1.2 Forschungsstand, Desiderate und Fragestellung

Die politikwissenschaftliche Forschung hat sich dem neuen Gegenstand Cybersicherheit aus unterschiedlichen Blickwinkeln angenähert. Eine erste prominente Studie legten John Arquilla und David Ronfeldt 1993 vor, sie wurde auch tonangebend für künftige akademische und politische Debatten. Unter dem Titel »Cyberwar is coming!« (Arquilla und Ronfeldt, 1993) diskutierten die Autoren verschiedene Auswirkungen der Informationstechnik auf zukünftige Formen der Kriegführung. Sie legten damit den Grundstein für verschiedene Studien, die sich bis heute konzeptionell mit den Folgen der Verbreitung von Informations- und Kommunikationstechnik für den Konfliktaustrag befassen.

In dieser Tradition stehen Untersuchungen, die grundlegende Fragen nach den Wirkungen des neuen sicherheitspolitischen Handlungsraumes adressieren. Konkret untersuchen Studien in diesem Kontext bspw. die Übertragbarkeit tradierter strategischer Konzepte auf den Cyberspace – häufig wird in diesem Kontext über Abschreckung debattiert (Brantly, 2018; Fischerkeller und Harknett, 2017; Harknett und Nye, 2017; Libicki, 2018; Lindsay, 2015; Nye, 2017; M. Schulze, 2019) – ferner finden sich hier Untersuchungen, die der Frage nachgehen, was Macht im Cyberspace bedeutet und wie sie genutzt werden kann (Nye, 2010; Sheldon, 2014; Siedler, 2016; Willett, 2019) oder ob es Cyberwaffen gibt, bzw. was unter dem Begriff zu verstehen ist (Goines, 2017; Rid und McBurney, 2012; Stevens, 2018). In diesem Zusammenhang stehen auch Diskussionen über das Verhältnis zwischen Offensive und Defensive in der Cybersicherheitspolitik. Oftmals wird in diesem Kontext die These debattiert, die Offensive sei der Defensive im Netz überlegen, da die Verteidigung permanent beim Schutz der eigenen Systeme, die zumeist mit kommerzieller Software betrieben werden und daher (unbekannte) Sicherheitslücken aufweisen, wachsam sein müsse, während AngreiferInnen nur einmal erfolgreich sein müssten. Ferner sei die Schwelle zur Konfliktfähigkeit im Cyberspace auch durch nichtstaatliche Akteure leichter zu überwinden (Gartzke und Lindsay, 2015; Lindsay und Gartzke, 2018).

Weiterhin finden sich in diesem Kontext Studien, die sich mit den strategischen Besonderheiten des Netzes und deren Implikationen für sicherheitspolitisches Handeln beschäftigen. Hier wurde bspw. immer wieder auf das sogenannte Attributionsproblem hingewiesen, das sowohl eine Abschreckung von, als auch eine schnelle Reaktion auf Cyberangriffe schwierig mache, da diese durch die Paketvermittlung im Internet immer über verschiedene Stationen (in unterschiedlichen Ländern) geleitet werden können. Ferner können AngreiferInnen fremde Schadsoftware verwenden, Rechner in bereits verdächtigen Drittländern kapern oder nichtstaatliche Akteure (Proxies) mit der Durchführung von Attacken beauftragen. All dies erhöhe die Unsicherheit und erschwere die Cybersicherheitspolitiken bzw. gezielte Reaktionen auf Angriffe. WissenschaftlerInnen haben sich

daher mit den technischen und später auch politischen Herausforderungen dieser Problematik beschäftigt (Berghel, 2017; Egloff und Wenger, 2019; Green, 2015; Guitton, 2017; Lindsay, 2015; Rid und Buchanan, 2014; Schulzke, 2018).

Die stärkere Hinwendung zum tatsächlichen sozialen Umgang mit dem neuen Problemfeld war der Einsicht geschuldet, dass potenziell folgenschwere Cyberangriffe zwar theoretisch möglich, bislang aber ausgeblieben sind. ForscherInnen wiesen daher spätestens ab den 2010er Jahren vermehrt auch darauf hin, dass es eines besseren Verständnisses der sozialen Praktiken bedürfe, um bspw. die bisherige Zurückhaltung zu verstehen (Betz und Stevens, 2011, S. 124). Damit wurde ein Defizit vieler theoretisch-technischer Analysen aufgeworfen, die die soziale Integration von Technik sowie deren (Um-)Deutung und praktische Nutzung oft ausgespart oder nur kursorisch betrachtet haben. Dies soll technischen Analysen nicht die Relevanz absprechen, verdeutlicht aber, die Notwendigkeit empirischer Untersuchungen (Schünemann und Steiger, 2019). Die vorliegende Arbeit kann daher einen Beitrag dazu leisten, zu verstehen, wie der Handlungsraum durch die Regierungen der Bundesrepublik und des Vereinigten Königreichs gestaltet wird und wie sie einigen dieser Unsicherheiten begegnet sind.

Ein Großteil der skizzierten Studien zeichnet sich ferner durch einen Fokus auf besonders folgenschwere Cyberangriffe aus. Damit wurde früh in der wissenschaftlichen Auseinandersetzung mit dem neuen Forschungsgegenstand ein militärischer Analysefokus gesetzt. Prominenter Ausdruck dieser Perspektive ist das Bild eines Cyberwar, das bis heute für zahlreiche auch deutsche Publikationen titelgebend wirkt (Gaycken, 2011; Kurz und Rieger, 2018).[11] Diese konzeptionelle Engführung wurde immer wieder aus unterschiedlichen Perspektiven bemängelt. Die Kritiklinien haben dabei zur weiteren Ausdifferenzierung des Feldes beigetragen.

Eine konzeptionelle Kritik wurde aus der gleichen wissenschaftlichen Community formuliert, aus der auch die ersten Analysen hervorgingen (den positivistischen *strategic studies*). KritikerInnen konstatierten aber, dass der Kriegsbegriff im Kontext des neuen Handlungsraumes unangemessen sei. Einflussreich vorgetragen wurde diese Einschätzung von Thomas Rid (2012; 2013) und Eric Gartzke (2013). Thomas Rid argumentierte 20 Jahre nach Arquilla und Ronfeldt in seiner Studie »Cyber war will not take place«, dass Cyberangriffe nicht als kriegerische Akte verstanden werden könnten. Um dies zu belegen überprüfte Rid, inwiefern digitale Angriffe der Kriegsdefinition von Carl von Clausevitz entsprechen könnten. Gemessen an drei Indikatoren, wonach sich Kriege 1. durch Gewaltsamkeit, 2. Zweckdienlichkeit und 3. eine politische Natur auszeichneten, hat sich nach Rid noch kein Cyberangriff als kriegerischer Akt qualifiziert. Aus seiner Sicht dienen Cyberangriffe letztlich der Spionage, Subversion oder Sabotage. Sie sind damit

11 Für eine Problematisierung s. Schünemann/Steiger (2019).

keine neuen sicherheitspolitischen Phänomene. Ein Cyberwar im Wortsinne sei zudem unwahrscheinlich, da ein Opponent nur mit Cyberangriffen allein kaum zur Kapitulation gezwungen werden könnte (Rid, 2012). Mit Blick auf etablierte Kriegsdefinitionen argumentiert auch Eric Gartzke, dass Cyberangriffe allein ungeeignet seien, klassische militärische Ziele zu erreichen – bspw. die Eroberung und Verteidigung von Territorien (Gartzke, 2013). Diese Einschätzungen blieben allerdings nicht unwidersprochen, WissenschaftlerInnen haben darauf hingewiesen, dass ein Cyberwar im Zeitalter vernetzter Streitkräfte durchaus möglich ist (Clarke und Knake, 2010; Stiennon, 2015; Stone, 2013) bzw. sogar bereits stattfindet (Arquilla, 2012).

Eine zweite, empirische Kritik an der Ausrichtung auf besonders folgenreiche Vorfälle und militärische Aspekte der Cybersicherheit wurde sowohl von ForscherInnen aus der Konfliktforschung sowie von sozialkonstruktivistischen WissenschaftlerInnen aus dem Bereich der kritischen Sicherheitsstudien vorgebracht (Dunn Cavelty, 2013; Valeriano und Maness, 2015). VertreterInnen der Konfliktforschung bemängelten, dass Studien immer wieder um die gleichen, besonders prominenten Fälle kreisten. So gibt es zahlreiche Studien zu auch medial vieldiskutierten Angriffen bspw. gegen Estland 2007 (Herzog, 2011; Ottis, 2008), gegen Georgien 2008 (S. P. White, 2018), zu Stuxnet 2010 (Farwell und Rohozinski, 2011; Lindsay, 2013; Zetter, 2014), zum Sony-Hack 2014 (Sharp, 2017; Shaw und Jenkins, 2017) oder zu den durch Malware verursachten Stromausfällen in der Ukraine (Shackelford u. a., 2017). Vergleichende Studien, die verschiedene Fälle analysieren und dabei nicht nur die qualitativen Spitzen des Konfliktgeschehens abbilden, sind aber noch immer rar. Eine Folge dieser Kritik sind erste Projekte und Datensätze, die sich zum Ziel gemacht haben, politische Cyberangriffe strukturiert zu vermessen und so empirisch fundierte Analysen zu ermöglichen (Council on Foreign Relations, 2020; Steiger u. a., 2018; Valeriano und Maness, 2014).

Aus Perspektive der kritischen Sicherheitsstudien wurde betont, dass der Fokus auf Extreme potenziell eine problematische Militarisierung des Netzes ermögliche (Dunn Cavelty, 2012). Diese Arbeiten haben ebenfalls maßgeblich dazu beigetragen, die Begriffswahl kritisch zu reflektieren. Auch wenn die Debatte um die Anwendbarkeit des Kriegsbegriffs mittlerweile abgeflaut ist, ist unbestritten, dass zahlreiche Regierungen damit begonnen haben, ihre Streitkräfte mit offensiven Cyberkapazitäten auszustatten (Lewis und Neuneck, 2013). Nur wenige Studien haben aber theoriegeleitet untersucht, welche Mechanismen unterschiedliche staatliche Cybersicherheitspolitiken ermöglichen. Es gibt zwar Studien, die sich empirisch mit Cybersicherheitspolitiken befassen, diese sind aber zumeist theoriearm und deskriptiv (Austin, 2018; Baumard, 2017; Schallbruch und Skierka, 2018; Tabansky und Ben-Israel, 2015). Sie liefern daher keine Antworten auf die entscheidende Frage, was unterschiedliche Cybersicherheitspolitiken ermöglicht. Außerdem befassen sich die meisten empirischen Studien mit den prominen-

testen Fällen – den USA, China oder Russland (Christou, 2017; Sliwinski, 2014). Häufig befassen sich empirische Analysen auch mit den defensiven Maßnahmen, insbesondere dem Schutz kritischer Infrastrukturen (Argomaniz, 2015; Barichella, 2018; Brem, 2015; Dunn Cavelty und Kristensen, 2008; Freiberg, 2015; T. Schulze, 2006; Voeller, 2010).

Wenn Cybersicherheitspolitiken theoriegeleitet untersucht wurden, dann erfolgte das zumeist unter Rückgriff auf die Kopenhagener Schule (Sekuritisierungstheorie). Aus dieser Sicht unterstützte der wissenschaftliche Fokus auf Extrembeispiele staatliche Sekuritisierungstendenzen. Studien zeichneten dabei nach, wie Cyberangriffe sprachlich als Gefahr für die nationale Sicherheit konstruiert wurden. Empirisch lag der Fokus dieser Studien zumeist auf den Entwicklungen in den USA (Bendrath, Eriksson und Giacomello, 2007; Dunn Cavelty, 2008; Lawson u. a., 2016). Es gibt aber auch Analysen zur Bundesrepublik oder dem Vereinigten Königreich (Barnard-Wills und Ashenden, 2012; M. Schulze, 2016). Nur wenige Untersuchungen haben aber Vergleiche unterschiedlicher Cybersicherheitspolitiken durchgeführt (Gorr und Schünemann, 2013; Guitton, 2013). Diese Studien konnten nachzeichnen, wie Regierungen unter Verweis auf unterschiedliche Gefahren wie den internationalen Terrorismus oder feindliche Staaten, den Cyberspace mehr und mehr zu einem sicherheitspolitischen Handlungsfeld machten, in dem sie folglich ihre Kompetenzen erweiterten.

Die Untersuchungen konnten so zeigen, wie die Cybersicherheit zu einem Problem der nationalen Sicherheit wurde (Nissenbaum, 2005). Die Studien weisen aber (in unterschiedlichem Maße) auch Defizite und Blindstellen auf. Auch sie waren zumeist an der Militarisierung des Internets interessiert und untersuchten, wie das Netz und die damit verbundenen Gefahren als Problem für nationale Sicherheit konstruiert wurden. Sie konstatieren zumeist eine Sekuritisierung des Cyberspace, gehen aber nur selten darauf ein, dass der sicherheitspolitische Handlungskorridor nicht homogen ist. Vielmehr zerfällt der staatliche Schutzanspruch im Cyberspace in verschiedene Handlungsfelder, die durch unterschiedliche Akteurskonstellationen geprägt sind und dadurch variante Sekuritisierungsgrade ermöglichen. Die vorliegende Studie begegnet diesem Defizit durch eine systematische Unterscheidung zwischen drei Bereichen der Cybersicherheitspolitik. Auf diesem Weg soll die Entwicklung der Sicherheitspolitik differenzierter nachvollzogen werden. Dies ist theoretisch angemessen, will man ein ganzheitlicheres Bild der Cybersichehreitspolitken entwerfen, das nicht suggeriert, die Politik habe sich zunächst der Kriminalität zugewendet, um im Anschluss durch die Verbindung mit kritischer Infrastruktur auch militärische Maßnahmen zu ermöglichen. Diese Darstellung verstellt den Blick dafür, dass es zu parallelen Entwicklungen der Cybersicherheitspolitiken gekommen ist, die es in unterschiedlichen Handlungskontexten ermöglicht hat, staatlichen Sicherheitsbehörden neue Kompetenzen zuzuweisen. Anders formuliert: als die militärische

Sekuritisierung des Internets möglich wurde, endete damit nicht die Weiterentwicklung der Cybersicherheitspolitik bzw. die Kompetenzausweitung mit Bezug zur Kriminalitätsbekämpfung. Diese Entwicklung steht bei den meisten Sekuritisierungsstudien aber nicht mehr im Fokus des Interesses, obwohl sich auch hier wichtige gesellschaftliche Implikationen und Folgen für die IT-Sicherheit ergeben. Ein umfassenderes Bild der Cybersicherheitspolitik sollte auch jene Kontexte integrieren und systematisch analysieren, in denen Regierungen unterhalb der Schwelle der nationalen Sicherheit für sich in Anspruch genommen haben, Cyberangriffe durchzuführen. Hinzu kommt, dass nicht nur Cyberangriffe selbst zur Sekuritisierung des Netzes beigetragen haben, sondern dass Regierungen auch mit Blick auf traditionelle sicherheitspolitische Herausforderungen für sich auch in Anspruch nehmen, IT-Sicherheit zu unterminieren. So zielen bspw. die offensiven Maßnahmen im Bereich der Strafverfolgung oder der Nachrichtendienste nicht primär auf Cyberkriminalität, sondern auf die Prävention und Verfolgung traditioneller Straftaten.

Neben dieser empirischen Blindstelle, können auch theoretische Prämissen der Sekuritisierungstheorie im Cyberspace problematisch sein. So ist die Beurteilung dessen, was als »außergewöhnliche« Maßnahme gelten kann – der entscheidende Gradmesser für eine erfolgreiche Sekuritisierung (Floyd, 2015) – in einem neuen Handlungsraum, in dem das Normalmaß noch nicht etabliert ist, besonders schwierig und auch Analogieschlüsse sind potenziell problematisch. Ferner ist die Sekuritisierungstheorie auf einen zugänglichen Diskurs angewiesen. Praktiken, über die nicht gesprochen wird, können so schwerer analysiert werden (Dunn Cavelty, 2008, S. 132-137). Geheimhaltung ist zwar auch für diese Untersuchung ein Problem. Der rollentheoretische Fokus auf soziale Praxis erlaubt aber zumindest einen flüchtigen Blick auf die Praktiken (wenn sie bspw. durch WhistleblowerInnen oder JournalistInnen aufgedeckt werden). Weiterhin wird die Sekuritisierung zumeist als ein Prozess zwischen der Regierung und einer zumeist ausschließlich domestischen Audienz konzeptualisiert. Dies verstellt potenziell den Blick für internationale Einflüsse bzw. deren Interaktion mit der domestischen Ebene. Ein Defizit, dem im Rahmen dieser Untersuchung durch den Entwurf eines rollentheoretischen Zwei-Ebenen-Spiels begegnet werden soll. Zudem ist die Handlungsträgerschaft der Audienz in der Sekuritisierungstheorie umstritten. Einige AutorInnen halten den Einfluss der Audienz für gering (Côté, 2016; Léonard und Kaunert, 2011). Außerdem haben die Studien nur selten untersucht, inwiefern die Cybersicherheit durch Interaktionsprozesse ggf. wieder politisiert wurde. Für derartige Prozesse sprechen Gesetzesnovellen in unterschiedlichen Ländern, die die Kontrollrechte der Judikative und Legislative ausgebaut haben (bspw. das BND-Gesetz in der Bundesrepublik oder der Investigatory Powers Act in Großbritannien).

Die vorliegende Studie kann damit einen Beitrag dazu leisten, die etablierten Sekuritisierungsbefunde einerseits mit Blick auf unterschiedliche Handlungskontexte zu qualifizieren und ein differenzierteres Bild der Cybersicherheitspolitiken und deren (parallelen) Entwicklung in drei Untersuchungsbereichen zeichnen. Sie kann weiterhin deren Fokus auf Diskurse durch die Integration von Praktiken ausweiten und mit Hilfe des Vergleichs zudem systematisch Unterschiede zwischen den Untersuchungsstaaten aufdecken. Zudem verschränkt sie innen- und außenpolitische Einflüsse systematisch durch das Zwei-Ebenen-Rollenspiel. Insbesondere dieser Punkt sorgt dafür, dass die Arbeit nicht nur die theoriegeleitete Außenpolitikforschung bereichern kann, sondern auch Anschlüsse an eine andere sozialkonstruktivistische Forschungslinie mit Blick auf das Feld der Cybersicherheit erlaubt.

Auf internationaler Ebene hat sich die sozialkonstruktivistische Forschung mit der Emergenz von Cybersicherheitsnormen beschäftigt (Erskine und Carr, 2016; Finnemore, 2016; Hathaway, 2017; Maurer, 2011). In diesem Kontext wurde bspw. die Norm einer staatlichen Sorgfaltsverantwortung (due diligence) für Cyberangriffe aus dem eigenen Territorium debattiert. Hiernach sollten es Regierungen nicht dulden bzw. unterstützen, dass »ihr« Netz zur Durchführung illegaler Cyberoperationen genutzt wird (Antonopoulos, 2015; Bendiek, 2016; Liu, 2017; Takano, 2018). Außerdem werden in diesem Forschungsstrang bisher erfolglose Bestrebungen zur Regulation von Angriffsfähigkeiten (im Sinne der Rüstungskontrolle) und zur Durchführung von Cyberoperationen analysiert (Baribieri, Danis und Polito, 2018; Eggenschwiler und Silomon, 2018; Stevens, 2018). Die Untersuchungen in diesem Kontext haben überwiegend ernüchternde Befunde zur Emergenz von Normen und deren Bindewirkung geliefert. So konstatiert Melissa Hathaway »that states are not following their own doctrines of restraint«, dies könne zu Fehlattributionen und Eskalationen führen (Hathaway, 2017, S. 1).

Durch die Analyse der deutschen und britischen Cybersicherheitspolitiken können auch deren Implikationen für die emergente Cybersicherheitsordnung eingeschätzt werden. Ferner ist dieser Forschungsstrang dafür kritisiert worden, dass er mitunter eine einheitliche Trennlinie zwischen Demokratien und autokratischen Regimen suggeriert. Diese Darstellung verdeckt aber gleich zwei Befunde, nämlich, dass auch zwischen demokratischen Staaten Differenzen bei der Gestaltung ihrer Cybersicherheitspolitiken bestehen und dass diese Politiken auch domestisch umstritten sind (Maurer, 2019). Die Unterstützung oder Ablehnung bestimmter Normen ist daher auch unter Demokratien variant. Dieser Befund wurde bislang allerdings noch kaum durch empirische Vergleiche untersucht. Die Analyse der Cybersicherheitspolitiken zweier Demokratien ist vor diesem Hintergrund fruchtbar und kann dazu beitragen, die verkürzte Darstellung zu differenzieren. In diesem Zusammenhang kann diese Untersuchung die

unterschiedlichen Perspektiven auf und Herausforderungen von Normen in zwei Demokratien beleuchten und bestehende Einschätzungen ergänzen.

Christopher Whyte hat offene Fragen sowie die Desiderate zur Integration internationaler und domestischer Einflüsse auf die Cybersicherheitspolitik wie folgt skizziert:

> »[…] scholars would do well to consider the cyberpolitics field as one amenable to study under the auspices of both the IR and comparative politics research programs. Doing so would aid in accomplishing the much-needed step of integrating the main branches of the research program on cyberspace and politics that currently exist with the assumptions and sociological explorations of those authors that have, to date, considered the digital world in a more holistic fashion. Then, the field would be better placed to begin the incorporation of research projects that answer questions on the determinants of variations in state-society cyber relationships and foreign policy outcomes.« (Whyte, 2018, S. 12)

In diesem Kontext sollten Whyte zufolge bspw. Fragen nach unterschiedlichen historischen Erfahrungen und deren Folgen für die nationalen Cybersicherheitspolitiken untersucht werden (ebd., S. 12).

Die vorliegende Studie leistet einen Beitrag hierzu. Durch den systematischen Vergleich der deutschen und britischen Cybersicherheitspolitiken sollen die unterschiedlichen Einflüsse identifiziert werden, die die unterschiedlichen Politiken ermöglichen. Konkret wendet sich diese Untersuchung folgenden Fragen zu:

1. Wie haben sich die Cybersicherheitspolitiken der deutschen und britischen Regierungen in den Bereichen Strafverfolgung, Nachrichtendienste und Militär zwischen 1997 und 2019 entwickelt?
2. Welche Einflüsse haben Veränderungen der Politiken ermöglicht?

Die vorliegende Studie adressiert damit signifikante empirische und theoretische Forschungslücken und leistet einen Beitrag zum besseren Verständnis der Cybersicherheitspolitiken in den Untersuchungsstaaten. Aus empirischer Perspektive analysiert und vergleicht die Untersuchung die Cybersicherheitspolitiken zweier Staaten, die in der Forschung bisher nur wenig Beachtung gefunden haben. Theoretisch entwirft die Studie unter Rückgriff auf die symbolisch-interaktionistische Rollentheorie ein Zwei-Ebenen-Spiel, das das internationale Rollenspiel durch ein domestisches Pendant ergänzt und so das Verhältnis von Innen- und Außenpolitik aus rollentheoretischer Perspektive neu ausleuchtet. Eine theoretische Weiterentwicklung, die besonders angesichts des Untersuchungsgegenstandes und der mit ihm verbundenen schwierigen Trennung zwischen Innen- und Außenpolitik geboten scheint.