der NSA nicht zu gefährden. Die domestischen Kontestationen forderten unter anderem deshalb keine einschneidenden Begrenzungen für die technischen Fähigkeiten des Nachrichtendienstes. Im militärischen Bereich waren es, neben der Gefahrenlage, Erwägungen zur Verbesserung der Kooperationsfähigkeit mit den NATO-Partnern, die in Deutschland den Aufbau des Kdo CIR erleichterten. In Großbritannien wurde der Ausbau durch die zunehmende Konfrontation mit Russland ermöglicht. Die unterschiedlichen Kryptopolitiken werden ebenfalls erst dann besser verständlich, wenn auch die internationale Ebene mitgedacht wird. Während in Deutschland eine zu ausgreifende US-Politik abgelehnt wurde, wurde dies von der britischen Regierung nicht so kritisch gesehen. Hierdurch wurde in Großbritannien zumindest ein freiwilliges System nach amerikanischem Vorbild installiert, während Deutschland eine weniger restriktive Politik verfolgte.

In beiden Untersuchungsstaaten und in unterschiedlichen Bereichen der Cybersicherheitspolitik zeigt das rollentheoretische Modell so, dass sowohl außen- als auch innenpolitische Entwicklungen die Politiken beeinflussen. Die empirische Analyse hat verdeutlicht, dass das rollentheoretische Zwei-Ebenen-Spiel dabei hilft, die unterschiedlichen Dynamiken und Interaktionen zwischen den Sphären zu analysieren und die Politikentwicklung besser zu verstehen. Das Zwei-Ebenen-Rollenspiel illustriert dabei erstens, dass das internationale Rollenspiel nicht im realistischen Sinne gleich auf beide Staaten wirkt und dass ein Fokus auf eine Ebene wichtige Interaktionen ausblendet. Zweitens wird deutlich, dass sich die beiden Ebenen wechselseitig beeinflussen und in dynamischem Interaktionsverhältnis stehen. Die Fruchtbarkeit dieses Ansatzes zeigt sich daher auch in unterschiedlichen Wechselwirkungen zwischen domestischer und innenpolitischer Sphäre, die die unterschiedlichen Cybersicherheitspolitiken in den beiden Untersuchungsstaaten besser verständlich machen.

7.3 Limitationen, Desiderate und Ausblick

Grundsätzlich lassen sich zwei Limitationen der vorliegenden Studie identifizieren. Die erste folgt aus dem Design der Studie, das durch sein verstehendes Vorgehen und die begrenzte Fallzahl mit Blick auf die Übertragbarkeit der Befunde notwendigerweise begrenzt bleibt. Die zweite ergibt sich aus dem empirischen Forschungsgegenstand, der sich durch ein beträchtliches Maß staatlicher Geheimhaltung auszeichnet. Die Befunde sind daher in doppelter Hinsicht kritisch zu reflektieren.

Die Untersuchung ist mit dem Ziel gestartet, zu analysieren, wie sich die Cybersicherheitspolitiken in den beiden Untersuchungsstaaten entwickelt haben. Für die beiden Regierungen konnte gezeigt werden, dass sie ihre Beschützer-Rollen innerhalb des Untersuchungszeitraumes ausgebaut haben. In beiden Staa-

ten haben sich – in unterschiedlichem Maße – kontestierende oder katalytische Effekte mit den Rollen als Garant liberaler Grundrechte bzw. Wohlstandsmaximierer ergeben. Die Untersuchung ist in ihrer verstehenden theoretisch-methodischen Herangehensweise aber nicht darauf angelegt, generalisierbare Erkenntnisse über Cybersicherheitspolitiken zu gewinnen. Sie zielt darauf, die beiden untersuchten Fälle besser zu verstehen und einen möglichst plausiblen Interaktionsverlauf nachzuzeichnen. Die Befunde der Untersuchung sprechen dafür, dass sich auch westliche Demokratien, die sich durch Mitgliedschaften in ähnlichen Organisationen und durch ähnliche kulturelle Prägungen auszeichnen, substanziell in ihren Cybersicherheitspolitiken unterscheiden. Aufschlussreich wären daher weitere Studien, mit mehr Fällen auch aus anderen geografischen und kulturellen Kontexten. Nur auf diesem Weg ließe sich ein umfassenderes Bild, auch mit Blick auf die internationale Cybersicherheitsordnung, zeichnen.

Insgesamt ist zu hoffen, dass die theoriegeleitete Forschung auch in Zukunft verstärkt vergleichend arbeiten wird, um das Verständnis für unterschiedliche Einflüsse auf Cybersicherheitspolitiken zu verbessern. Ein Blick auf innen- wie außenpolitische Einflüsse hilft dabei, ein differenziertes Bild der Politiken zu zeichnen. Jedes Gemeinwesen nimmt, durch seine historischen Erfahrungen und die Einbettung in unterschiedliche soziale Handlungskontexte, einen eigenen Weg in die sicherheitspolitische Erschließung des Netzes. Diese Wege besser zu verstehen, wird dabei helfen, auszuloten, welche internationalen Verhaltensstandards an die Rollen der Regierungen anschlussfähig sind. Auch zwischen Demokratien bestehen, wie diese Untersuchung gezeigt hat, beträchtliche Unterschiede in den Cybersicherheitspolitiken.

In diesem Kontext ist aber darauf hinzuweisen, dass eine Übertragbarkeit des Analysekonzepts insbesondere jenseits demokratischer Systeme schwierig ist bzw. substanzieller empirischer Nacharbeit bedarf. In autokratischen Regimen ist die Rolle als Garant liberaler Grundrechte wenn überhaupt nur begrenzt anwendbar. Ein einfacher Transfer des Analysekonzeptes ist damit kaum möglich. Vielmehr müssten für autokratische Systeme zunächst die prägenden Rollen der Cybersicherheitspolitik aus den entsprechenden Dokumenten herausdestilliert werden. Es muss ferner bezweifelt werden, dass das innenpolitische Rollenspiel in Autokratien ähnlichen Regeln folgt wie in Demokratien. Die signifikanten Anderen sind vermutlich andere (bspw. das Militär, Herrscherdynastien, Parteien, etc.) und auch die Interaktionen folgen anderen Mustern. All das müsste empirisch nachvollzogen werden. Eine Erweiterung der analysierten Fälle – auch über demokratische Staaten hinaus – wäre aber dennoch wünschenswert, um ein besseres Verständnis für die unterschiedlichen Interaktionen und für die internationale Cybersicherheitsordnung zu gewinnen. Insbesondere mit Blick auf die Erweiterung der untersuchten Fälle und Integration von Autokratien ergeben sich aber besondere Schwierigkeiten beim Zugang zum empirischen Analysematerial.

Die Cybersicherheitspolitik gehört zu den besonders sensiblen Bereichen der Sicherheitspolitik und ist daher ein potenziell schwieriger Forschungsgegenstand. Es bleibt daher stets fraglich, ob denn tatsächlich die Politiken in Gänze analysiert werden können. Diese Einschränkung gilt weniger für den Bereich der Strafverfolgung, der durch die entsprechenden gesetzlichen Regelungen relativ explizit geregelt ist. Sie betrifft aber besonders die Arbeit der Nachrichtendienste sowie der Streitkräfte. Zwei Argumente lassen sich kritischen Stimmen entgegnen, die in diesem Kontext ggf. sogar für einen Forschungsverzicht plädieren, da keine abschließenden und belastbaren Erkenntnisse gewonnen werden könnten. Erstens lässt sich dem Argument grundsätzlich mit Blick auf die hier vertretene wissenschaftstheoretische Position begegnen. Wendet man das Argument zum Forschungsverzicht nämlich radikal um, zeigt sich, dass ein Verzicht aus Furcht davor, keine finalen Erkenntnisse zu generieren fehl geht, da unhintergehbares Wissen ohnehin nicht erreichbar ist. Wissen bleibt aus pragmatistischer Perspektive stets veränderbar und muss sich in Interaktion bewähren. Die Untersuchung von Cybersicherheitspolitiken unterscheidet sich hier nicht von anderen wissenschaftlichen Studien. Das bedeutet daher nicht, dass die Analyse von Cybersicherheitspolitiken aufgrund der (potenziell höheren) Fallibilität unterbleiben sollte.

Zweitens lässt sich der Kritik im Kontext dieser Studie empirisch begegnen. Da es sich bei den beiden hier untersuchten Staaten um Demokratien handelt, sind Daten zumindest teilweise zugänglich. Die Regierungen unterliegen auch in sensiblen Sicherheitspolitiken parlamentarischer und juristischer Kontrolle. Auch wenn diese Kontrollen nicht alle Praktiken öffentlich machen, besteht so doch die Möglichkeit, Einblick in die praktische Politikgestaltung zu erlangen. Dies wird in demokratischen Systemen durch die Arbeit einer freien Presse und der damit einhergehenden Publikation geheimer Dokumente weiter begünstigt. Die Snowden-Enthüllungen und die damit verbundene erzwungene Öffentlichkeit, waren für diese Studie – wie für viele andere – die einzige Gelegenheit, die Entwicklung der Politiken im Bereich der Nachrichtendienste zu analysieren. Sie zeigen auch, dass es mitunter einer/eines Mitwisserin/Mitwissers bedarf, um verdeckte Praktiken öffentlich zu machen. Eine Analyse der Cybersicherheitspolitiken ist daher in Demokratien potenziell einfacher, da die Regierungen verschiedenen Kontrollen unterworfen sind und es so einfacher möglich ist, Interaktionen zu rekonstruieren. Es ist aber nicht auszuschließen, dass weitere Veröffentlichungen oder das zukünftige Öffnen staatlicher Archive die Informationslage signifikant verändern und die Befunde der Arbeit infrage stellen werden.

Ein Forschungsverzicht ist aber auch mit Blick auf Autokratien nicht angeraten, denn das dritte Argument richtet sich allgemeiner gegen KritikerInnen. Auch wenn Untersuchungen nicht das ganze Ausmaß staatlicher Cybersicherheitspolitiken aufdecken können, tragen sie doch wesentlich zum Erkenntnisgewinn in diesem Bereich bei. Regierungen müssen ihre Positionen zumindest grundsätz-

lich rechtfertigen und nicht alle Maßnahmen im Netz können geheimgehalten werden. Dies liegt einerseits an WhistleblowerInnen, an nichtstaatlichen Akteuren im Netz, die Infrastrukturen betreiben und Attributionen durchführen und andererseits daran, dass sich folgenschwere Cyberangriffe nicht geheimhalten lassen und dass auch nachrichtendienstliche Operationen entdeckt und mitunter veröffentlicht werden. All dies lässt sich analysieren. Regierungen handeln in diesen Kontexten sowohl international als auch domestisch. Dieses Handeln konstituiert – in Interaktion mit den signifikanten Anderen – soziale Realität. Es ist diese soziale Realität, die einer wissenschaftlichen Analyse offensteht. Die zugänglichen Praktiken berühren dabei so zentrale Werte, dass auch ein begrenzter Erkenntnisgewinn gesellschaftlich und wissenschaftlich wertvoll ist. Dass die informationstechnische Verwundbarkeit in absehbarer Zukunft eher zu- als abnehmen wird, spricht ebenfalls dafür, sich dem Thema zuzuwenden. Untersuchungen können dabei helfen, die emergente internationale Cybersicherheitsordnung besser zu verstehen. Die Politiken zu verstehen, heißt dabei auch nachzuvollziehen, welche Abwägungen die Regierungen vornehmen, welche Konflikte zwischen Staaten auftreten und welche Dynamiken sich hieraus ergeben können. Auch wenn Untersuchungen zur Cybersicherheitspolitik durch künftige Enthüllungen infrage gestellt werden, so bilden sie doch zum Zeitpunkt der Erstellung soziale Wirklichkeit ab. Der rollentheoretische Zugang mit seinem Fokus auf den Praktiken sozialer Interaktion kann diese soziale Wirklichkeit rekonstruieren und analysieren.