7.1 Empirische Befunde

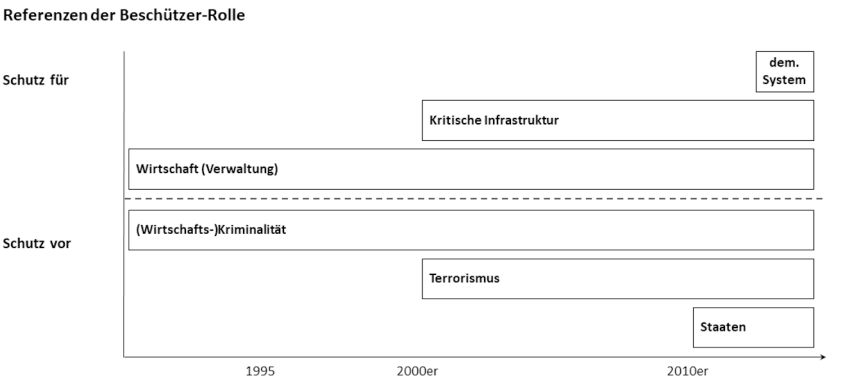
7.1.1 Entwicklung der Cybersicherheitspolitiken

Die Untersuchung hat gezeigt, dass die empirischen Sekuritisierungsbefunde, die lange die theoriegeleitete Analyse von Cybersicherheitspolitiken geprägt haben, durch die Unterscheidung zwischen drei Untersuchungsbereichen deutlich ausdifferenziert werden können. Die Studie konnte zeigen, dass die Politiken durch die unterschiedlichen (domestischen wie internationalen) signifikanten Anderen sowie durch unterschiedliche Referenzen auf das historische Selbst ermöglicht wurden. In den Untersuchungsstaaten haben sich dabei unterschiedliche Dynamiken zwischen dem domestischen und internationalen Rollenspiel ergeben. Die empirischen Befunde werden im Folgenden im Kontext der forschungsleitenden Annahmen kurz zusammengefasst.

1. Die Regierungen beider Untersuchungsstaaten haben im Laufe des Untersuchungszeitraums ihre Beschützer-Rollen in der Cybersicherheitspolitik erweitert.

In beiden Untersuchungsstaaten und über das gesamte Spektrum der drei Analysebereiche hinweg, ergibt sich über den Untersuchungszeitraum ein Aufwachsen der Beschützer-Rollen der Regierungen. Dies zeigt sich in der Inklusion zusätzlicher schützenswerter Referenzobjekte, im Bezug zu immer gefährlicheren AngreiferInnen und in den daraus folgenden Kompetenzzuwächsen der Sicherheitsbehörden. Damit hat sich die doppelte Referenz der Beschützer-Rollen (Schutz für wen/was bzw. Schutz vor wem) über den Untersuchungszeitraum verändert. Die Frage nach dem Schutz für wen wurde zunehmend universeller beantwortet. Der Katalog abzuwehrender AngreiferInnen erweiterte sich ebenfalls. Waren die Beschützer-Rollen zu Beginn noch auf den Schutz der Wirtschaft ausgerichtet, wurden durch die zunehmende Vernetzung und die damit verbundene (physische) Verwundbarkeit immer mehr Referenzobjekte schutzbedürftig. Die Entwicklung der Straftatbestände spiegelt so exemplarisch die Lösung vom Referenzobjekt Wirtschaft und die veränderte Einschätzung der Fähigkeiten von AngreiferInnen wider. In beiden Untersuchungsstaaten haben die Regierungen die Beschützer-Rollen durch Bezüge zu den kritischen Infrastrukturen und deren essenzieller gesellschaftlicher Bedeutsamkeit erweitert, da durch die Verknüpfung von Cyberangriffen mit kritischen Infrastrukturen kinetische Folgen realistischer wurden. Die Prävention von internationalem Terrorismus war ab den 2000er Jahren prägend. Nach dem Bekanntwerden von Stuxnet wiesen beide Regierungen ferner auch auf die Gefahr von staatlichen Cyberangriffen hin. Mit dem demokratischen System erhielt die Rolle zudem ein weiteres Schutzgut. Dies folgte insbesondere auf die Vorwürfe, Russland habe versucht den US-Präsidentschaftswahlkampf durch Cyberangriffe zu manipulieren. Die Entwicklung ist in der Abbildung 3

Abbildung 3: Entwicklung der Referenzen der Beschützer-Rollen, Quelle: Eigene Darstellung



schematisch dargestellt. Soweit entspricht dieser Befund den eingangs erwähnten Studien zur Sekuritisierung bspw. in den USA.

Beide Regierungen haben in allen drei Untersuchungsbereichen ferner damit begonnen, selbst offensive Fähigkeiten aufzubauen. In den drei Handlungskontexten unterminieren die Regierungen IT-Sicherheit zur Aufrechterhaltung der Beschützer-Rollen. Sie haben diesen Aufbau eingeleitet, um einerseits das klassische sicherheitspolitische Handlungsrepertoire zu erweitern und um andererseits neuen digitalen Angriffsformen zu begegnen. Im Bereich der Strafverfolgung nutzen die Polizeibehörden Schadsoftware zum Abhören von Kriminellen oder Terrororganisationen. Die Nachrichtendienste überwachen Kommunikationsvorgänge im Internet, um (externe) Gefahren zu identifizieren und die Streitkräfte greifen auf Sicherheitslücken zurück, um militärische Operationen zu flankieren oder zu ersetzen.

Die Entwicklungen in den drei Bereichen unterscheiden sich aber deutlich. Die Politiken wurden dabei sowohl durch das innen- als auch das außenpolitische Rollenspiel beeinflusst.

> *2. Die Beschützer-Rollen unterscheiden sich in den drei Untersuchungsbereichen aufgrund der Interaktion mit unterschiedlichen signifikanten Anderen (domestisch wie international) und aufgrund unterschiedlicher historischer Selbstbezüge. Die Regierungen müssen ihre Positionen in einem rollentheoretischen Zwei-Ebenen-Spiel einnehmen und sind dabei auf komplementäre Rollenübernahmen durch signifikante Andere angewiesen. Beide Rollenspiele stehen dabei in interaktivem Austausch und können sich gegenseitig beeinflussen.*

Im Bereich der Strafverfolgung etablierten beide Staaten neue Straftatbestände. Was als illegitimes Verhalten in diesem Bereich gewertet werden sollte, wurde daher relativ schnell festgelegt. Da diese Bezüge der Beschützer-Rollen unter vielen

demokratischen Staaten ähnlich waren und da Cyberkriminalität international ein wachsendes Problem darstellte, waren sie auch international anschlussfähig. Dies ermöglichte eine internationale Harmonisierung der gesetzlichen Regelungen im Europarat und in der EU. Die internationale Kooperation zur Strafverfolgung wurde vereinfacht, da die Referenz auf der Regulation nichtstaatlicher Akteure – also Dritter – lag.

Die Etablierung der Verhaltensstandards für nichtstaatliche Akteure und deren Explikation in Straftatbeständen verlief in beiden Untersuchungsstaaten relativ ähnlich. Die britische Regierung konnte aber bereits früher eine expansivere Beschützer-Rolle etablieren. Sie zeigt sich unter anderem in höheren Strafmaßen, in der Sanktionierung jeglicher Hackingaktivitäten und in den Bestrebungen, Verschlüsselung restriktiver zu regulieren. Dies wurde durch die Bezüge zum historischen Selbst – die Erfahrungen mit Terrorismus in Nordirland ermöglicht. Die Referenz der Rolle (Schutz vor wem?) lag damit schon von Beginn an auf gefährlicheren AngreiferInnen. Aufgrund der domestisch relativ stabilen Beschützer-Rolle, konnte die britische Regierung ihre Rolle sogar extraterritorial ausdehnen. Sie nimmt so in Anspruch, auch ausländische Dienstleister zur Entschlüsselung zu zwingen. Mit Blick auf die Regulation von Verschlüsselung verfolgte die deutsche Regierung eine liberalere Politik, da es substanzielle domestische Kontestationen, gestützt auf Bezüge zum negativen historischen Selbst, gab. Außerdem wurde diese Ablehnung auch durch das internationale Rollenspiel ermöglicht in dem die Bundesrepublik eine globalisierte Beschützer-Rolle der USA ablehnte, da diese die eigenen Rollen zu unterminieren drohte. Während die britische Regierung aus einer stabilen domestischen Beschützer-Rolle heraus auch international (insbesondere im Rahmen der 5-Eyes) für eine stärkere Regulation von Verschlüsselung warb bzw. noch wirbt, ist die deutsche Regierung sowohl durch das domestische als auch durch das internationale Rollenspiel einer solchen Regulation gegenüber skeptischer. Die deutsche Regierung konnte in der domestischen Sphäre ferner die eigene Beschützer-Rolle noch nicht stabilisieren. Kontestationsprozesse aus Zivilgesellschaft und Opposition sorgten, gestützt auf Gerichtsurteile, dafür, dass die Regierung die Beschützer-Rolle anpassen bzw. beschränken musste. Die domestischen Kontestationen und die Rolle als Garant liberaler Grundrechte begrenzen auch die außenpolitische Kooperationsbereitschaft der Bundesregierung, so steht die Bundesregierung europäischen Bemühungen skeptisch gegenüber, externen Ermittlungsbehörden Zugriff auf digitale Spuren in Deutschland zu gewähren. Die britische Regierung hat demgegenüber ein solches Abkommen zum gegenseitigen Datenzugriff mit den USA abgeschlossen. Dies wurde durch eine domestisch stabilere Beschützer-Rolle sowie die besonderen Beziehungen zu den USA erleichtert.

Im Bereich der Nachrichtendienste zeigt sich eine deutliche Differenz in der Einschätzung, was als akzeptables staatliches Verhalten gilt. Die deutsche

Bundesregierung versuchte sich nach den Snowden-Enthüllungen zunächst domestisch und international der eigenen Beschützer-Rolle zu versichern. Sie tat dies durch die innenpolitische Aufklärung der Vorwürfe sowie internationale Verhandlungen über ein Abkommen zur Begrenzung gegenseitiger Spionage. Durch die ablehnenden Reaktionen der amerikanischen und britischen Regierungen frustriert, versuchte die deutsche Administration domestisch durch die Kündigung kommerzieller Verträge mit amerikanischen Dienstleistern und international durch die Unterstützung neuer transatlantischer Internetkabel, den physischen Zugriff auf Internetkommunikation zu erschweren. Außerdem ergänzte die Regierung die Referenz der Beschützer-Rolle (Schutz vor wem?), um auch Aktivitäten befreundeter Nachrichtendienste aufzudecken und ggf. zu verfolgen. Eine innenpolitisch geforderte, konfrontative Haltung gegenüber den USA wurde durch die Regierung aber aufgrund der internationalen Abhängigkeit abgelehnt. Da eine internationale Aufarbeitung der Vorwürfe keine Erfolge zeigte und die Enthüllungen auch den Verdacht genährt hatten, der deutsche BND sei möglicherweise Komplize der NSA gewesen, wurden die Enthüllungen domestisch durch den NSA-Untersuchungsausschuss aufgearbeitet. Hierbei wurde deutlich, dass der BND selbst zahlreiche problematische Praktiken etabliert hatte. Das führte zu domestischen Kontestationsprozessen und der Forderung, neue gesetzliche Regelungen für den Auslandsnachrichtendienst zu erlassen. Diese Neuregelung führte in der Folge aber nicht zu einer Begrenzung der eigenen Beschützer-Rolle, sondern, unter Verweis auf bestehende Gefahren (insbesondere den internationalen Terrorismus) und die Notwendigkeit des Informationsaustauschs, zu einer Rechtfertigung zahlreicher zuvor enthüllter Praktiken. Allerdings beschränkte die Bundesregierung explizit die Tätigkeiten des BND mit Blick auf europäische Ziele so, dass der ursprünglichen Kritik der Kanzlerin am Ausspähen unter Freunden, eine Beschränkung der eigenen Beschützer-Rolle folgte. Sie begrenzte damit die Referenz (Schutz vor wem?) der Rolle und etablierte hohe Anforderungen für die Überwachung europäischer Ziele.

In Großbritannien reagierte die Regierung offensiv auf die Enthüllungen und suchte die Funktionsfähigkeit der Beschützer-Rolle unter anderem durch das Vorgehen gegen den Guardian zu wahren und weitere Publikationen zu verhindern. Die britische Regierung wurde domestisch mit weniger Kontestationen der Beschützer-Rolle konfrontiert als die deutsche. Die historischen Selbstbezüge erlaubten der Regierung im Vereinigten Königreich dabei gleich in doppelter Hinsicht eine expansivere Beschützer-Rolle. Einerseits konnte sie zum Nachweis der Notwendigkeit weitreichender sicherheitspolitischer Maßnahmen auf die historischen Erfahrungen mit Terrorismus verweisen. In diesem Kontext wurde der Auf- und Ausbau der Beschützer-Rolle unter Bezugnahme auf Terrorismus in Nordirland sowie auf die Anschläge vom 7. Juli 2005 in London gerechtfertigt. Damit war die Gefahrensituation für das Vereinigte Königreich stets präsenter. Anderer-

seits konnte die Regierung auf die historischen Leistungen der Sicherheitsbehörden verweisen. Das GCHQ als zentrale Institution für die britische Cybersicherheitspolitik genießt unter allen politischen Parteien einen ausgezeichneten Ruf. Auch überwachungsskeptische PolitikerInnen betonten die historischen Leistungen des Nachrichtendienstes. Historischer Bezugspunkt war dabei zumeist der Zweite Weltkrieg und die Erfolge, die durch die Entschlüsselung deutscher Kommunikation möglich wurden. Die vergangenen Herausforderungen wurden dabei auf eine Stufe mit der aktuellen Gefahrenlage gestellt und erforderten so auch im Cyberspace einen handlungsfähigen Nachrichtendienst. Dieses Vertrauen in die Institution, das von zahlreichen domestischen signifikanten Anderen geteilt wurde, ermöglichte es der britischen Regierung insgesamt eine deutlich offensivere und weitreichendere Beschützer-Rolle einzunehmen. International wurde die Ausrichtung des Nachrichtendienstes folglich nicht angepasst. Aus Sicht der Regierung ist es für die Sicherheit im Vereinigten Königreich zudem zentral, dass das GCHQ international als technisch versiert und auf Augenhöhe mit der NSA wahrgenommen wird. So wird aus Sicht der Regierung eine Kooperation mit dem GCHQ attraktiv und der Datenaustausch gesichert. Die Einbettung in den Kreis der 5-Eyes stabilisierte die expansive Beschützer-Rolle so auf internationaler Ebene.

Mit Blick auf die militärische Nutzung des Netzes betonten zwar beide Regierungen, die Übertragbarkeit etablierter völkerrechtlicher Vorgaben. In der Einschätzung, was legitim sein sollte, unterscheiden sie sich dennoch. Während die deutsche Regierung zur freiwilligen Selbstbeschränkung mit Blick auf die militärische Zielauswahl bereit ist, entwickelt die britische Regierung eine Bandbreite verschiedener Angriffsmöglichkeit, darunter auch solche mit potenziell schwerwiegenden kinetischen Effekten. In beiden Untersuchungsstaaten lag die Referenz (Schutz für wen?) der militärischen Beschützer-Rolle zunächst auf dem Schutz der Infrastruktur der Streitkräfte, um die sicherheitspolitische Handlungsfähigkeit zu wahren. In beiden Untersuchungsstaaten wurden aber unter Verweis auf die immer ausgefeilteren Angriffe und die wachsende Verwundbarkeit eigene Angriffskapazitäten aufgebaut. Die Bundesregierung betonte in diesem Kontext domestisch, dass Cyberangriffe geringere kinetische Effekte und Kollateralschäden verursachen und daher militärische Ziele relativ schonend erreicht werden könnten. Die historisch gewachsenen domestischen Begrenzungen der militärischen Beschützer-Rolle wurden von der Regierung nach Kontestationsprozessen der parlamentarischen Opposition bestätigt und auf die Cybersicherheitspolitik übertragen. So versicherte die Regierung, dass der Einsatz der CNO-Kräfte ein konstitutives Mandat des Bundestages erfordert. Cyberangriffe erreichen bislang aber kaum die Schwelle eines bewaffneten Konflikts, so dass es in Deutschland nach wie vor umstritten ist, ob bzw. wann die Bundeswehr auf Cyberangriffe reagieren darf. Die Bundesregierung hat die Beschützer-Rolle

in diesem Kontext im Gegensatz zur britischen Regierung nicht neu ausgerichtet, da aufgrund der domestischen Beschränkungen im Bereich des Militärs ein flexibler Einsatz unterhalb der Schwelle eines bewaffneten Angriffs unzulässig ist. Die Beschützer-Rolle blieb damit auf die historisch gewachsenen Aufgaben Landesverteidigung bzw. parlamentarisch mandatierte Einsätze beschränkt. Die Debatte um die Zuständigkeit für einen Hack-Back im Falle eines Cyberangriffs illustriert diese unsichere Gestaltung der Beschützer-Rolle.

Die britische Regierung sah in offensiven Cyberfähigkeiten dagegen schon früh ein wichtiges Werkzeug zur Abschreckung feindlicher Staaten. Nach den zunehmenden internationalen Spannungen mit Russland und insbesondere nach der Vergiftung von Sergei Skripal, wurde Russland zum Referenzpunkt der Rolle (Schutz vor wem?). Die Beschützer-Rolle der britischen Regierung wurde daher flexibel auf die internationale Konfrontation mit Russland zugeschnitten. Cyberangriffe sind aus dieser Warte ein sicherheitspolitisches Werkzeug unterhalb der Schwelle einer konventionellen Vergeltung. Sie ergänzten damit das Portfolio sicherheitspolitischer Handlungsmöglichkeiten. Domestisch musste die Regierung aber auch dem Parlament Kontrollrechte mit Bezug zu den neuen Fähigkeiten einräumen. Sie betraute daher das ISC mit der Überwachung der offensiven Cyberkapazitäten. Da die Trennung zwischen den drei Untersuchungsbereichen in Großbritannien nicht so ausgeprägt ist wie in Deutschland, wurde das GCHQ mit der Entwicklung dieser neuen Kapazitäten beauftragt.

3. Da die Untersuchungsbereiche aufgrund ihrer Akteurskonstellationen und historischen Bezüge durch unterschiedliche Interaktionsprozesse geprägt sind, kommt es zu unterschiedlichen Konvergenzen von Interaktionsarenen.

Mit der Kooperation zwischen GCHQ und den britischen Streitkräften wird deutlich, dass die klare Trennung der drei Sphären zwar konzeptionell und analytisch hilfreich ist, dass diese empirisch durch die Praxis der Cybersicherheitspolitiken aber mitunter unterlaufen wird. Dies kann als ein eigenständiger Befund gewertet werden, denn die Konvergenz verschiedener Untersuchungsbereiche ist nicht in beiden Untersuchungsstaaten erfolgt. Nur in Großbritannien ist mit dem GCHQ eine Institution entstanden, die Funktionen in unterschiedlichen Bereichen übernimmt und diese so verknüpft. Das GCHQ ist erstens maßgeblich am Aufbau offensiver Fähigkeiten für das Militär beteiligt und führt in diesem Kontext auch Operationen durch. Es ist zweitens mit der Signals Intelligence beauftragt und stellt drittens seine Expertise durch das NCSC auch Strafverfolgungsbehörden zur Verfügung. In Deutschland besteht dagegen nach wie vor eine stärkere Trennung zwischen den Handlungsfeldern, die durch innenpolitische Kontestationen stabilisiert wird.

Die Teilung ergibt sich aus den historisch geronnenen Beschützer-Rollen. Die Debatte um die Zuständigkeit für einen Hack-Back im Falle eines Cyberangriffs

stehen ebenso exemplarisch hierfür wie Diskussionen um das Trennungsgebot. Hier wird der Spielraum der Regierung einerseits durch die historisch gewachsenen Rollenbegrenzungen der Verfassung und durch die domestische Kontestation beschränkt. Zwar beraten die unterschiedlichen Institutionen im Nationalen Cyber-Abwehrzentrum über Reaktionen auf Cyberangriffe – ein Austausch findet also statt. Die Zuständigkeit für Vergeltungsmaßnahmen im Cyberspace ist aber nach wie vor nicht entschieden. Die Debatte, ob digitale Vergeltung durch den BND oder die Bundeswehr erfolgen, hält nach wie vor an. Beide Varianten würden gesetzliche Neuregelungen erfordern. Außerdem wurden in Deutschland auch Bedenken mit Blick auf das Völkerrecht formuliert, wonach militärische Cyberangriffe nur durch Kombattanten durchgeführt werden dürften. Eine enge Verzahnung im Sinne einer Arbeitsteilung zwischen Militär und Nachrichtendiensten ist in Deutschland daher schwieriger als in Großbritannien. Die britische Regierung konnte das GCHQ und die Streitkräfte gemeinsam mit dem Aufbau der militärischen Beschützer-Rolle betrauen, ohne folgenreiche Kontestationen auszulösen. Damit stellte die Regierung eine institutionelle Verknüpfung zwischen der nachrichtendienstlichen und militärischen Beschützer-Rolle her. Dies wurde wiederum durch die historischen Selbstbezüge ermöglicht, die auch auf die erfolgreiche Zusammenarbeit der Streitkräfte mit dem GCHQ verwiesen. Daher wurde es auch möglich, dass die offensiven Maßnahmen gegen den Islamischen Staat durch den Nachrichtendienst ausgeführt wurden. Im Gegensatz zu Deutschland, erkannte die britische Regierung hierin keine völkerrechtlichen Probleme.

4. Es bestehen unterschiedliche Wechselwirkungen zwischen den Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte.

Die Beschützer-Rollen wurden in den Untersuchungsstaaten immer wieder durch Bezüge zu den Rollen Wohlstandsmaximierer und Garant liberaler Grundrechte beschränkt oder katalysiert. Im Folgenden werden einige dieser Prozesse kurz skizziert.

Sowohl in Deutschland als auch in Großbritannien wurde die Etablierung der Beschützer-Rollen im Bereich der Strafverfolgung zunächst durch die Rolle des Wohlstandsmaximierers katalysiert. Von der neuen Verwundbarkeit waren zunächst überwiegend Unternehmen betroffen und die volkswirtschaftliche Prosperität schien gefährdet. Dies ermöglichte den Regierungen ihre Beschützer-Rollen einzunehmen und Cyberkriminalität zu sanktionieren. Beschränkungen der Rolle wurden ebenfalls an der Rolle als Wohlstandsmaximierer ausgerichtet. So galt es durch die Regelungen nicht zu tief in die wirtschaftlichen Freiheiten einzugreifen.

Im Bereich der militärischen Beschützer-Rolle entfaltete sich ebenfalls eine katalytische Wirkung der Rolle als Garant liberaler Grundrechte. Diese führte in

beiden Untersuchungsstaaten dazu, dass das demokratische System nach 2016 selbst zur Referenz (Schutz für wen?) der Beschützer-Rolle wurde. Dies wurde durch den Verdacht ermöglicht, der US-Präsidentschaftswahlkampf bzw. das Brexit-Referendum seien durch Cyberangriffe von außen manipuliert worden. In der Folge wurde das demokratische System selbst zum Schutzgut, bemerkenswert ist, dass dies in beiden untersuchten Staaten im Kontext der militärischen Schutzfunktion debattiert wurde.

Katalytische oder begrenzende Wirkungen fanden aber nicht in beiden Untersuchungsstaaten gleichläufig statt. Auch hier ergeben sich Unterschiede, die durch die unterschiedlichen Interaktionen verstehbar werden. Im Bereich der Nachrichtendienste besteht in Großbritannien eine potenziell katalytische Beziehung zwischen der Rolle als Wohlstandsmaximierer und der Beschützer-Rolle. Sie äußert sich in der Zuschreibung, dass die Nachrichtendienste auch mit der Aufgabe betraut sind, das ökonomische Wohlergehen des Vereinigten Königreichs zu sichern. Eine Funktion, die auch in der Auseinandersetzung um nachrichtendienstliche Befugnisse für einen Ausbau sicherheitspolitischer Kompetenzen angeführt wird. Dieses Verhältnis wurde domestisch zwar kritisiert, bisher allerdings nicht aufgelöst. Im Gegensatz dazu beschränkt in Deutschland die Rolle als Wohlstandsmaximierer die Beschützer-Rolle in diesem Bereich, da die Bundesregierung hofft, durch das explizite Verbot von Wirtschaftsspionage, eine neue Norm zu unterstützen. Dies steht exemplarisch dafür, dass die Rollen nicht immer in gleicher Weise auf die Politiken wirken, sondern auch hier ergeben sich in der Interaktion Differenzen.

In beiden Untersuchungsstaaten hat die Rolle als Garant liberaler Grundrechte jedoch beschränkend auf die Beschützer-Rollen gewirkt. So haben die Exekutiven die Kontrollfunktionen der Parlamente und der Judikativen gestärkt. Dies gilt für den Bereich der Strafverfolgung, der juristisch kontrolliert wird. Aber auch für die Nachrichtendienste, wo sowohl in Deutschland als auch in Großbritannien neue Institutionen zur Kontrolle der Geheimdienste etabliert bzw. bestehende Institutionen gestärkt wurden. Außerdem sicherte die Regierung den Parlamenten bei militärischen Cyberoperationen die gleichen Kontrollbefugnisse wie beim Einsatz konventioneller Mittel zu.

Insgesamt wurde die Beschützer-Rolle in Deutschland deutlicher durch die Rolle als Garant liberaler Grundrechte beschränkt, als dies in Großbritannien der Fall war. Im Außenverhalten hat bspw. die anhaltende Kontestation der Beschützer-Rolle im Bereich der Strafverfolgung dazu geführt, dass die Bundesregierung einen europäischen Vorschlag zum Zugriff ausländischer Ermittlungsbehörden auf Daten in Deutschland ablehnte. Diese Haltung resultiert aus der Besorgnis, dass die Rolle als Garant liberaler Grundrechte durch Dritte nicht angemessen wahrgenommen werden könnte. Oft erfolgte die Beschränkung der Beschützer-Rolle in Kombination mit Verweisen auf das negative historische

Selbst oder aus den entsprechend historisch geronnenen Begrenzungen der Beschützer-Rolle. Dies zeigt sich bspw. bei der Regulation von Verschlüsselung und der restriktiven militärischen Nutzung des Netzes.

Insgesamt konnte die Untersuchung damit die bestehenden Befunde aus Sekuritisierungsstudien ausdifferenzieren und ein detaillierteres Bild der Cybersicherheitspolitiken zeichnen. Dies ist auch für das Verständnis potenzieller internationaler Kooperation hilfreich.

7.1.2 Implikationen für die internationale Cybersicherheitsordnung und das Netz

Die Darstellung, internationale Cybersicherheitsnormen seien nur zwischen Demokratien und Autokratien umstritten, konnte durch die Untersuchung differenziert werden. Die Regierungen der Untersuchungsstaaten weisen in ihren Politiken Unterschiede bei der Unterstützung internationaler Normen auf. Außerdem konnte die Analyse zeigen, dass auch die Cybersicherheitspolitiken der beiden Demokratien die IT-Sicherheit im globalen Netz unterminieren und potenziell geeignet sind, Unsicherheit zu verbreiten.

Konkret zeigt sich, dass Bestrebungen zur Regulation der militärischen Nutzung des Internets durch die britische Regierung von Beginn an grundsätzlich abgelehnt wurden. Die britische Regierung zeigte keine Bereitschaft, die Beschützer-Rolle im Cyberspace signifikant zu beschränken, sondern sieht in ihr eine logische Erweiterung des eigenen (Abschreckungs-)Potenzials. Die deutsche Bundesregierung dagegen setzte sich auch nach der Etablierung erster offensiver Kapazitäten im Jahr 2007 für eine Kultur der Zurückhaltung im Cyberspace ein. Die Position, die Bundeswehr arbeite nicht an Schadsoftware zeigt die Bereitschaft zur freiwilligen Selbstbeschränkung der Beschützer-Rolle. Sie wäre so mit einer weitgehenden Regulation militärischer Kapazitäten im Sinne eines Regimes zur Kontrolle von Cyberwaffen theoretisch vereinbar gewesen. Erst als sich die außenpolitische Gefahreneinschätzung änderte und signifikante Andere diese Haltung nicht teilten, gab auch die Bundesregierung diese Haltung auf. Beide Regierungen haben stets betont, dass die bestehenden völkerrechtlichen Regelungen auf den Cyberspace übertragbar seien. Während die deutsche Exekutive aber nach wie vor auf das explizite Verbot von Angriffen auf bestimmte Infrastrukturen hinarbeitet, ist eine solche Beschränkung der Beschützer-Rolle für die britische Regierung nicht akzeptabel, da sie in ihren Cyberfähigkeiten die Möglichkeit zur flexiblen Reaktion auf unterschiedliche Angriffsszenarien sieht. Das GCHQ hat im Zuge der parlamentarischen Kontrolle eingeräumt, auch die Fähigkeit zu folgenschweren Cyberangriffen aufzubauen. Dies legt zumindest die Vermutung nahe, dass es sich hierbei um Angriffe gegen kritische Infrastrukturen handeln könnte.

Der Aufbau einer verifizierbaren Kultur der Zurückhaltung wird zudem durch die verdeckten Operationen im Netz erschwert. Beide Regierungen nutzen das Netz zur Durchführung klandestiner Operationen. Die deutsche Bundesregierung hat im Kontext der militärischen Nutzung explizit darauf hingewiesen, dass zwar die durchführenden Kräfte als Kombattanten zu erkennen sein müssten, dass dies aber nicht für die technische Infrastruktur der Angriffe gelte. Auch wenn die gezielte Nutzung falscher Identitäten zur Schuldverschiebung aus Sicht der deutschen Regierung verboten ist, ist die Möglichkeit einer Fehlattribution in diesen Fällen dennoch gegeben. Die Sicht der britischen Regierung auf das Völkerrecht definiert ein noch weitreichenderes Handlungsrepertoire für staatliche Cyberoperationen. So erkennt die britische Exekutive in Cyberangriffen nicht zwingend eine Verletzung nationaler Souveränität. Erst wenn durch diese Aktivitäten eine nicht klar definierte Schwelle (bspw. die Manipulation von Wahlen) überschritten wird, stellt dies für die britische Exekutive eine Verletzung der Souveränität dar. Unterhalb dieser Schwelle sind Cyberangriffe damit legitim.

Verdeckte Operationen gegen Ziele im Ausland führen nicht nur die militärischen Cyberkräfte durch, sondern auch die Nachrichtendienste. Die britische Regierung hat mit dem Angriff auf Belgacom gezeigt, dass sie den Einsatz von Cyberkapazitäten auch gegen Verbündete nicht scheut. Sie sieht in der Überwachung Verbündeter Regierungen eine übliche nachrichtendienstliche Praxis. Die deutsche Regierung hat zwar die Überwachung europäischer Ziele beschränkt, sonst aber die Überwachungstätigkeiten des BND weitgehend legalisiert. Mit Blick auf das Eindringen in gegnerische Systeme ist auch das nicht unproblematisch, da die mit der Infiltrationen verbundenen Intentionen nicht ersichtlich sind und so zur Eskalation beitragen können. Die beiden Demokratien tragen so auch zur globalen Unsicherheit im Cyberspace bei. Was als unzulässige Operation im Netz gewertet wird, ist damit bereits zwischen diesen beiden Regierungen umstritten.

Die Cybersicherheitspolitiken der beiden Regierungen haben dabei auch Folgen für das globale Netz. Beide Regierungen nutzen Sicherheitslücken in allen drei Untersuchungsbereichen. Damit unterminieren sie potenziell die IT-Sicherheit im gesamten Internet, da Fehler nicht gemeldet und Lücken nicht geschlossen werden. Die unintendierten Konsequenzen, die durch die Geheimhaltung entstehen können, wurden durch WannaCry eindrücklich illustriert. Zur Bewertung, ob eine Sicherheitslücke gemeldet oder geheimgehalten wird, evaluieren die Staaten nur die Gefahren für die nationalen Infrastrukturen. Eine Schutzpflicht für das Netz als Ganzes, wie es immer wieder von VertreterInnen der Netzgemeinde gefordert wird, ist damit nicht anschlussfähig. Es lässt sich zwar argumentieren, dass die meisten Industrienationen von ähnlichen kommerziellen Soft- und Hardwareprodukten abhängig sind, sodass die Risikoeinschätzungen potenziell ähnlich ausfallen könnten. Dies ist aber keine Gewähr dafür,

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