abductive methodology, based on the joining together of emipirics and analytics« (Pouliot, 2017, S. 252). Ganz im Sinne der pragmatistischen Perspektive wird die erreichte Erkenntnis dabei stets als fallibel und offen für Herausforderungen verstanden »[…] because configurations of practices are so complex and shifting […] one can never claim to have found the one causal practice« (ebd., S. 259). Mittels Practice Tracing wurde für jeden der Untersuchungsbereiche ein möglichst plausibler Interaktionsverlauf rekonstruiert (s. Kapitel 4). Ferner soll durch diese Methode untersucht werden, ob es in diesen Interaktionsverläufen weitere Gemeinsamkeiten oder Unterschiede zwischen den Fällen gibt, die den konkreten Umgang mit dem neuen Problemfeld in beiden Staaten prägen.

3.3 Rollen und Handlungskontexte

Da die Arbeit einen Beitrag zur sicherheitspolitischen Forschung liefern soll, steht die Rolle als Beschützer im Zentrum des Analyseinteresses. Die Materialauswahl hat bereits verdeutlicht, dass das empirische Material so gewählt wurde, dass sicherheitspolitische exekutive Funktionsübernahmen sowie deren Herausforderung strukturiert nachvollzogen werden können. Andere Rollen, die die Regierungen ebenfalls übernommen haben, bspw. um das Netz zur Steigerung des nationalen Wohlstands zu nutzen, scheinen nur an den Stellen auf, an denen Berührungspunkte zur Beschützer-Rolle bestehen. Dies bedeutet nicht, dass diese anderen Rollen empirisch weniger bedeutend sind. Der Forschungszuschnitt und die analytische Engführung ergibt sich vielmehr aus dem sicherheitspolitischen Erkenntnisinteresse. Wenn im Folgenden die drei Rollen beschrieben werden, die für die britische und deutsche Cybersicherheitspolitik besonders relevant sind, ist damit folglich nicht impliziert, dass die Arbeit alle drei empirisch in gleichrangiger Weise eingehend analysiert. Vielmehr geht es darum zu untersuchen, wie die Beschützer-Rolle ausgestaltet wurde. Dies erfolgte aber teilweise unter Verweis auf andere Rollenübernahmen. Diese sind daher für die Analyse nicht gänzlich ausblendbar und für das Verständnis der Politikentwicklung hilfreich.

Die Regierungen haben bereits mit der Öffnung des Internets begonnen, den Schutzanspruch für ihre Bevölkerungen auch online gegen neue Gefahren durchzusetzen. Die Beschützer-Rolle zeichnet sich in der Cybersicherheitspolitik durch eine doppelte Funktionsübernahme aus: Erstens fallen hierunter Maßnahmen zur Gewährleistung von Sicherheit, die durch Verletzung der Cybersicherheit »erkauft« werden. Konkret geht es also um Situationen, in denen der Staat IT-Sicherheit bricht, um sicherheitspolitisch handlungsfähig zu bleiben oder zu werden. Dies kann im Rahmen der Strafverfolgung bspw. zum digitalen Abhören von Kriminellen notwendig sein. Zweitens umfasst die Beschützer-Rolle Definitionen und Sanktionen für unangemessene Unterminierungen von IT-Sicherheit

im Cyberspace. Hier wird festgelegt, was als akzeptables Verhalten im Netz angesehen wird. In der Beschützer-Rolle tritt eines der einleitend skizzierten Dilemmata der Cybersicherheitspolitik offen zutage (s. Kapitel 1): Regierungen unterminieren und fördern Cybersicherheit in unterschiedlichen sicherheitspolitischen Handlungskontexten (Nissenbaum, 2005).

Wann immer die Regierungen Funktionen mit Bezug zu einer dieser beiden Ebenen übernehmen oder delegieren, wird das folglich als Beschützer-Rolle bezeichnet. Wenn die Regierungen die Referenz der Rolle, den Regelungsbereich, die Befugnisse zur Erreichung der Schutzziele oder ein Delegationsverhältnis verändern, wird das als Wandel der Rolle verstanden. Genau genommen hat die Beschützer-Rolle zwei Referenzen: Eine nimmt Bezug auf das zu schützenswerte Gut (Schutz für wen/was?), die zweite weist auf den abzuwehrenden Anderen (Schutz vor wem?). Diese beiden Referenzen sind theoretisch veränderbar.

Oft kommt es bei Veränderungen der Beschützer-Rolle zu Wechselwirkungen mit den beiden weiteren Rollen, die daher auch in der empirischen Analyse erscheinen. Eine Wechselwirkung ergibt sich dabei im Kontext der ökonomischen Nutzung des Netzes. Die globale Vernetzung und die Möglichkeit praktisch verzögerungsfrei Informationen auszutauschen, hat das Internet rasch zu einem bedeutenden Wirtschaftsfaktor gemacht, der entscheidenden Einfluss auf gesellschaftlichen Wohlstand haben kann. Die Rolle Wohlstandsmaximierer zielt auf den Erhalt, den Ausbau bzw. die Wiederherstellung der ökonomischen Leistungsfähigkeit der Gesellschaft. Sicherheitspolitische Regulationen können diesen neuen Wirtschaftsraum beeinflussen. Die zweite Funktion, die häufig Verbindungen mit der Beschützer-Rolle aufweist, bezieht sich auf die Wahrung von Grundrechten bzw. der demokratischen Ordnung (bspw. der Gewaltenteilung). Maßnahmen der Cybersicherheitspolitik werfen hier bspw. die Frage nach dem Schutz der Privatsphäre im digitalen Raum auf oder beziehen sich auf die Kontrolle der Exekutive. Bereits mit dem Aufkommen der neuen Technologie waren Hoffnungen auf eine erweiterte demokratische Teilhabe und eine Schwächung von autoritären Regimen verbunden (s. Kapitel 2). Demokratische Regierungen sehen sich daher in der Pflicht die demokratischen Freiheiten auch online zu schützen oder gar zu verbreiten. Die Rolle als Garant liberaler Grundrechte umfasst folglich Funktionsübernahmen, die darauf zielen liberale Freiheits-, Abwehr- und Partizipationsrechte zu garantieren bzw. diese auszuweiten oder wiederherzustellen sowie die Gewährleistung der demokratischen Ordnung.

Mit diesen Rollen sind damit beständig an die Regierungen herangetragene Erwartungen verbunden, die diese zum Ausgleich bringen muss, um stabile domestische wie internationale Beziehungen zwischen den Handelnden zu etablieren bzw. aufrechtzuerhalten.

Tabelle 2: Definition der drei Rollen, Quelle: Eigene Darstellung

Rolle	Kurzbeschreibung
Beschützer	Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Sicherheit zielen und IT-Sicherheit unterminieren sowie Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Cybersicherheit zielen.
Wohlstandsmaximierer	Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung ökonomischer Leistungsfähigkeit zielen.
Garant liberaler Grundrechte	Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Partizipations-, Abwehr- und Freiheitsrechten zielen.

Zwischen diesen generischen Rollen kann es zu unterschiedlichen Wechselwirkungen kommen.[8] Wie im Theoriekapitel bereits angeklungen ist, differenziert die Analyse drei verschiedene Wirkungen, die in der empirischen Analyse bedeutend sein können. Erstens können die unterschiedlichen Funktionsübernahmen dazu führen dass die Beschützer-Rolle erweitert wird – katalytische Wirkung. Sie liegt vor, wenn der Regelungsbereich oder die Regelungstiefe der Beschützer-Rolle durch Bezug zu anderen Rollen ausgebaut wird. Dies kann bspw. dann der Fall sein, wenn durch zunehmende Cyberangriffe Firmen wachsende Verluste erleiden zu deren Vermeidung dann sicherheitspolitische Maßnahmen ergriffen werden. Zweitens kann die Beschützer-Rolle durch Prozesse der Rollenkontestation eingeschränkt werden – beschränkende Wirkung. Sie liegt vor, wenn der Regelungsbereich oder die Regelungstiefe der Beschützer-Rolle verringert wird. Das kann bspw. der Fall sein, wenn weitreichende staatliche Eingriffe in die Verschlüsselung Geschäftsgrundlagen unterminieren und daher eine restriktive, sicherheitspolitisch gewünschte, Regulierung unterbleibt. Die dritte theoretische Möglichkeit ist folglich, dass es entweder keine Beeinflussung gibt, bzw. dass diese indifferent oder ambivalent ist. Zusätzlich kann auch das historische Selbst katalytisch oder beschränkend wirken. Wie die Interaktion verläuft und welche Dynamiken letztlich auftreten, kann nur in der konkreten Handlungssituation interpretiert werden.

Die Entscheidung darüber, welche Arenen für die Cybersicherheitspolitik zentral sind, wurde ebenfalls nicht ex ante getroffen, sondern ist Ergebnis der ersten Analyse. Die Unterscheidung von drei Handlungsräumen dient dem Ziel, den systematischen Vergleich beider Fälle zu strukturieren. Sie folgt gleichzeitig einer rollentheoretischen Logik, da die Interaktionen in den Analysebereichen aufgrund

8 Das bedeutet nicht, dass die Rollen selbst diese Wechselwirkungen entfalten, sondern, sie entstehen durch die Interaktion der Handelnden (s. Kapitel 2).

der verschiedenen Handelnden unterschiedlich verlaufen können. Die Differenzierung fußt dabei auf der institutionellen Ausgestaltung des Interaktionsrahmens. Bei der Analyse wurde deutlich, dass die Regierungen Cybersicherheitspolitik weitgehend entlang tradierter sicherheitspolitischer Institutionen gestaltet haben.

Im ersten Interaktionskontext stehen daher die Kompetenzen der Strafermittlungsbehörden im Mittelpunkt des Interesses, im zweiten geht es um die Nutzung des Internets durch die Geheimdienste und im dritten um die militärische Dimension des neuen Handlungsraumes. In diesen Bereichen haben die Regierungen ihre Beschützer-Rollen im Verlauf des Untersuchungszeitraums entwickelt. Die Interaktionskontexte zeichnen sich sowohl innen- als auch außenpolitisch durch unterschiedliche Akteurskonstellationen aus. Innenpolitisch stehen in der ersten Sphäre die Polizeibehörden im Fokus des Untersuchungsinteresses. In beiden Staaten geht es hierbei um die übergeordneten Polizeien, das Bundeskriminalamt bzw. die Serious Crime Agency.[9] Im zweiten Untersuchungsbereich liegt der Analysefokus auf den Kompetenzen der Auslandsgeheimdienste.[10] Im Zentrum der Untersuchung stehen daher der Bundesnachrichtendienst sowie das GCHQ. Der dritte Komplex befasst sich mit der militärischen Nutzung des Netzes und analysiert daher, welche Aufgaben der Bundeswehr bzw. den British Armed Forces übertragen wurden. Auch internationale Interaktionen folgen dieser Differenzierung und bestätigen damit die Relevanz der Unterscheidung auf internationaler Ebene. Während in der Kriminalitätsbekämpfung der Europarat und die EU wesentliche Institutionen darstellen, verlaufen Debatten um die militärische Nutzung des Internets zumeist im Kreis der Vereinten Nationen (UN GGE) oder bilateral. Zur Spionage gibt es fast ausschließlich bilaterale Vereinbarungen und Verhandlungen, eine Ausnahme stellt der Geheimdienstverbund der angelsächsischen Staaten dar (5-Eyes).

Damit unterscheiden sich von staatlicher Seite die Institutionen, die mit den Funktionsübernahmen betraut werden. Zudem variieren die Rollenträger der Gegenrollen sowie die historischen Selbstbilder in den Untersuchungsbereichen. Daraus können unterschiedliche Interaktionsprozesse folgen. Maßnahmen, die

9 In beiden Staaten ist die Polizeigesetzgebung nicht den Bundesebenen überlassen. In Deutschland, wie in Großbritannien regeln dies die Bundesländer bzw. vier Landesteile. In beiden Staaten wurden aber substanzielle Kompetenzen den übergeordneten Polizeien übertragen. Außerdem wurden Gesetze zur Regelung der Straftatbestände sowie zur Etablierung neuer Ermittlungsbefugnisse durch die (Bundes-)Regierungen erlassen. Diese Entwicklungen stehen im Zentrum des Untersuchungsinteresses. Regelungen, die in den Landesteilen oder Bundesländern erlassen wurden, werden nur dann berücksichtigt, wenn diese Einfluss auf die Rollen der Regierungen hatten.

10 Im Fall Großbritannien auf dem mit der Signals Intelligence betrauten Dienst GCHQ.

im Bereich der Geheimdienste akzeptiert werden, werden für die Strafverfolgungsbehörden möglicherweise nicht anerkannt oder umgekehrt.

Die Differenzierung in drei Handlungskontexte ist daher eine hilfreiche Heuristik zum Verständnis der unterschiedlichen Interaktionen. Sie wird aber teilweise durch die politische Praxis unterlaufen, bspw. dann wenn für die Cybersicherheit genuin neue Institutionen geschaffen werden, die unterschiedliche Bereiche integrieren. Diese neuen Institutionen werden in der folgenden Analyse in den Kontexten betrachtet, in denen ihnen konkrete Funktionen übertragen werden. Letztlich kann aber auch durch unterschiedliche Praktiken bei der Trennung bzw. Konvergenz der Arenen das Verständnis für die Cybersicherheitspolitiken der Untersuchungsstaaten geschärft werden, schließlich werden auch sie durch unterschiedliche Interaktionsprozesse ermöglicht.

3.4 Forschungsleitende Annahmen

Aus den bisherigen theoretischen und methodisch-konzeptionellen Überlegungen ergeben sich verschiedene Annahmen über die Cybersicherheitspolitiken in Deutschland und Großbritannien. Sie folgen aus den theoretischen Argumenten zum rollentheoretischen Zwei-Ebenen-Spiel, aus der konzeptionellen Differenzierung der drei Rollen sowie aus den drei Handlungskontexten der Cybersicherheitspolitik. Die Annahmen lauten:

1. Die Regierungen beider Untersuchungsstaaten haben im Laufe des Untersuchungszeitraums ihre Beschützer-Rollen in der Cybersicherheitspolitik erweitert.
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.
3. Da die Untersuchungsbereiche aufgrund ihrer Akteurskonstellationen und historischen Bezüge durch unterschiedliche Interaktionsprozesse geprägt sind, kommt es zu unterschiedlichen Konvergenzen von Interaktionsarenen.
4. Es bestehen unterschiedliche Wechselwirkungen zwischen den Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte.