dass Sicherheitsbehörden bei der Evaluation einer Schwachstelle tatsächlich zu ähnlichen Entscheidungen gelangen. Für die Wahrung der Beschützer-Rollen in allen Untersuchungsbereichen akzeptieren die beiden Staaten ein potenzielles Risiko für das Netz und die NutzerInnen. Werden Staaten so auch zu Einkäufern von Zero-Day-Exploits, unterstützen sie zudem einen potenziell problematischen Markt für Sicherheitslücken.

Im Bereich der Kriminalitätsbekämpfung hat bisher die weitreichendste internationale Kooperation stattgefunden. Mit der Convention on Cybercrime konnten Straftatbestände harmonisiert und die Zusammenarbeit verbessert werden. Mit Blick auf weitere Kooperationen im Bereich der Strafverfolgung zeigt der deutsche Fall aber, dass die nächsten Schritte – die gegenseitige Zugriffsgewährung auf Daten – problematisch werden, da rechtsstaatliche Bedenken im Wege stehen. Großbritannien hat ein solches Abkommen mit den USA zwar abgeschlossen, ist aber darauf bedacht, die souveräne Kontrolle über die Beschützer-Rolle zu wahren. Der Ausbau der Kooperation im Bereich der Strafverfolgung ist daher ebenfalls nicht sicher.

Eine gewisse Skepsis bleibt auch mit Blick auf eine Norm, die die Regierungen wiederholt betont haben. Beide Regierungen haben immer wieder darauf hingewiesen, dass Staaten eine Sorgfaltsverantwortung für den eigenen Cyberspace tragen. Sie haben daher darauf gedrängt, dass Staaten illegitime Cyberangriffe, die von ihren Territorien ausgehen, nicht dulden oder unterstützen dürften. Diese Forderung wurde insbesondere immer lauter formuliert, als die Angriffe durch Proxies zunahmen. Domestisch wurden aber auch in beiden Staaten Bedenken dazu geäußert, welche Maßnahmen die Normeinhaltung gewährleisten könnten. Befürchtet wurde in diesem Kontext, dass dies eine umfassende Kontrolle der Internetverkehrs nötig mache. Der Nachweis der Compliance könnte so im Widerspruch mit der Rolle als Garant liberaler Grundrechte stehen. Eine Norm der Staatenverantwortung könnte auch von Autokratien zur Rechtfertigung eigener Überwachungspraktiken genutzt werden und ggf. eine Fragmentierung des Netzes befördern, da Eingriffe in Inhalte oder Praktiken unter dem Vorwand der Normdurchsetzung erfolgen könnten.

7.2 Theoretische Reflexion: Fruchtbarkeit des Zwei-Ebenen-Rollenspiels und alternative Erklärungen

Die Studie hat zur Analyse der Cybersicherheitspolitiken ein neues rollentheoretisches Zwei-Ebenen-Spiel entworfen. In Abgrenzung zu realistischen Ansätzen, die das internationale Rollenspiel als vorrangig betrachten und liberalen Perspektiven, die die innerstaatlichen Prozesse des Interessenuploads in den Vordergrund stellen, wurde so ein theoretisches Konzept entwickelt, das keiner der Sphären

Vorrang einräumt, sondern diese gleichberechtigt betrachtet und deren Wechselwirkungen nachvollzieht.

Das rollentheoretische Zwei-Ebenen-Spiel wurde hier in Abgrenzung zum etablierten TLG von Putnam für Handlungskontexte angewendet, in denen es nicht um die Aushandlung eines Abkommens geht, sondern im Rahmen der Entwicklung von Cybersicherheitspolitiken. Es wurde zuvor meist in relativ kontextarmen Analysen genutzt. Hier wurde es dagegen für eine vergleichsweise lange diachrone Untersuchung angewendet. Die theoretische Weiterentwicklung hat sich in diesem Kontext als hilfreich beim Verständnis der Cybersicherheitspolitiken bewährt. Der Vorteil gegenüber der etablierten Analyse von domestischen Kontestationsprozessen aus rollentheoretischer Perspektive liegt in der Auflösung der strikten Trennung zwischen innen- und außenpolitischen Einflüssen. Das rollentheoretische Zwei-Ebenen-Spiel dynamisiert das Verhältnis der beiden Sphären über die Interaktion der Regierungen mit domestischen und internationalen signifikanten Anderen. Es ermöglicht so auch Befunde, wie bspw. das internationale Rollenspiel, dass auf das domestische zurückwirkt (Second Image reversed).

Dass etablierte Theorien der IB, die Befunde dieser Arbeit nicht besser erklären können als der gewählte theoretische Zugang, lässt sich an zwei Beispielen illustrieren: Erstens mit einem neorealistischen Blick auf die Politiken, der die systemischen Machtverteilungen zur Erklärung staatlichen Handelns heranzieht sowie zweitens aus der Perspektive eines liberalen Ansatzes, bei dem das domestische Rollenspiel im Fokus der Betrachtung steht.

Mit Blick auf den Neorealismus stellen sich fragen zu dessen Erklärungskraft auch dann, wenn man nur den Bereich der Streitkräfte betrachtet und sich damit auf den Kernbereich realistischen Erklärungsanspruchs beschränkt. Auch wenn im Neorealismus das Verhältnis zwischen Macht on- und offline nach wie vor umstritten ist (s. Kapitel 1), gibt es Befunde, die eine neorealistische Erklärung vor substanzielle Herausforderungen stellen. Geht man davon aus, dass es der Cyberspace potenziell unterlegenen Akteuren ermöglicht, konventionelle Defizite teilweise zu kompensieren und damit asymmetrische Konstellationen etwas anzugleichen, eine Einschätzung die beide Regierung teilen, dann stellt sich die Frage, warum Deutschland, das sich im konventionellen Bereich durch freiwillige Selbstbeschränkung auszeichnet und über keine eigene nukleare Abschreckung verfügt, die Option offensiver Cyberkapazitäten nicht stärker nutzt, sondern im Gegenteil auch hier zurückhaltender agiert als das Vereinigte Königreich. Die deutsche Regierung lässt damit bewusst eine Chance zur Kompensation konventioneller Unterlegenheit aus. Großbritannien hat dagegen öffentlich deutlich gemacht, dass das GCHQ auch Angriffsfähigkeiten mit erheblichen kinetischen Potenzialen aufbaut, obwohl die eigene Abschreckungsfähigkeit konventionell verfügbar ist. Der relative Gewinn durch den Aufbau der Fähigkeiten ist daher für das Vereinigte Königreich deutlich geringer als er für die konventionell schwächere

Bundesrepublik wäre. Dieser Befund macht es zweifelhaft, dass eine realistische Erklärung für die empirischen Ergebnisse dieser Studie besser geeignet ist, da die domestischen Einflüsse in einer strukturell realistischen Untersuchung keinen Raum finden.

Die Annahme, das internationale System präge allein durch den anarchischen Anpassungsdruck die Außenpolitiken, greift daher zu kurz. Sie wird mit Blick auf die deutsche Bundesregierung durch die freiwillige Selbstbeschränkung konterkariert. Diese Zurückhaltung findet sich aber nicht nur im militärischen, sondern auch im Bereich der nachrichtendienstlichen Nutzung des Netzes. Auch hier begrenzt die Exekutive die Maßnahmen gegen europäische Ziele bzw. setzt für sie besonders hohe Hürden. Aus realistischer Perspektive, in der die Verbündeten von heute die Gegner von morgen sein können (Waltz, 2000, S. 10), ist dies kein plausibles Vorgehen. Aber auch im Vereinigten Königreich sind die domestischen Einflüsse für das Verständnis der Cybersicherheitspolitiken bedeutsam. Die positiven historischen Erfahrungen mit den Nachrichtendiensten und die negativen Erfahrungen als Opfer terroristischer Anschläge begünstigen, zusammen mit der internationalen Gefahrenlage und der besonderen Beziehung zu den USA, eine offensivere und weniger restriktive Cybersicherheitspolitik. Die frühe Entwicklung der britischen Beschützer-Rolle im Bereich der Strafverfolgung, ist ohne die historischen Erfahrungen mit domestischem Terrorismus dagegen gar nicht zu verstehen (sie entzieht sich zugegebenermaßen aber auch realistischen Erklärungsansprüchen). Die innenpolitischen Faktoren abzuschneiden, verdeckt daher einen substanziellen Teil der Interaktionen, die für das Verständnis der Politiken bedeutsam sind.

Aus liberaler Perspektive ergeben sich andere Fragen. Prinzipiell zielt die liberale Annahme darauf, dass durch den Wechsel der RollenträgerInnen andere gesellschaftliche Interessen auf die Regierung übertragen werden. Es bleibt hier aber einerseits zweifelhaft, ob die Cybersicherheitspolitiken in den Untersuchungsstaaten die Salienz aufweisen, die Wahlentscheidung der BürgerInnen zu beeinflussen. Ob also überhaupt gezielt neue Interessen transferiert werden. In beiden Fällen sprechen Indizien gegen diese Annahme. Einerseits stand die britische Regierung nach den Snowden-Enthüllungen domestisch wie international aufgrund ihrer ausgreifenden Überwachungstätigkeiten in der Kritik. Diese führte bei der Wahl 2015 aber nicht zu einer Stärkung des überwachungsskeptischen Koalitionspartners (den Liberal Democrats), sondern zu einem Sieg und einer Alleinregierung für die Tories. In Deutschland spricht der Niedergang der Piraten Partei und die Abwahl der FDP während bzw. nach den Snowden-Enthüllungen ebenfalls dafür, dass die Cybersicherheitspolitiken bzw. Kritik an diesen, nicht wahlentscheidend waren.

Die Wechsel der RollenträgerInnen durch Wahl bzw. Abwahl haben im gesamten Untersuchungszeitraum die Cybersicherheitspolitiken nur geringfügig beein-

flusst (bspw. in Großbritannien mit Blick auf die militärische Cybersicherheit 2010). Die Erwartung, (physische) Sicherheit zu gewährleisten, hat VertreterInnen unterschiedlicher Parteien dazu veranlasst, den Ausbau der Beschützer-Rollen mitzutragen. Auch wenn bei Regierungswechseln die Cybersicherheitspolitiken der Vorgängerregierung als zu umfassend kritisiert wurden, wurde der weitere Aufbau der Beschützer-Rolle nach dem Machtwechsel oftmals fortgesetzt. Dies zeigt sich bspw. nach dem Wahlerfolg der Labour Party 1997, die noch vor der Wahl die Haltung der Tories zur Kryptographie abgelehnt hatte, nach der Wahl aber eine ähnliche Politik verfolgte. In Deutschland zeigt sich ein ähnliches Phänomen zum Zeitpunkt der Snowden-Enthüllungen. Noch vor dem Regierungswechsel war die oppositionelle SPD in ihrer Kritik an der Regierung aus CDU/CSU und FDP deutlicher als nach dem Eintritt in die Regierung. Die Parteien definieren die Beschützer-Rollen zwar etwas unterschiedlich und liberale bzw. linke Parteien sind öfter gewillt, diese Rolle unter Abwägung mit der Rolle als Garant liberaler Grundrechte zu beschränken. Allerdings hat dies in keinem Fall zu einem Rückbau der Kompetenzen geführt. So hat die antizipierte soziale Erwartungshaltung, dass die Regierung für den Schutz der BürgerInnen verantwortlich ist und auch die Sorge davor, im Ernstfall für ein Versagen verantwortlich gemacht zu werden, auch eigentlich skeptische Parteien für Erweiterungen der Beschützer-Rolle stimmen lassen (bspw. die Liberal Democrats für DRIPA 2014). Liberale Ansätze zur Erklärung der Politiken scheitern ferner daran, dass Veränderungen nicht zu den Hochzeiten innergesellschaftlichen Interessenuploads (Wahlen) stattfinden, sondern sich langsam auch über unterschiedliche Regierungskonstellationen hinweg vollziehen. Vielmehr zeigt sich, dass die Beschützer-Rolle durch verschiedene Parteien zwar unterschiedlich definiert wird, kommt es dann zum Machtwechsel, sind die Politiken aber zumeist ähnlich. Das spricht dafür, dass die mit der Rolle verbundenen antizipierten sozialen Erwartungen und die Konsequenzen von deren Nichterfüllung im Ernstfall auch skeptischere Parteien zu Anpassungen veranlassen.

Für liberale Erklärungsansätze ist zudem problematisch, dass sie Rückwirkungen der internationalen Ebene auf die domestischen Entwicklungen (second image reversed) nicht nachvollziehen. Ein Defizit, das auch rollentheoretische Arbeiten betrifft. Dass diese Effekte für das Verständnis der Cybersicherheitspolitiken aber wichtig sind, zeigt die empirische Analyse. In der Bundesrepublik wurde der Ausbau der Beschützer-Rolle im Bereich der Nachrichtendienste durch die Abhängigkeit von den USA beeinflusst. Das außenpolitische Scheitern der Verhandlungen und die ablehnende Haltung der USA und des Vereinigten Königreichs, begünstigten, dass sich die domestische Aufklärung auf die Untersuchung der eigenen Beschützer-Rolle fokussierte. Die antizipierten Folgen eines Bruchs mit den Verbündeten moderierten diese domestische Aufarbeitung. In Großbritannien ging es in diesem Bereich auch darum, die Kooperation mit

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-