereinten Nationen wurde seit Ende der 1990er Jahre wiederholt über verbindliche Regelungen zu staatlichem Verhalten im Cyberspace debattiert (Maurer 2011). Die letzte Runde der ExpertInnenkonsultationen (GGE) konnte 2017 aber keinen gemeinsamen Bericht vorlegen, da bspw. über die Auslegung des Selbstverteidigungsrechts im Cyberspace substanzielle Differenzen bestanden (Henriksen 2019). ForscherInnen haben entsprechend argumentiert, dass die Regulation staatlichen Verhaltens im Cyberspace bisher noch nicht über »quasi-norms« hinausgegangen ist (Erskine/Carr 2016, s. auch Finnemore/Hollis 2016).

Zur Frage der internationalen Normentwicklung passt die bislang vornehmlich aus dieser Perspektive erfolgte Untersuchung des europäischen Ansatzes in der Cybersicherheitspolitik. Denn dieser sieht in verschiedener Hinsicht (politische Verhandlungsressourcen, Marktmacht, innovative Governance-Formen, Werteorientierung und soft power) eine mögliche Ausnahmerolle für die EU in der internationalen Normentwicklung (Kettemann et al. 2018). In diesem Sinne haben VertreterInnen einer dezidierten Forschung zur EU-Cybersicherheitspolitik betont, dass angesichts der transnationalen Herausforderungen der Cybersicherheitspolitik ein europäischer Ansatz zur Problemlösung geboten sei (Sliwinski 2014, 476; Carrapico/Barrinha 2018). In der Realität indes sucht die EU erkennbar nach ihrer Rolle, die sie zwischen anderen Staaten, nichtstaatlichen Akteuren und den Mitgliedsstaaten einnehmen kann und soll (Klimburg/Tirmaa-Klaar 2011).

Wo die EU-Cybersicherheitspolitik erforscht wird, erfolgt dies zumeist aus den aus der Forschung zur EU-Außen- und Sicherheitspolitik vertrauten Blickwinkeln. So wird der EU auch in diesem Feld attestiert, die typischen Defizite in ihrer Akteurschaft sowie der Kohärenz ihrer Handlungen aufzuweisen. Passend zu dieser Orientierung an bestehender Forschung stellt eine Reihe von ForscherInnen eine

besondere Wertorientierung der EU-Cybersicherheitspolitik fest, die sich bspw. im Verzicht auf eine Militarisierung der Cybersicherheit manifestiert (Bendiek 2018; Dunn Cavelty 2018). Die empirischen Befunde variieren dabei mit den verwendeten Akteurs- bzw. Machtbegriffen, an denen die EU gemessen wird sowie mit den analysierten Politikbereichen bzw. mit den zum Vergleich genutzten Kontrastfolien (meist die NATO). Inwiefern diese Politik aktiv gewählt und angestrebt wird oder ob sie nicht aus dem Beharren auf sicherheitspolitische Souveränität der Mitgliedsstaaten folgt, wird zumeist nicht problematisiert.

Gerade an der Schnittmenge zwischen Datenschutz und Cybersicherheitspolitik hat die Europäische Union in Reformtätigkeit und politischem Handeln in der jüngeren Vergangenheit im Hinblick auf ihre Werteorientierung kein einheitliches Bild hinterlassen (Busch 2012; Ripoll Servent 2017; Schünemann 2019b). Auch in dem in jüngerer Zeit intensiver diskutierten Problemfeld Desinformation und Manipulation öffentlicher Meinung zeigen die Organe der Europäischen Union in Teilen Tendenzen zu sicherheitspolitischen Lösungen (EU-Kommission 2018), die im Folgenden behandelt werden sollen.

6. Wider neue Tendenzen der Versicherheitlichung – Plädoyer für einen Perspektivwechsel

Insbesondere seit den US-Präsidentschaftswahlen und dem britischen Referendum über die Mitgliedschaft in der EU 2016 wird öffentlich zunehmend über die Beeinflussung des demokratischen Entscheidungsprozesses durch die Verbreitung von Desinformationen und Propaganda diskutiert. Die Bedrohungswahrnehmung wird durch den mutmaßlichen oder tatsächlichen Ursprung derartiger Operationen im Ausland sowie den Verdacht auf Automatisierung von Informationskampagnen (Social Bots) erheblich gesteigert. Im Zuge dessen ist eine weitere Aufladung des Verständnisses von Cybersicherheit zu beobachten, denn die genannten Phänomene werden immer häufiger unter den vielfältigen »Cyber-Gefahren« subsumiert (Spektrum.de 2019) und zusammengenommen dem sicherheitspolitischen Problem- und Aktivitätsfeld zugeschlagen, augenscheinlich ohne großen Widerspruch in der gesellschaftspolitischen Debatte. Schon im Weißbuch der deutschen Bundesregierung zur Sicherheitspolitik und zur Zukunft der Bundeswehr aus dem Jahr 2016 wird die Verbreitung von Propaganda im Internet erörtert. Zwar unterscheidet die Regierung hierbei konzeptionell zwischen Cyberangriffen und Informationsoperationen, rückt aber beides in den Zuständigkeitsbereich der Sicherheitsbehörden (Bundesregierung 2016, 39). Einen zurückhaltenderen, dezidiert auf Mittel der Medienregulierung setzenden Ansatz wählte die Bundesregierung (ausgehend vom Justizministerium) im Vorfeld der Bundestagswahlen, als sie das ebenfalls umstrittene Netzwerkdurchsetzungsgesetz (NetzDG) verabschiede-

te, das im Rahmen der Co-Regulierung den Betreibern großer sozialer Netzwerke Löschpflichten im Kampf gegen rechtswidrige Inhalte auferlegt.

Der sicherheitspolitische Ansatz ist demgegenüber in jüngerer Zeit erneut auf EU-Ebene sichtbar geworden (siehe oben). So haben die Europäische Kommission und die Hohe Vertreterin für die Außen- und Sicherheitspolitik im Dezember 2018 einen Aktionsplan Desinformation verabschiedet, der die Verbreitung von Desinformation und ausländischer Propaganda explizit als sicherheitspolitische Herausforderung rahmt und entsprechende Maßnahmen fordert (EU-Kommission 2018).

Auf wissenschaftlicher Seite steht eine viel beachtete Untersuchung von Kathleen Hall Jamieson exemplarisch für diesen Trend. In ihrem Buch »Cyberwar – How Russian Hackers and Trolls Helped Elect a President« (Jamieson 2018) beschreibt sie die viel diskutierten mutmaßlich russischen Beeinflussungen des US-Präsidentschaftswahlkampfs 2016 als eine Form des Krieges (siehe auch Kurz/Rieger 2018; Maness 2019). Sie rechtfertigt die Begriffswahl unter anderem durch Bezug auf Richard A. Clarke, der den Kriegsbegriff bereits in den beginnenden 2010er Jahren prominent vertreten hat und auch in diesem Kontext wieder betonte (Jamieson 2018, 8) sowie durch Verweis auf die Äußerungen von prominenten PolitikerInnen wie Nancy Pelosi, die die Ereignisse ebenfalls als Krieg bezeichnete:

> »This is a very big deal. What we're talking about is cataclysmic. It is cyber warfare. A major foreign power with sophistication and ability got involved in our presidential election.« (Pelosi, zitiert nach Jamieson 2018, 9)

Das Textbeispiel steht exemplarisch für einen neuen Trend der Versicherheitlichung, der nach der Ernüchterung der Debatte über tatsächlich »heiße« Cyberkriege ansetzt, aber durch Hinzuziehung propagandistischer Mittel eine noch größere und drängendere Aufladung des Sicherheitsbegriffs vornimmt. Aufgrund der häufigen Unklarheit unterstellter Rechtsbrüche durch Desinformation und die schwierige Abgrenzung von legalen Kommunikationsakten in einer freien (auch transnationalen) Online-Kommunikationsumgebung steht zu befürchten, dass die Legitimationsstrategien der Sekuritisierungsagenten noch weitreichendere Eingriffe mittels Überwachung und Content-Regulierung beinhalten, als es bislang der Fall war. Aufgrund hoher Sensibilität für die Integrität des demokratischen Systems insbesondere in Wahlkampfzeiten ist zudem anzunehmen, dass die Chancen auf Legitimierung in der Bevölkerung vergleichsweise gut stehen. Augenscheinlich werden auch die weitaus niedrigschwelligeren Aktivitäten von Staaten oder anderen Akteuren zunehmend zur Rechtfertigung sicherheitspolitischer (Gegen-)Maßnahmen genutzt. Damit scheint ausgerechnet die von den kritischen Sicherheitsstudien beförderte Erkenntnis, wonach Staaten nicht zum folgenschweren offensiven Einsatz ihrer Cyberkapazitäten neigen und ein Cyberkrieg in diesem Sinne unwahrscheinlich ist, ohne bleibenden Folgen für die wissenschaftliche und öffentliche Debatte geblieben zu sein. Der Fokus auf katastrophenförmige Szenarien

folgenschwerer Cyberangriffe ist lediglich durch eine gesteigerte (konjunkturelle) Aufmerksamkeit für Desinformationskampagnen ersetzt worden, ohne (politisch wie oft auch wissenschaftlich) das konzeptionelle Vokabular angemessen anzupassen.

Interessanterweise ist auch in diesem jüngeren Literaturstrang erneut zu beobachten, wie mit einiger Selbstverständlichkeit von Cyberkrieg die Rede ist (Jamieson 2018; Kurz/Rieger 2018; Maness 2019), vielfach ohne erneut kritisch zu fragen, ob der Begriff den Phänomenen angemessen ist und inwiefern die Ereignisse überhaupt Kernbereiche der Cybersicherheit berühren. Eine Bezugnahme auf die Kerndefinition der IT-Sicherheit kann als Bemessungsrahmen Klarheit über konzeptionelle Unterschiede der diskutierten Phänomene herstellen und ferner helfen, die angemessene regulatorische Zuständigkeit besser einzuschätzen. Betrachtet man etwa die Ereignisse vor der US-Präsidentschaftswahl, an denen sich die aktuelle Problemwahrnehmung entzündet hat, zeigt sich, dass viele der diskutierten Themen nicht den eigentlichen Bereich der IT-Sicherheit betreffen (etwa das Agieren sog. Trolle, die Verbreitung von Desinformation, Social Bots etc.). Hierbei handelt es sich eher um überwiegend niedrigschwellige »information operations« (Ruhmann/Bernhardt 2014). Sie fallen in die Bereiche strategischer Kommunikation und – womöglich staatlich gesteuerter – Propaganda. Hierbei geht es also um Maßnahmen, die darauf zielen, Informationen sowie deren Fluss und Rezeption zu den eigenen Gunsten zu beeinflussen.

Zu den Schwierigkeiten mit dieser erweiterten Problemwahrnehmung gehört auch, dass die Bedrohungsperzeption sich bislang nicht mit den bestenfalls uneindeutigen empirischen Befunden in Einklang bringen lässt. So sind die Wirkungen von Desinformationskampagnen auf gesellschaftliche Debatten bisher nur unzureichend erforscht. Empirische Untersuchungen, etwa zu den USA (Allcott/Gentzkow 2017) geben jedenfalls wenig Anlass zur Beunruhigung. Auch die Auswirkungen der Automatisierung sind, wie die Debatte um Social Bots gezeigt hat, ebenfalls sehr hypothetisch. Bislang konnten auch hier keine empirisch belastbaren Aussagen über deren Wirkungsweisen und tatsächlichen Wirkungen von Bot-Kommunikation formuliert werden (Ihieltges/Hegelich 2018). Es reicht nicht aus, zu wissen, dass eine von Russland finanzierte Werbung 126 Millionen Facebook-UserInnen (The New York Times 2017) erreicht hat, um von einer substanziellen Manipulation zu sprechen. Die Einschätzung der Gefahr sollte daher stets kritisch reflektiert werden – eine pauschale Annahme des »Worst-Case« scheint auf Grundlage der empirischen Evidenz nicht angemessen und im Kontext neuer Sekuritisierungstendenzen jedenfalls nicht hilfreich.

Der sicherheitspolitische Fokus auf die Verbreitung von Desinformationen ist für liberale Demokratien in ganz grundlegender Hinsicht problematisch. Denn Forderungen nach staatlicher Überwachung und Intervention greifen tief in die demokratischen Freiheitsrechte ein. Die Regulationsforderungen zur Bekämpfung

von Desinformationen in demokratischen Wahlkämpfen sind angesichts der nicht nachgewiesenen Wirkungen und der Tiefe der Eingriffe besonders kritisch zu beurteilen, rufen sie doch in einer Hochphase des politischen Wettbewerbs dazu auf, das politische System vor der freien Rede zu schützen und Wahrheit von Lüge zu trennen. Abgesehen davon, dass schon dieses Schutzbedürfnis für liberale Demokratien nicht unbedingt angemessen ist: Wer sollte in der Position sein, die Entscheidung über Wahrheit oder Lüge, Desinformation oder bloße Zuspitzung im Wahlkampf zu treffen?

7. Schlussüberlegungen und Ausblick

Cybersicherheit ist ein vieldeutiger und schillernder Begriff. Er geht im Kern und Ursprung von einem technischen Verständnis von IT-Sicherheit aus. Sein Gebrauch geht aber weit darüber hinaus, denn dieser umfasst ebenso klassische Sicherheitsbedrohungen und ihre digitalen Transformationen wie gesellschaftliche und politische Aufladungen als Ergebnisse von Versicherheitlichungsdiskursen. Die sozial- und im Besonderen die politikwissenschaftliche Cybersicherheitsforschung kann diese weiteren Begriffsdimensionen nicht unberücksichtigt lassen. In den vorangegangenen Abschnitten haben wir einen Überblick über das dementsprechend heterogene Feld der politikwissenschaftlichen Cybersicherheitsforschung gegeben. Im Einzelnen haben wir einen strategisch-militärpolitischen Zugang von der Auseinandersetzung mit Begriff und Aufladungen aus Perspektive der kritischen Sicherheitsstudien unterschieden. Darüber hinaus haben wir uns mit ersten empirischen Vergleichsstudien aus der Sicherheitspolitik- und Konfliktforschung befasst. Hierin sehen wir ein besonderes Potential, die dichte Beschreibung einzelner prominenter Cybersicherheitsvorfälle durch empirisch gesättigte vergleichende Befunde zu ergänzen. Studien dieser Art sind nicht zuletzt hilfreich, um die Bindewirkung internationaler Normen zu ermessen. Die internationale Normentwicklung im Bereich Cybersicherheit haben wir zudem als Gegenstand eines eigenen Subfelds identifiziert und die Grundlinien der darin überwiegenden völkerrechtlichen und politikwissenschaftlichen Arbeiten skizziert. Schließlich haben wir mit den aktuell diskutierten Bedrohungsszenarien für den öffentlichen Raum und den demokratischen Prozess neue Tendenzen der erweiterten Cybersicherheitsdebatte vorgestellt und kritisch diskutiert.

Insgesamt ergeben sich für die wissenschaftliche Forschung zu Cybersicherheit im Lichte der vorangegangenen Abschnitte die folgenden Desiderate: Erstens sind die kritischen Sicherheitsstudien gefragt, aktuelle Problemwahrnehmungen, Debatten und politische Maßnahmenkataloge zur Bekämpfung von Desinformation und (ausländischer) Propaganda im Netz auf Sekuritisierungstendenzen hin kritisch zu untersuchen. Zweitens sollten die Darstellungen von Sicherheitsbe-

drohungen durch empirische Studien überprüft und fundiert werden. Drittens ist zu wünschen, dass sich das Feld vergleichender Cybersicherheitsforschung weiter ausbildet und zugängliche Datensätze für die empirische Analyse auf- oder ausgebaut werden. Viertens plädiert der Beitrag dafür, dass dort, wo empirische Überprüfungen etwa aufgrund mangelnder Datenverfügbarkeit nicht möglich sind, auf die schwerpunktmäßige Darstellung von Worst-case-Szenarien und alarmistische Töne verzichtet wird. Im Hinblick auf den politischen Handlungsrahmen und die zunehmend diskutierte Regulation von Online-Kommunikation sollte fünftens zwischen sicherheitspolitischen Bedrohungen und medienregulatorischen Herausforderungen differenziert werden.

Literaturverzeichnis

Albahar, Marwan (2017): Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. In: Science and engineering ethics.

Allcott, Hunt/Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. In: Journal of Economic Perspectives 31 (2), S. 211–236.

Andress, Jason (2015): The basics of information security. Understanding the fundamentals of InfoSec in theory and practice. 2. Auflage. Waltham, MA, Amsterdam.

Arquilla, John (2013): Twenty Years of Cyberwar. In: Journal of Military Ethics 12 (1), S. 80–87. DOI: 10.1080/15027570.2013.782632.

Arquilla, John/Ronfeldt, David (1993): Cyberwar is coming! In: Comparative Strategy 12 (2), S. 141–165.

Assaf, Dan (2008): Models of critical information infrastructure protection. In: International Journal of Critical Infrastructure Protection 1, S. 6–14.

Barrett, Edward T. (2015): Reliable Old Wineskins. The Applicability of the Just War Tradition to Military Cyber Operations. In: Philosophy & Technology 28 (3), S. 387–405.

Bendiek, Annegret (2018): Die EU als Friedensmacht in der internationalen Cyberdiplomatie (SWP-Aktuell).URL:berlin.org/fileadmin/contents/products/aktuell/2018A22_bdk.pdf (14.05.2019).

Bendrath, Ralf/Eriksson, Johan/Giacomello, Giampiero (2007): From ›cyberterrorism‹ to ›cyberwar‹, back and forth: How the United States securitized cyberspace. In: Eriksson/Giacomello (Hg.): International relations and security in the digital age. London und New York, S. 57–82.

Bernard, Rose (2017): These are not the terrorist groups you're looking for. An assessment of the cyber capabilities of Islamic State. In: Journal of Cyber Policy, S. 1–11.

BfDI (2019): Der Bundesdatenschutzbeauftragte stellt seinen 27. Tätigkeitsbericht vor. Positive Bilanz der Datenschutz-Grundverordnung, Kritik an immer mehr Befugnisse für Grundrechtseingriffe der Sicherheitsbehörden. URL: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/16_27_TB.html (14.05.2019).

Blank, Stephen (2017): Cyber War and Information War à la Russe. In: George Perkovich und Ariel Levite (Hg.): Understanding cyber conflict. Fourteen analogies. Washington, DC, S. 81–98.

Borghard, Erica D./Lonergan, Shawn W. (2016): Can States Calculate the Risks of Using Cyber Proxies? In: Orbis 60 (3), S. 395–416.

Bossong, Raphael/Wagner, Ben (2016): A typology of cybersecurity and public-private partnerships in the context of the EU. In: Crime, Law and Social Change.

Boyte, Kenneth J. (2017): A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine. Exemplifying the Evolution of Internet-Supported Warfare. In: International Journal of Cyber Warfare and Terrorism 7 (2), S. 54–69.

Brem, Stefan (2015): Critical Infrastructure Protection from a National Perspective. In: European Journal of Risk Regulation 6 (02), S. 191–199.

Brunner, Elgin M./Suter, Manuel (2009): International CIIP Handbook 2008/2009. URL: www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf (14.05.2019).

Buchan, Russell (2016): Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm. In: Journal of Conflict and Security Law 21 (3), S. 429–453.

Bundesgesetzblatt (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).URL: www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf (14.05.2019).

Bundesregierung (2016): Weissbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. URL: https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-bmvg-data.pdf (14.05.2019).

Busch, Andreas (2012): Die Regulierung transatlantischer Datenströme: zwischen Diktat und Blockade. In: Busch/Hofmann (Hg.): Politik und die Regulierung von Information. Baden-Baden, S. 408–440.

Cairncross, Frances (2001): The death of distance. How the communications revolution is changing our lives. Boston.

Canfil, Justin Key (2016): Honing Cyber Attribution: A Framework for assessing foreign state complicity. In: Journal of International Affairs 70 (1), S. 217–226.

Carr, Madeline (2016a): US Power and the Internet in International Relations: The Irony of the Information Age. London.

Carr, Madeline (2016b): Public-private partnerships in national cyber-security strategies. In: International Affairs 92 (1), S. 43–62.

Carrapico,Helena/Barrinha, Andre (2018): European Union cyber security as an emerging research and policy field. In: European Politics and Society 19 (3), S. 299–303.

Choucri, Nazli (2012): Cyberpolitics in international relations. Cambridge, Massachusetts.

Christensen, Kristoffer Kjærgaard/Petersen, Karen Lund (2017): Public–private partnerships on cyber security. A practice of loyalty. In: International Affairs 93 (6), S. 1435–1452.

Christou, George (2017): The EU's Approach to Cybersecurity: Challenges and Opportunities. URL: http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf (14.05.2019).

Chung, John J. (2018): Critical Infrastructure, Cybersecurity, and Market Failure. In: Oregon Law Review 96 (2), S. 441–476.

Clarke, Richard A./Knake, Robert K. (2010): Cyber war. The Next Threat to National Security and What to Do About It. New York.

Clough, Jonathan (2012): The Council of Europe Convention on Cybercrime. Defining ›Crime‹ in a Digital World. In: Criminal Law Forum 23 (4), S. 363–391.

Colarik, Andrew/Ball, Rhys (2016): Anonymous Versus ISIS. The Role of Non-state Actors in Self-defense. In: Global Security and Intelligence Studies 2 (1).

Council on Foreign Relations (2019): Cyber Operations Tracker. URL: https://www.cfr.org/interactive/cyber-operations (14.05.2019).

Couzigou, Irène (2018): Securing cyber space. The obligation of States to prevent harmful international cyber operations. In: International Review of Law, Computers & Technology 32 (1), S. 37–57.

CSIS (2019): Significant Cyber Incidents. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf.

Dunn Cavelty, Myriam (2008): Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. In: Journal of Information Technology & Politics 4 (1), S. 19–36.

Dunn Cavelty, Myriam (2010): Cyber-threats. In: Dunn Cavelty/Mauer (Hg.): The Routledge handbook of security studies. Milton Park, Abingdon, Oxon, New York, S. 180–189.

Dunn Cavelty, Myriam (2012): The Militarisation of Cyberspace: Why Less May Be Better. In: Czosseck/Ottis/Ziolkowski (Hg.): 2012 4th International Conference on Cyber Conflict. Proceedings. Piscataway, NJ: IEEE, S. 141–153.

Dunn Cavelty, Myriam (2013): Der Cyber-Krieg, der (so) nicht kommt. Erzählte Katastrophen als (Nicht)Wissenspraxis. In: Hempel/Bartels/Markwart (Hg.): Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart. Bielefeld, S. 209–234.

Dunn Cavelty, Myriam (2018): Europe's cyber-power. In: European Politics and Society 19 (3), S. 304–320.

Dunn Cavelty, Myriam/Jaeger, Mark Daniel (2015): (In)visible Ghosts in the Machine and the Powers that Bind. The Relational Securitization of Anonymous. In: International Political Sociology 9 (2), S. 176–194.

Durante, Massimo (2015): Violence, Just Cyber War and Information. In: Philosophy & Technology 28 (3), S. 369–385.

Egloff, Florian (2017): Cybersecurity and the Age of Privateering. In: Perkovich/Levite (Hg.): Understanding cyber conflict. Fourteen analogies. Washington, DC, S. 231–247.

Erskine, Toni/Carr, Madeline (2016): Beyond ›Quasi-Norms‹: The Challenges and Potential of Engaging with Norms in Cyberspace. In: Osula/Rõigas (Hg.): International cyber norms. Legal, policy & industry perspectives. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, S. 87–110.

EU (2016): Richtlinie (EU) 2016/1148. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148 (14.05.2019).

EU-Kommission (2018): Aktionsplan gegen Desinformation. JOIN (2018) 36 final.

Farwell, James P./Rohozinski, Rafal (2011): Stuxnet and the Future of Cyber War. In: Survival 53 (1), S. 23–40.

Finlay, Christopher J. (2018): Just War, Cyber War, and the Concept of Violence. In: Philosophy & Technology 9 (4), S. 384.

Finnemore, M./Hollis, D. B. (2016): Constructing Norms for Global Cybersecurity. In: American Journal of International Law 110 (3), 425–479.

Freiberg, Michael (2015): Grenzen und Möglichkeiten der öffentlich-privaten Zusammenarbeit zum Schutz Kritischer IT-Infrastrukturen am Beispiel des Umsetzungsplan KRITIS. In: Lange/Bötticher (Hg.): Cyber-Sicherheit. Wiesbaden, S. 103–120.

Freedom House (2018): Freedom on the Net 2018. The Rise of Digital Authoritarianism. New York/Washington. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf (14.05.2019).

Gartzke, Erik (2013): The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. In: International Security 38 (2), S. 41–73

Gaycken, Sandro (2011): Cyberwar. Das Internet als Kriegsschauplatz. München.

Gaycken, Sandro (2012): Cyberwar – Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand. München.

Gilbert Ramsay (2016): ›Terrorist‹ Use of the Internet: An Overblown Issue. In: Middle East – Topics & Arguments 6, S. 88–96.

Goldsmith, Jack (2013): How Cyber Changes the Laws of War. In: European Journal of International Law 24 (1), S. 129–138.

Gorr, David/Schünemann, Wolf J. (2013): Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia. In: International Review of Information Ethics 20, S. 39–51.

Guitton, Clement (2013): Cyber insecurity as a national threat. Overreaction from Germany, France and the UK? In: European Security 22 (1), S. 21–35.

Guitton, Clement (2017): Inside the enemy's computer. Identifying cyber-attackers. New York.

Hansen, Lene/Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School. In: International Studies Quarterly 53 (4), S. 1155–1175.

Heickerö, Roland (2014): Cyber Terrorism. Electronic Jihad. In: Strategic Analysis 38 (4), S. 554–565.

Henriksen, Anders (2019): The end of the road for the UN GGE process. The future regulation of cyberspace. In: Journal of Cybersecurity 5 (1).

Herzog, Stephen (2011): Revisiting the Estonian Cyber Attacks. Digital Threats and Multinational Responses. In: Journal of Strategic Security 4 (2), S. 49–60.

Jamieson, Kathleen Hall (2018): Cyberwar. How russia helped elect a President – What We Don't, Can't, and Do Know. New York.

Jarvis, Lee/Macdonald, Stuart/Whiting, Andrew (2017): Unpacking cyberterrorism discourse. Specificity, status, and scale in news media constructions of threat. In: European Journal of International Security 2 (01), S. 64–87.

Jenkins, Ryan (2013): Is Stuxnet physical? Does it matter? In: Journal of Military Ethics 12 (1), S. 68–79.

Kello, Lucas (2013): The Meaning of the Cyber Revolution. Perils to Theory and Statecraft. In: International Security 38 (2), S. 7–40

Kettemann, Matthias C./Kleinwächter, Wolfgang/Senges, Max (2018): The time is right for Europe to take the lead in global internet governance. URL: http://publikationen.ub.uni-frankfurt.de/files/48008/Governance_Kettemann_Kleinwaechter_Senges.pdf (14.05.2019).

Kierkegaard, Sylvia Mercado (2008): International Cybercrime Convention. In: Janczewski/Colarik (Hg.): Cyber warfare and cyber terrorism. Hershey: Information Science Reference, S. 469–476.

Klimburg, Alexander/Tirmaa-Klaar, Heli (2011): Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU. URL: www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf (14.05.2019).

Kurz, Constanze/Rieger, Frank (2018): Cyberwar – Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können. München.

Leisegang, Daniel (2015): Der cyber- militärische Komplex: Die dunkle Seite des Silicon Valley. In: Wissenschaft & Frieden (2), S. 27–30.

Lam, Christina (2018): A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 US Presidential Election. In: Boston College Law Review 59 (6), S. 2167–2201.

Lewis, James A./Neuneck, Götz (2013): The Cyber Index. International Security Trends and Realities. URL: www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (14.05.2019).

Libicki, Martin C. (2017): The Convergence of Information Warfare. In: Strategic Studies Quarterly Spring, S. 49–65.

Lindsay, Jon R. (2013): Stuxnet and the Limits of Cyber Warfare. In: Security Studies 22 (3), S. 365–404.

Liu, Ian Yuying (2017): The due diligence doctrine under Tallinn Manual 2.0. In: Computer Law & Security Review 33 (3), S. 390–395.

Maness, Ryan C. (2019): A crisis of trust. Transatlantic cybersecurity relations in the post-Snowden era. In: Harnisch/Thies/Friedrichs (Hg.): Crisis across the Atlantic? Institutional Resilience and Democratic Decision-making under Pressure. New York, S. 143–160.

Marion, Nancy E. (2010): The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. In: International Journal of Cyber Criminology 4 (2), S. 699–712.

Maurer, Tim (2011): Cyber norm emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security. URL: https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf (14.05.2019).

Maurer, Tim (2016): ›Proxies‹ and Cyberspace. In: Journal of Conflict and Security Law 21 (3), S. 383–403.

Maurer, Tim (2018): Cyber Mercenaries. The state, hackers, and power. Cambridge.

McCarthy, Daniel R. (2015): Power, information technology, and international relations theory. The power and politics of US foreign policy and the internet. New York.

Nissenbaum, Helen (2005): Where Computer Security Meets National Security. In: Ethics and Information Technology 7 (2), S. 61–73.

Ottis, Rain (2008): Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In: Remenyi (Hg.): Proceedings of the 7th European Conference on Information Warfare and Security. 7th European Conference on Information Warfare and Security. Plymouth, S. 163–168.

Rid, Thomas (2012): Cyber War Will Not Take Place. In: Journal of Strategic Studies 35 (1), S. 5–32.

Rid, Thomas (2013): Cyber war will not take place. Oxford, New York.

Rid, Thomas/Buchanan, Ben (2014): Attributing Cyber Attacks. In: Journal of Strategic Studies 38 (1–2), S. 4–37.

Ripoll Servent, Ariadna (2017): Protecting or processing? Recasting EU data protection norms. In: Schünemann/Baumann (Hg.): Privacy, Data Protection and Cybersecurity in Europe. [S.l.], S. 129–145.

Ruhmann, Ingo/Bernhardt, Ute (2014): Information Warfare und Informationsgesellschaft: Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft & Frieden (1).

Sanger, David E. (2018): The perfect weapon. War, sabotage, and fear in the cyber age. New York.

Schmitt, Michael N. (2013): Tallinn manual on the international law applicable to cyber warfare. Prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge, New York.

Schmitt, Michael N. (2017): Tallinn manual 2.0 on the international law applicable to cyber operations. New York.

Schmitt, Michael N./Watts, Sean (2016): Beyond State-Centrism. International Law and Non-state Actors in Cyberspace. In: Journal of Conflict and Security Law 21 (3), S. 595–611.

Schulze, Matthias (2016): (Un)Sicherheit hinter dem Bildschirm: Die Versicherheitlichung des Internets. In: Fischer/Masala (Hg.): Innere Sicherheit nach 9/11. Wiesbaden, S. 165–185.

Schünemann, Wolf J. (2019a, i.E.): Cybersicherheit. In: Klenk/Nullmeier/Wewer (Hg.): Handbuch Digitalisierung in Staat und Verwaltung. Wiesbaden.

Schünemann, Wolf J. (2019b): Business as Usual or Norm Promotion? Divergent Modes and Consequences of Transatlantic Crisis Resilience in Cybersecurity and Data Protection after the Snowden Revelations. In: Harnisch/Thies/Friedrichs (Hg.): Crisis across the Atlantic? Institutional Resilience and Democratic Decision-making under Pressure. New York, S. 126–142.

Schünemann, Wolf J./Harnisch, Sebastian (2015): Cybersicherheit. In: Nohlen/Grotz (Hg.): Kleines Lexikon der Politik.

Sharp, Travis (2017): Theorizing cyber coercion. The 2014 North Korean operation against Sony. In: Journal of Strategic Studies 58 (3), S. 1–29.

Shaw, Tony/Jenkins, Tricia (2017): An Act of War? The Interview Affair, the Sony Hack, and the Hollywood–Washington Power Nexus Today. In: Journal of American Studies 29, S. 1–27.

Sliwinski, Krzysztof Feliks (2014): Moving beyond the European Union's Weakness as a Cyber-Security Agent. In: Contemporary Security Policy 35 (3), S. 468–486.

Singer, Peter W./Friedman, Allan (2014): Cybersecurity. New York, Oxford.

Spektrum.de (2019): Wie Social Bots den Brexit verursachten. URL: https://www.spektrum.de/news/wie-social-bots-den-brexit-verursachten/1423912 (14.05.2019).

Steiger, Stefan/Harnisch, Sebastian/Zettl, Kerstin/Lohmann, Johannes (2018): Conceptualising conflicts in cyberspace. In: Journal of Cyber Policy 3 (1), S. 77–95.

Stiennon, Richard (2015): There Will Be Cyberwar: How the Move to Network-Centric Warfighting Set The Stage For Cyberwar. Birmingham, MI.

Stone, John (2013): Cyber War Will Take Place! In: Journal of Strategic Studies 36 (1), S. 101–108.

Sullivan, Clare (2016): The 2014 Sony Hack and the Role of International Law. In: Journal of National Security Law & Policy 8 (3).

Tabansky, Lior (2011): Basic Concepts in Cyber Warfare. In: Military and Strategic Affairs 3 (1), S. 75–92.

The New York Times (2017): Russian Influence Reached 126 Million Through Facebook Alone. URL: https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html (14.05.2019).

Thieltges, Andree/Hegelich, Simon (2018): Falschinformationen und Manipulation durch social bots in sozialen Netzwerken. In: Blätte et al. (Hg.): Computational Social Science. Die Analyse von Big Data. Baden-Baden, S. 357–377.

Tikk, Eneken/Kaska, Kadri/Vihul, Liis (2010): International Cyber Incidents: Legal Considerations. CCDCOE. URL: https://ccdcoe.org/publications/books/legalconsiderations.pdf (14.05.2019).

Valeriano, Brandon/Maness, Ryan C. (2014): The dynamics of cyber conflict between rival antagonists, 2001–11. In: Journal of Peace Research 51 (3), S. 347–360.

Valeriano, Brandon/Maness, Ryan C. (2015): Cyber war versus cyber realities. Cyber conflict in the international system. Oxford und New York.

Zetter, Kim (2014): Countdown to Zero Day. Stuxnet and the launch of the world's first digital weapon. New York.