neue Politikfeld zu Beginn des Untersuchungszeitraumes noch relativ wenig Beachtung gefunden hat. Erst im Zeitverlauf und mit zunehmender Bedeutung des Netzes ist auch die Interaktionsdichte gestiegen. Sichtbarer Ausdruck der gewachsenen Bedeutung sind die Cybersicherheitsstrategien, die beide Regierungen Ende der 2000er bzw. zu Beginn der 2010er Jahre formuliert haben. Dementsprechend entfällt die Mehrheit der analysierten Dokumente auf den Zeitraum nach 2010, in dem auch die Entwicklung der Cybersicherheitspolitik erheblich an Dynamik gewonnen hat.

3.2 Die interpretative Analyse: Grounded-Theory-Methodologie und Practice Tracing

Wie andere pragmatistisch inspirierte Studien, ist auch die vorliegende Untersuchung durch ein rekonstruktives, erschließend-interpretatives Vorgehen geprägt (Franke, 2013; Franke und Roos, 2017; Herborth, 2017). Um aus dem Datenmaterial Erkenntnisse zu gewinnen, wurde ein zweistufiges Analyseverfahren gewählt, das in der ersten Phase an der Grounded-Theory-Methodologie (Strauss und Corbin, 1996) orientiert ist und in der zweiten Phase auf Practice Tracing (Pouliot, 2017) zurückgreift. Beiden Ansätzen ist gemeinsam, dass es nicht darum geht, kausale Gesetzmäßigkeiten zu finden, sondern durch eine in der Empirie verankerte, interpretative Analyse die Interaktionspraxis in den jeweiligen Kontexten offenzulegen und damit das Verständnis der Politiken zu ermöglichen. Die Grounded-Theory-Methodologie wurde angewendet, um die generischen Rollen beider Regierungen sowie die zentralen Interaktionsfelder zu identifizieren. Die Vorgehensweise wurde also dazu genutzt, zentrale Konzepte aus der Empirie zu rekonstruieren und damit die Grundlagen zu etablieren, die dann die weitere Analyse ermöglichten. Practice Tracing diente als konstitutiv-logische Variante des Process Tracing und erlaubt es, die Entwicklung der Cybersicherheitspolitiken systematisch nachzuvollziehen und die Rollen zueinander in Beziehung zu setzen. Beide Ansätze sind dabei wesentlich durch den US-amerikanischen Pragmatismus geprägt.

Eine rekonstruktionslogische Vorgehensweise, die sich an der Methodologie der Grounded-Theory orientiert, zeichnet sich dadurch aus, dass »die Forschenden ihren Gegenständen mit einer offenen Grundhaltung [begegnen; Anm. d. Verf.] und […] eine hohe Bereitschaft [zeigen; Anm. d. Verf.], sich von den Ergebnissen ihrer Rekonstruktionen überraschen zu lassen« (Franke und Roos, 2017, S. 620). Für diese Studie bedeutet das konkret, dass nicht mit vordefinierten Rollen in die Analyse gestartet wurde, sondern, dass diese in einem ersten empirischen Interpretationsschritt aus den Daten gewonnen wurden. Im ersten Zugang wurden daher die Rollen identifiziert, die die Regierungen in der Cybersicher-

heitspolitik regelmäßig übernehmen bzw. die Rollen, die die Politiken regelmäßig beeinflussen. Ferner ging es darum, die wichtigen Handlungskontexte zu finden, in denen sich Cybersicherheitspolitik entfaltet. Dabei mussten die Konzepte so abstrakt sein, dass sie zur Analyse beider Untersuchungsstaaten nützlich waren und folglich den Vergleich ermöglichten. Dieser Schritt folgte den Prinzipien der Grounded-Thoery-Methodologie, die besonderen Wert auf die offene, gegenstandsbezogene Erschließung der empirischen Daten legt: »In this method, data collection, analysis, and eventual theory stand in close relationship to one another« (Strauss und Corbin, 1998, S. 12). Konkret nutzte die Analyse hierzu das offene Kodieren:

> »Das offene Kodieren zielt darauf ab, den Sinn der einzelnen Handlungs- bzw. Textsequenzen zu rekonstruieren und die sich darin ausdrückenden Handlungsregeln mit einem Code zu versehen. Hierbei werden die verschiedenen Handlungsregeln gewissermaßen flexibel inventarisiert und der Forscher erhält im Laufe des offenen Kodierens einen immer kompletteren Überblick über die im Material sich ausdrückenden Handlungsregeln.« (Franke und Roos, 2017, S. 634)

In diesem Prozess, der stets den gegenwärtigen Erkenntnisstand kritisch reflektiert und versucht die Analyse gezielt fortzuentwickeln, wurden die Quellen nach den Rollen und Interaktionsräumen (s. Abschnitt 3.3) durchsucht. Die Quellenwahl wurde dabei so gestaltet, dass zunächst möglichst viele verschiedene Akteure und Handlungskontexte berücksichtigt wurden. Dann wurden systematisch weitere Quellen einbezogen, die zielgerichtet die weitere Schärfung der Konzepte erlaubten. Diese Analyse wurde beendet, als die zusätzliche Aufnahme von Quellen keine weiteren Erkenntnisse mehr lieferte und damit der Punkt der Sättigung erreicht war: »A category is considered saturated when no new information seems to emerge during coding, that is, when no new properties, dimensions, conditions, actions/interactions, or consequences are seen in the data« (Strauss und Corbin, 1998, S. 136).

Durch diese erste interpretative Sichtung des empirischen Materials konnten drei generische Rollen identifiziert werden, die die Regierungen beider Untersuchungsstaaten in der Cybersicherheitspolitik regelmäßig übernehmen bzw. die die Cybersicherheitspolitiken beeinflussen. Es sind dies: Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte. Ferner wurden in diesem Analyseschritt drei Handlungskontexte offengelegt, die für die Cybersicherheitspolitiken zentral sind. Sowohl die Rollen als auch die Handlungskontexte werden im folgenden Abschnitt 3.3 kurz eingeführt.

Nachdem das offene Kodieren verwendet wurde, um das »konzeptionelle Inventar« der Untersuchung zu generieren, wurde im Anschluss daran auf Practice

Tracing zurückgegriffen, um die wesentlichen Interaktionen zwischen den Akteuren nachzuvollziehen. Da der Analysefokus auf sozialer Praxis liegt, ist die Methode gut für eine rollentheoretische Untersuchung geeignet. Vincent Pouliot konzipiert Practice Tracing dabei als eine interpretative Variante des Process Tracing (Bennett und Checkel, 2017; Collier, 2011), die auch mit nicht-positivistischen ontologischen und epistemologischen Annahmen vereinbar ist und auch damit gut zur rollentheoretischen Ausrichtung dieser Untersuchung passt (Pouliot, 2017, S. 239).

Der Ansatz zielt einerseits darauf, durch eine dichte Beschreibung der empirischen Ereignisse, die Prozesse zu rekonstruieren, die Politiken ermöglichen, um dann hieran anknüpfend »Mechanismen« zu identifizieren, die abstrakt genug sind, auch auf andere Fälle anwendbar zu sein. Mechanismen sind dabei abstrakte Konzepte die erst im Forschungsprozess generiert werden und dabei helfen Vergleichbarkeit herzustellen (ebd., S. 238f.).

> »[…] social mechanisms are abstracted away from context: their whole point is to depart from reality, not to match it. As such, the mechanisms coined by researchers do not have empirical referents that would make them true or false. Instead of testing theoretical constructs, then, one should show their heuristic usefeulness […] Mechanisms refer to analytical classes of ways of doing things that the analyst deems worthwhile to group together in view of cross-case analysis.« (Ebd., S. 252f.)

Die mittels Grounded-Theory-Methodologie identifizierten drei Rollen lassen sich folglich schon als Mechanismen im Sinne des Practice Tracing verstehen, also als Konzepte, die auch von den Fällen abstrahiert werden können und beim Verständnis anderer Cybersicherheitspolitiken potenziell nützlich sein können.[7] Practice Tracing wurde, hierauf aufbauend, dazu verwendet, die Interaktionen in ihren Verläufen schrittweise nachzuvollziehen und ein Verständnis der Entwicklung der Cybersicherheitspolitiken zu ermöglichen.

Bei der Untersuchung der konkreten Interaktionsprozesse wechselt die/der Forschende beim Practice Tracing, wie auch in der Grounded-Theory-Methodologie, beständig zwischen Induktion, Interpretation und Abstraktion, um die Einflüsse offenzulegen, die die Politiken ermöglichen: »Practice tracing is thus an

7 Das bedeutet nicht, dass sie immer in gleicher Weise wirken. Vielmehr entsteht die jeweilige Wirkung immer erst in der konkreten Interaktion. Die Annahme, dass Regierungen Schutzfunktionen ausfüllen und versuchen das ökonomische Wohlergehen zu gewährleisten, ist aber auch für andere Fälle plausibel. Für Demokratien ist es ferner plausibel anzunehmen, dass sie die Freiheitsrechte schützen (Wobei bei einer Entwicklung hin zu einer Autokratie diese Funktionsübernahme aufgegeben werden kann. Daher scheint dieser Teil nur für etablierte Demokratien plausibel vgl. Kapitel 2).

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