3. Methodik und Konzeption

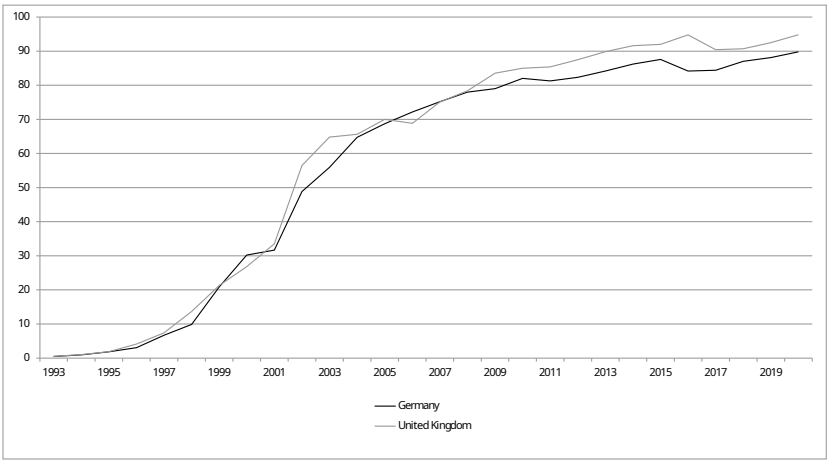
Bei der vorliegenden Studie handelt es sich um eine diachronisch-ländervergleichende Analyse, die die Entwicklung der Cybersicherheitspolitiken in zwei Untersuchungsstaaten nachzeichnen und verstehen will. Im Folgenden wird das entsprechende methodische Vorgehen vorgestellt und die grundlegenden Konzepte erläutert. Das Kapitel adressiert dazu vier Themenkomplexe. Zunächst werden die Argumente erörtert, die zur Auswahl der beiden Untersuchungsstaaten, der analysierten Dokumente und zur Festlegung des Untersuchungszeitraums geführt haben. Der zweite Abschnitt befasst sich mit dem eigentlichen Analyseprozess des empirischen Materials und orientiert sich an der Grounded-Theory-Methodologie in Verbindung mit Practice Tracing. Anschließend werden die drei Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte sowie die drei Analysebereiche kurz eingeführt. Abschließend werden die forschungsleitenden Annahmen expliziert, die sich aus den theoretisch-methodischen Überlegungen ergeben.

3.1 Auswahlentscheidungen: Fälle, Quellen und Untersuchungszeitraum

Deutschland und das Vereinigte Königreich wurden als Vergleichsfälle gewählt, da sie sich durch viele Gemeinsamkeiten auszeichnen, vermutlich aber dennoch unterschiedliche Cybersicherheitspolitiken verfolgen. Bei den Untersuchungsstaaten handelt es sich um zwei westeuropäische parlamentarische Demokratien, die sich weiterhin durch (überschneidende) Mitgliedschaften in zahlreichen internationalen Organisationen auszeichnen (bspw. in der OSZE, der EU[1], der NATO und dem Europarat). Neben diesen institutionellen Gemeinsamkeiten, bestehen

1 Auch wenn der britische Austritt aus der EU mit dem Referendum vom 23. Juni 2016 beschlossen wurde, war Großbritannien doch bis zum Ende des Untersuchungszeitraums Mitglied der EU.

Abbildung 2: Entwicklung der Internetnutzerzahlen in Deutschland und Großbritannien 1993-2017 (in Prozent der Bevölkerung), Quelle: World Bank (2019)



auch mit Blick auf die (ökonomische) Nutzung und die gesellschaftliche Einbettung des Internets kaum Unterschiede. 2017 verfügten 93% aller Haushalte in Deutschland über einen Internetanschluss, im Vereinigten Königreich waren es 94%. Mehr als dreiviertel aller BürgerInnen in beiden Staaten nutzen das Netz täglich (Eurostat, 2018a). Die zunehmende gesellschaftliche Integration des Netzes ist dabei in beiden Staaten über den gesamten Untersuchungszeitraum parallel verlaufen (s. Abbildung 2). Auch die wirtschaftliche Nutzung ist nahezu identisch: 2017 nutzten 95% aller Unternehmen im Vereinigten Königreich das Internet, in Deutschland waren es 97% (Eurostat, 2018b). Weiterhin gibt es in beiden Staaten wichtige Internetknoten (LINX in London sowie DE-CIX in Frankfurt am Main), die gemessen am Datendurchsatz zu den größten weltweit zählen. Auch in einschlägigen Indizes liegen die beiden Untersuchungsstaaten oft nahe beisammen. So sind Deutschland und Großbritannien bspw. im 2011 erstellten Cyber Power Index mit den Rängen 4 und 1 Teil der internationalen Spitzengruppe (Booz Allen Hamilton, 2011, S. 4). Damit sind beide Staaten auch bei der Ausgestaltung der internationalen Cybersicherheitsordnung von Bedeutung.

Zum Verständnis von variantem Verhalten in der Cybersicherheitspolitik, kann folglich aber nicht auf materielle Differenzen (bspw. in der Abhängigkeiten von IT) rekurriert werden. Positivistisch gesprochen folgt die Fallauswahl damit der Logik der »similar systems with different outcomes« bei der Fälle mit möglichst ähnlich ausgeprägten unabhängigen Variablen betrachtet werden, die

sich aber durch unterschiedlich ausgeprägte abhängige Variablen voneinander unterscheiden (Jahn, 2015, S. 64f.).[2]

Wie bereits im vorangegangen Kapitel dargelegt, ist die These, dass sich die Cybersicherheitspolitiken der beiden Untersuchungsstaaten trotz der zahlreichen Gemeinsamkeiten unterscheiden, eine plausible Ausgangsannahme. Empirische Analysen zu den Außen- und Sicherheitspolitiken beider Staaten haben signifikante Unterschiede offengelegt (Cornish, 2013; Harnisch, 2013; Junk und Daase, 2013; B. White, 2013). Die vorliegende Studie untersucht daher, ob bzw. inwiefern sich Differenzen auch in einem neuen sicherheitspolitischen Handlungsfeld finden und durch welche innen- und außenpolitischen Interaktionen die Politiken ermöglicht werden.

Die Wahl des Untersuchungszeitraums richtet sich daher nach dem Entstehen bzw. dem gesellschaftlichen Relevantwerden dieses neuen Interaktionsfeldes. Er beginnt 1995 und endet mit dem Jahr 2019. 1995 wurde als Ausgangspunkt der Analyse gewählt, da in diesem Jahr in beiden Staaten die gesellschaftliche Internetnutzung erstmals die 1%-Schwelle überschritten hat und in den Folgejahren rasant zugenommen hat. Damit wurde das Netz Mitte der 1990er Jahre auch für Privatpersonen nutzbar und Sicherheitsprobleme, die mit dem Netz verbunden waren, konnten zunehmend zu gesellschaftlichen Problem werden, die auch politisch reguliert werden mussten.[3] Die Interaktionsdichte ist in den Folgejahren ebenfalls gestiegen.

Um die Cybersicherheitspolitiken der beiden Untersuchungsstaaten zu analysieren, wurden zunächst die für dieses Politikfeld zentralen Akteure in beiden Untersuchungsstaaten identifiziert. Da die Rollen der Regierungen im Mittelpunkt des Forschungsinteresses stehen, bildeten die ersten Cybersicherheitsstrategien der beiden Untersuchungsstaaten den Startpunkt zur Erschließung der Akteure (Bundesministerium des Innern, 2011; Cabinet Office, 2009). Diese Dokumente sind besonders geeignet, die komplexe Konstellation aus Sicht der Exekutiven zu erschließen, da in diesen Strategien das Thema erstmals ganzheitlich betrachtet wurde und die unterschiedlichen, zuvor ergriffenen, Maßnahmen zusammenführend skizziert wurden. Die Dokumente legen damit nicht nur die relevanten Akteure aufseiten der Regierungen (Ministerien und Behörden) offen, sondern

2 Die Analyse folgt dieser Logik aber freilich ohne den Anspruch aus der Analyse allgemeingültige Gesetzmäßigkeiten im Sinne eines nomologischen Wissenschaftsverständnisses offenzulegen, sondern mit dem Ziel die Politiken und damit auch die vermuteten Unterschiede zu verstehen (s. Kapitel 2 und 3.2).

3 Es gab zwar in beiden Staaten bereits vor diesem Zeitpunkt Regelungen zum Umgang mit Computerkriminalität, diese richteten sich aber auf Wirtschaftskriminalität und waren noch nicht auf weiträumig vernetzte Systeme zugeschnitten.

nehmen auch Bezug auf parlamentarische Einflüsse (bspw. Kontrollbefugnisse) und legen Schnittstellen zu nichtstaatlichen Akteure offen.

Sie geben ferner erste Aufschlüsse darüber, welche Funktionen die Exekutive in der Cybersicherheitspolitik übernimmt. Ausgehend von diesen Dokumenten wurde dann der weitere Untersuchungszeitraum, sowohl vor als auch nach deren Veröffentlichung, durch die Sichtung weiterer Dokumente schrittweise erschlossen. Auf diesem Weg konnte identifiziert werden, welche signifikanten Anderen die Cybersicherheitspolitik beider Staaten beeinflussen bzw. dies versuchen. Weiterhin wurden auf diesem Weg zusätzliche Dokumente anderer Akteure integriert, die wiederum neue Akteure offenlegten. Das Resultat dieser ersten Erschließung der Akteure ist in Tabelle 1 abgebildet und folgte der interpretativ-offenen Vorgehensweise der Grounded-Theory-Methodologie (s. Abschnitt 3.2).[4]

Tabelle 1: Institutionen und Akteure, Quelle: Eigene Darstellung

	Deutschland	**United Kingdom**
Exekutive	Bundesregierung	HM Government
Ministerien	Bundeskanzleramt, Bundesministerium des Innern, Bundesministerium der Verteidigung, Auswärtiges Amt, Bundesministerium der Justiz, Bundesministerium für Verkehr und digitale Infrastruktur, Bundesministerium für Wirtschaft	Cabinet Office, Home Office, Ministry of Defence, Foreign Commonwealtch Office, Department for Business, Energy and Industrial Strategy
Behörden	Bundesamt für Sicherheit in der Informationstechnik, Bundesbeauftragter für den Datenschutz, Nationales Cyber-Abwehrzentrum	Office of Cyber Security and Information Assurance, Investigatory Powers Commissioner, National Cyber Security Centre
Polizeien	Bundeskriminalamt	National Crime Agency
Nachrichtendienste	Bundesnachrichtendienst	Government Communications Headquarters (GCHQ)
Streitkräfte	Bundeswehr	British Armed Forces

4 Auch wenn einige Unterschiede bestehen (bspw. die Mitgliedschaft im Nachrichtendienstverbund 5-Eyes), ergeben sich mit Blick auf die internationalen signifikanten Anderen zahlreiche Überschneidungen. Daher wird an dieser Stelle auf eine tabellarische Darstellung verzichtet. Weiterhin wurden Institutionen im Verlauf des Untersuchungszeitraumes umbenannt, restrukturiert oder neugegründet. Die Darstellung zeigt Denominationen Stand Ende 2019.

Legislative Ausschüsse und Gremien	Bundestag, Bundesrat Auswärtiger Ausschuss, Innenausschuss, Verteidigungsausschuss, Wirtschaftsausschuss, Enquete-Kommission Internet und digitale Gesellschaft, Parlamentarisches Kontrollgremium, G 10 Kommission, Ausschuss Digitale Agenda, NSA-Untersuchungsausschuss	House of Commons, House of Lords Foreign Affairs Committee, Home Affairs Committee, Defence Committee, Business Innovation and Skills Committee, Science and Technology Committee, Intelligence and Security Committee, National Security Strategy Committee
Judikative	Bundesverfassungsgericht, Bundesgerichtshof	High Court of Justice of England and Wales, The Supreme Court, Investigatory Powers Tribunal
Nichtstaatliche Akteure		
Zivilgesellschaft	Chaos Computer Club, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Gesellschaft für Informatik e.V., Gesellschaft für Freiheitsrechte e.V., Humanistische Union e.V., Reporter ohne Grenzen e.V.	Amnesty International, Article 19, Privacy International, Open Rights Group, Big Brother Watch, English PEN, Liberty, Electronic Frontier Foundation, Access Now, JUSTICE, Rights Watch UK, Human Rights Watch
Unternehmen und Branchenverbände	BITKOM, eco, DE-CIX, Deutsche Telekom, SAP	GreenNet, British Telecommunications, techUK

Diesem Schritt folgte die Erhebung der relevanten Dokumente direkt bei den identifizierten Akteuren. Dazu wurde auf die entsprechenden Internetseiten zurückgegriffen und dort systematisch nach den Begriffen IT-Sicherheit bzw. Cybersicherheit gesucht und die resultierenden Dokumente dem Untersuchungskorpus hinzugefügt.[5] Diese Datengrundlage wurde dann um weitere Quellen ergänzt, die im Analyseprozess gefunden wurden und für die Interaktionen der Akteure bedeutsam waren. Diese Datengrundlage enthält folglich Reden, Strategiedokumente, Gesetzesvorhaben, Stellungnahmen, Berichte, Parlamentsdebatten, Gutachten, Pressemitteilungen und Gerichtsurteile. Sie ermöglicht damit die Rekonstruktion der wesentlichen Interaktionen zwischen Exekutive, Legislative, Judikative und nichtstaatlichen Akteuren.

Diese, von den Akteuren selbst generierten, Quellen dienen dazu, die Interaktionen zu rekonstruieren und so einerseits die emergente Sozialstruktur zu erfassen und zusätzlich, der zweiten Prämisse Blumers folgend, die Bedeutungszuschreibung zu analysieren. Allerdings lässt sich Praxis nicht nur aus den

5 Im Englischen wurden die Begriffe IT-security und cybersecurity verwendet. Um unterschiedliche Schreibweisen zu integrieren, wurden auch die folgenden Terme gesucht: D - Cyber Sicherheit, Cyber-Sicherheit; UK - cybersecurity, cyber security, IT security. Dokumente, die ausschließlich technische Bezüge bspw. Anleitungen zur Implementierung bestimmter Standards enthalten, wurden verworfen.

Dokumenten der Akteure herausdestillieren. Daher haben pragmatistisch arbeitende WissenschaftlerInnen ihre Untersuchungskorpora oft durch weitere Quellen (meist Medienbeiträge und wissenschaftliche Literatur) ergänzt (M.-O. Baumann, 2014, S. 89), denn nicht jeder Interaktion korrespondiert ein (zugänglicher) textförmiger Beleg der Akteure. Diese ergänzenden Daten können zwar nur mittelbar zur Interpretation der Bedeutungszuschreibung durch die handelnden Akteure beitragen, sie legen aber dennoch Interaktionen offen und dienen so als komplementäres Element zu anderen Quellen. Nicht zuletzt hierin liegt ein Vorteil praxisorientierter Ansätze, die auch durch Berichte Dritter Erkenntnis über die Interaktionspraktiken gewinnen können. Im Kontext dieser Analyse ist diese flankierende Ergänzung durch Medienbeiträge besonders bedeutend, da die Studie in mindestens zwei Teilen der Untersuchung (den Bereichen der Nachrichtendienste und der Militärs) mit der Problematik staatlicher Geheimhaltung umgehen muss. Die Veröffentlichungen investigativ arbeitender JournalistInnen haben, nicht nur im Zuge der Snowden-Enthüllungen, die Erkenntnisse über die staatlichen Cybersicherheitspolitiken signifikant erweitert. Auf ihrer Grundlage wurden zuvor geheime Politiken publik und die intensive (öffentliche) Interaktion zwischen den beteiligten Akteuren ermöglicht. Die jeweiligen Interaktionskontexte werden daher durch Berichte entsprechender Medien vervollständigt.[6] Auf diesem Weg wurden aus den politischen Systemen (Regierung, Judikative, Parlament) für Deutschland 110 und für Großbritannien 131 Dokumente erhoben. Diese wurden durch Quellen von nichtstaatlichen Akteuren, internationalen Organisationen sowie Medien ergänzt. Insgesamt umfasst der Korpus mehr als 350 Dokumente.

Um Untersuchungszeiträume möglichst repräsentativ abzudecken, wird meist eine zeitliche Gleichverteilung der Quellen angestrebt (Roos, 2010, S. 57 bzw. 80f.). Für diese Untersuchung konnte dieses Ziel jedoch nicht erreicht werden, da das

6 Dabei wurde auf Beiträge in folgenden Medien zurückgegriffen: Der Spiegel, Süddeutsche Zeitung, Die Zeit, Die Welt, The Guardian, The Telegraph, The Independent und The Times. Ebenfalls berücksichtigt wurden Berichte von speziell mit IT-Sicherheit befassten Medien wie heise.de oder wired.com. Daten von Enthüllungsplattformen wie Wikileaks wurden nur dann beachtet, wenn sie durch relevante Akteure aufgegriffen wurden oder in den genannten landesweiten Medien thematisiert wurden. Dies liegt einerseits in der praxisorientierten Forschungsperspektive begründet. Solange die Handelnden diese Informationen nicht aufgreifen (das bedeutet nicht zwingend einen expliziten Bezug, sondern kann auch durch die Problematisierung einer, in geleakten Dokumenten, erwähnten Praxis erfolgen) und weiterhin interagieren als gäbe es diese Dokumente nicht, solange haben sie auch keinen Einfluss auf die (sichtbare) Interaktion. Andererseits ist der Umgang mit geleakten Informationen problembehaftet, da deren Authentizität nur schwer verlässlich verifizierbar ist. Die Snowden-Dokumente wurden ebenfalls nicht als Primärquellen hinzugezogen, da diese quellenkritisch besonders problematisch sind (s. Stellungnahme Thomas Rid (Deutscher Bundestag, 2016a, S. 36)).

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-