4.1 Deutschland

4.1.1 Das deutsche IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens

Bereits geraume Zeit vor der kommerziellen Öffnung und globalen Verbreitung des Internets in den 1990er Jahren, führte die zunehmende Nutzung von Computern zu Debatten darüber, ob bzw. inwiefern durch die neue Technik strafrechtliche Lücken entstanden seien. Die ersten Diskussionen in diesem Kontext begannen in den 1970er Jahren und waren auf die missbräuchliche Nutzung von IT-Systemen in der Wirtschaft fokussiert, da Computer zu diesem Zeitpunkt noch nicht bei den EndnutzerInnen angekommen waren. 1972 setzte das Bundesjustizministerium eine Sachverständigenkommission ein, die Vorschläge zur Reform des Wirtschaftsstrafrechts erarbeiten sollte. Aber noch im Jahr 1974 sah die Bundesregierung keinen akuten Handlungsbedarf.

> »Die bisherigen praktischen Erfahrungen mit der Anwendung des geltenden Strafrechts auf diese neue Form der Kriminalität rechtfertigen die Feststellung, daß im wesentlichen keine Lücken bestehen, die allein aufgrund der spezifischen Möglichkeiten der EDV-Technik sichtbar werden könnten. […] Im Übrigen beobachtet die Bundesregierung die weitere Entwicklung mit besonderer Aufmerksamkeit, da nicht auszuschließen ist, daß größere Lücken des geltenden Strafrechts bisher nur wegen der geringen Verbreitung dieser Kriminalität verborgen geblieben sind.« (Deutscher Bundestag, 1974, S. 6)

1978 legte die Sachverständigenkommission konkrete Entwürfe zur Regulierung der Computerkriminalität vor. Diese enthielten unter anderem auch Vorschläge zur Schaffung neuer Straftatbestände. Sie mündeten in das 1. und 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (WiKG). Während das erste Gesetz noch keine Regelungen zur Computerkriminalität enthielt, wurde mit dem am 1. August 1986 in Kraft getretenen 2. WiKG die Grundlage für die Strafbarkeit von Computerdelikten gelegt. Seit dem Einsetzen der Sachverständigenkommission hatte die Nutzung von Computern deutlich zugenommen und die Regierung sah nun die Notwendigkeit, bestehende Lücken im Strafrecht zu schließen. Das Gesetz war damit Ausdruck der Beobachtung,

> »[…] daß der zunehmende Einsatz von Datenverarbeitungsanlagen in der Wirtschaft und in der Verwaltung die Möglichkeit von strafwürdigen Mißbräuchen eröffnet, denen mit Mitteln des Strafrechts nicht hinreichend begegnet werden kann.« (Deutscher Bundestag, 1986a, S. 11)

Durch die Zuordnung zum Bereich der Wirtschaftskriminalität wird deutlich, dass der Missbrauch von Computern noch nicht als umfassendes Problem für

alle BürgerInnen gesehen wurde. Mit der Verknüpfung von Computer- und Wirtschaftskriminalität folgte die deutsche Regierung einem internationalen Trend. Explizit bezog sich die Regierung in der Gesetzesbegründung auf Empfehlungen des Europarates (ebd., S. 11). Dieser hatte bereits 1981 in einer Stellungnahme Mitgliedsstaaten zur verstärkten Bekämpfung der Wirtschaftskriminalität aufgerufen und Computerkriminalität diesem Deliktsbereich zugerechnet (Council of Europe, 1981, S. 4).

Zur Rechtfertigung des neuen Gesetzes verwies Justizminister Engelhard auf Erfahrungen mit steigenden Angriffszahlen in den USA aber auch in Deutschland, die zu einer Gefahr für die wirtschaftliche Leistungsfähigkeit geworden seien (Deutscher Bundestag, 1983b, S. 1668). Die Bundesregierung vertrat damit die auch international verbreitete Auffassung, Computer seien primär für die wirtschaftliche Prosperität und das Funktionieren der Verwaltung von Bedeutung. In der Beschlussempfehlung des Justizausschusses zum 2. WiKG heißt es daher:

> »Neue Entwicklungen im Wirtschaftsleben, wie z. B. der verstärkte Einsatz der Datenverarbeitung, haben neue Kriminalitätsformen hervorgebracht, denen mit dem bisherigen Strafrecht nicht ausreichend begegnet werden kann.« (Deutscher Bundestag, 1986b, S. 1)

Regelmäßig wurde von VertreterInnen der Regierung und des Parlaments auf den »hohen wirtschaftlichen Wert« von Daten sowie auf die wachsende IT-Abhängigkeit von Unternehmen aber auch der öffentlichen Verwaltung hingewiesen (ebd., S. 34f.). Die Notwendigkeit, neue Straftatbestände zu schaffen, wurde dabei von allen Fraktionen im Bundestag geteilt, da durch diese Delikte ein erheblicher volkswirtschaftlicher Schaden entstünde (ebd., S. 24).

Der Gesetzentwurf, der am 29. September 1983 erstmals im Bundestag debattiert wurde, war noch in Teilen von der SPD-geführten Vorgängerregierung ausgearbeitet, dann von der neuen Koalition aus CDU und FDP aufgenommen und dem Bundestag vorgelegt worden (Deutscher Bundestag, 1983b, S. 1665). Das neue Gesetz war maßgeblich durch das Bestreben geprägt, den nationalen Wohlstand durch die Vermeidung wirtschaftlicher Verluste zu erhalten bzw. auszubauen. Dabei wurde bereits auf die besonderen neuen technischen Möglichkeiten verwiesen, die Computerdelikte potenziell besonders gefährlich machten. In diesem Kontext wurde die Skalierbarkeit von Angriffen sowie die schwierige und potenziell zeitverzögerte Aufklärung der Delikte diskutiert (Deutscher Bundestag, 1983a, S. 16).

Insgesamt fügte das 2. WiKG dem Strafgesetzbuch (StGB) fünf neue Straftatbestände für Computerkriminalität hinzu: § 202a Ausspähen von Daten, § 263a Computerbetrug, § 269 Fälschung beweiserheblicher Daten, § 303a Datenveränderung und § 303b Computersabotage (Bundesgesetzblatt, 1986). Die neu-

en Paragraphen spiegelten dabei (auch in unterschiedlichen Kombinationen) die technischen Schutzziele der IT-Sicherheit wider: Vertraulichkeit, Integrität und Verfügbarkeit.

Sie sind damit der erste praktische Ausdruck der exekutiven Beschützer-Rolle im Bereich der IT. Hervorzuheben ist dabei, dass Teile der neuen Straftatbestände erst durch Vorschläge des Justizausschusses des Bundestages in das Gesetz aufgenommen wurden. Die §§ 202a sowie 303a,b wurden erst nach Beratungen im Ausschuss bzw. Anhörung von Sachverständigen in den Gesetzentwurf integriert.

Der Aufbau strafrechtlicher Regelungen wurde auch maßgeblich durch eine überparteiliche Mehrheit im Parlament vorangetrieben und unterstützt. Bemerkenswert ist, dass die neuen Tatbestände (mit Ausnahme von § 303b) dann aber doch nicht explizit mit dem Referenzobjekt Wirtschaft bzw. der öffentlichen Verwaltung verknüpft wurden. Deren Anwendbarkeit war daher auch später gegeben, als sich das Internet zunehmend zu einem Massenphänomen entwickelte. Bereits in den Debatten über das Gesetz wurde problematisiert, dass die im Zuge der Reform des Wirtschaftsstrafrechts ergangenen Regelungen nicht nur für Wirtschaftskriminelle relevant seien:

> »Weder die Vermögensdelikte wie Computerbetrug, Computersabotage und Computerspionage noch die Delikte gegen Persönlichkeitsrechte wie das Ausspähen von Daten noch die verschiedenen Verstöße gegen staatliche Sicherheitsinteressen sind typische Verhaltensweisen, die auf die sogenannten Täter mit weißem Kragen beschränkt wären. Solche Unrechtshandlungen sind vielmehr ebenso wie Diebstahl, Betrug oder Urkundenfälschung im klassischen Sinn zum Jedermann Delikt geworden, bei dem das Stimulans nicht etwa in der Eigenart des ausgeübten Berufes, sondern eher im technischen Sachverstand liegt. Man sollte deswegen im Zusammenhang mit diesem Gesetz nicht pauschal von Wirtschaftskriminalität sprechen […].« (Deutscher Bundestag, 1986c, S. 15434)

Die Erwägungen, die maßgeblich zur Erarbeitung des Gesetzentwurfes beigetragen haben, wurden also bereits bei der Verabschiedung als unzureichend betrachtet.

Dennoch waren es im Wesentlichen Erwägungen zur Sicherung unternehmerischer Freiheit, die zur Begrenzung der neuen Regeln beitrugen. Die Regierung betonte in der Gesetzesbegründung entsprechend, dass die Maßnahmen stets verhältnismäßig sein müssten und die »freiheitliche Wirtschaftsverfassung« nicht über Gebühr einschränken dürften (Deutscher Bundestag, 1983a, S. 11). Diese Bedenken schlugen sich auch konkret in der Ausgestaltung des Gesetzes nieder.

Die Regierung ging zwar davon aus, dass zur Bekämpfung des Computerbetrugs (§ 263a) technische Sicherungsmaßnahmen effektiv seien, sah aber dennoch von einer verbindlichen Regelung in diesem Bereich ab, da die Vorgaben

einerseits »wegen der fortschreitenden technischen Entwicklung nicht nur unvollkommen und wenig praktikabel« wären, sondern andererseits auch im »Widerspruch zu der persönlichen Freiheit des Betriebsinhabers« stünden (ebd., S. 16). Die Rolle als Beschützer wurde folglich durch Verweis auf die Wohlstandsmaximierung begrenzt. Auf verbindliche Maßnahmen zum unternehmerischen Selbstschutz wurde verzichtet, da derartige Vorschriften als Beschränkung wirtschaftlicher Entscheidungsfreiheit gesehen und auch von UnternehmensvertreterInnen weitgehend abgelehnt wurden. Kritischer formuliert wurde diese Zurückhaltung auch als staatlich gedeckte Chance zur unternehmerischen Sorglosigkeit gedeutet. Diese Einschätzung wurde aber lediglich von einer Minderheit (bspw. von Abgeordneten der Grünen) geteilt, die verbindlichere Regeln und ggf. auch eine Haftung von Unternehmen forderte (Deutscher Bundestag, 1986c, S. 15443).

Neben diesen Abwägungen zwischen wirtschaftlicher Freiheit und staatlichem Schutzanspruch, wurden die Regelungen ferner durch das vorherrschende AngreiferInnenbild geprägt. Debatten im Justizausschuss führten dazu, dass eine, durch die Regierung geforderte, umfassendere Strafbarkeit des § 202a verhindert wurde. Die Regierung hatte vorgeschlagen bereits das Sich-Zugriff-Verschaffen auf gesicherte Daten strafbar zu machen. Diese Bestrebungen wurden aber durch das Parlament zurückgewiesen, da die Abgeordneten in diesem Ansinnen die Gefahr einer »Überkriminalisierung« sahen (Deutscher Bundestag, 1986b, S. 28). Der Ausschuss argumentierte, dass Hacker, »die sich mit dem bloßen Eindringen z. B. in ein Computersystem begnügen, also sich keine Daten unbefugt verschaffen, von Strafe verschont bleiben [sollten; Anm. d. Verf.]« (ebd., S. 28). Die zu sanktionierenden Anderen waren Kriminelle mit kommerzieller Gewinnabsicht, nicht technikbegeisterte Jugendliche, die aus Neugier Schwachstellen suchten. Die Absicht der Regierung hatte auch in der Gesellschaft und in der sich entwickelnden IT-Community für erheblichen Widerspruch gesorgt. Im Parlament konnte in der Folge fraktionsübergreifend Einigkeit darüber hergestellt werden, dass »nur eine Regelung in Betracht kommen könne, die nicht gleich jeden jugendlichen Computer-Freak bei der Ausübung seines Hobbys zum Kriminellen stempelt« (Deutscher Bundestag, 1986c, S. 15437). Einschränkungen der Beschützer-Rolle folgten daher auch aus Kontestationen, die auf der Antizipation potenziell wenig gefährlicher Angreifer beruhten und so die Etablierung eines Gefährdungsdelikts verhinderten. Da eine weitreichende Vernetzung noch nicht vorhanden war, waren die sensibelsten Angriffe ohnehin nur durch InnentäterInnen realisierbar.

Auch wenn das 2. WiKG überwiegend durch die Interaktion zwischen domestischen Akteuren geprägt wurde, gab es doch Bezüge zu internationalen PartnerInnen, die in der gleichen Zeitspanne ähnliche gesetzliche Regelungen erlassen hatten. Neben den Empfehlungen des Europarates, orientierte sich die Bundesregierung bei der Ausgestaltung bspw. an Erfahrungen in den USA und Kanada

(§§ 303a, 303b) bzw. Österreich, Dänemark und der Schweiz (§ 263a) (Deutscher Bundestag, 1986b, S. 29f. sowie 34).

Bereits in dieser Frühphase der Rechtsentwicklung zeigte sich das dynamisch interaktive Verhältnis zwischen den zentralen exekutiven Funktionsübernahmen: Schutz und Wohlstandsmaximierung. Entsprechend der Bedeutungszuschreibung den Computer primär als essenzielles Wirtschaftsgut zu sehen, war die Rolle des Wohlstandsmaximierers katalytisch für die erste Etablierung des staatlichen Schutzanspruches in der digitalen Welt. Gleichzeitig wurden die neuen Regelungen aber auch durch diese Rolle beschränkt, da auf einen unverhältnismäßigen Eingriff in die wirtschaftliche Freiheit verzichtet werden sollte. Das 2. WiKG wurde zwar deutlich vor der Verbreitung des Internets verabschiedet, dennoch blieb es lange (bis auf Details) unverändert. Mit der Verbreitung des Internets wurden aber schnell neue Probleme deutlich und der internationale Koordinierungsbedarf wuchs rasch.

Die erste Übernahme der Beschützer-Rolle war im Wesentlichen durch die Rolle als Wohlstandsmaximierer katalysiert und begrenzt. Die Referenz der Rolle (Schutz für wen?) lag folglich auf dem Erhalt bzw. Ausbau wirtschaftlicher Prosperität. Die Beschützer-Rolle wurde daher aber auch durch ökonomische Bedenken beschränkt. Mit Blick auf Fragen der Haftung oder konkreten Vorgaben über Schutzniveaus, die potenziell in die unternehmerische Freiheit Eingreifen könnten, agierte die Bundesregierung zurückhaltend. Dies wurde auch durch die Gefahreneinschätzung ermöglicht. In dieser frühen Entwicklungsphase wurde in Deutschland noch oft über jugendliche FreizeithackerInnen debattiert, ihr Verhalten sollte durch eine zu expansive Beschützer-Rolle nicht in unangemessener Weise sanktioniert werden.

4.1.2 Kryptopolitik

Dass die neuen Kommunikationsmöglichkeiten, die mit dem Internet einhergingen, für die staatliche Schutzfunktion auch problematisch sein konnten, wurde bereits mit der Öffnung des Netzes debattiert. Die Auseinandersetzung um den Einsatz von Kryptographie zum Schutz von Kommunikation ist einer der ersten zentralen Kristallisationspunkte der Cybersicherheitspolitik. Die Möglichkeit durch Verschlüsselung, Kommunikation praktisch jedwedem Zugriff zu entziehen und damit staatliche Kontrolle schwierig oder gar unmöglich zu machen, sorgte auch in Deutschland früh für Besorgnis. In einer Rede betonte Innenminister Manfred Kanther 1994: »die Kryptierungsmöglichkeiten im Fernmeldeverkehr dürfen keine für die Verbrechensaufklärung unüberwindbare Hürde bilden« (Bundesregierung, 1994). In der Folge entwickelte sich sowohl domestisch als auch international eine rege Debatte über die Nutzung und Regulation von Kryptographie, die das Spannungsfeld zwischen exekutiver Schutzfunktion, Wohlstandsma-

ximierung und der Gewährleistung liberaler Freiheitsrechte im digitalen Raum offen zu Tage treten ließ. Die Auseinandersetzung löste dabei das Thema Verschlüsselung aus dem zuvor prägenden militärischen und geheimdienstlichen Kontext, da Kryptographie mit dem Internet potenziell allen interessierten NutzerInnen zur Verfügung stand und auch für die Wirtschaft zu einem wesentlichen Bestandteil der Internetaktivitäten wurde (Beucher und Schmoll, 1999, S. 529).

Unter Verweis auf die erschwerte Strafverfolgung im Internet forderte Innenminister Kanther immer wieder weitgehende Maßnahmen zur Regulation von kryptographischen Verfahren. Eine von ihm und den Sicherheitsbehörden bevorzugte Key-Recovery Variante sah vor, die zur Dekryptierung benötigten Schlüssel zu duplizieren und für den Staat erreichbar zu hinterlegen (Deutscher Bundestag, 1998a, S. 65). Eine Praxis die auch von der Regierung der USA vorangetrieben wurde, aber dort innenpolitisch auf beträchtlichen Widerstand stieß. In Deutschland entzündete sich an den Plänen des Innenministers heftige Kritik von unterschiedlichen Akteuren. So gab es aus der Zivilgesellschaft massiven Widerstand gegen die Vorschläge zur Schwächung von Verschlüsselung bzw. zur Hinterlegung von Schlüsseln. Der Chaos Computer Club (CCC) verband seine Kritik mit dem Vorwurf, der Innenminister verfolge mit der Schlüsselhinterlegung das Ziel, »den amerikanischen Geheimdiensten weltweit den problemlosen Zugriff auf jedwede elektronische Kommunikation zu sichern« (heise.de, 1997).

Dieser Vorwurf erschließt sich nur durch einen Blick auf die internationale Entwicklung zu diesem Zeitpunkt. Nachdem die US-Regierung in innenpolitischen Auseinandersetzungen um ein nationales System zur Schlüsselhinterlegung eine Niederlage erlitten hatte, wurden in der Folge die Exportrichtlinien für Kryptographie-Produkte gelockert.[1] Gleichsam als Ersatz sollten, geprägt durch die marktbeherrschende Stellung der US-Unternehmen, in der Folge umfassende internationale Lösungen zur Key-Recovery etabliert werden. Ziel der US-Regierung war es, einen internationalen Konsens herzustellen, der nur den Export von Produkten mit Key-Recovery-Funktionalität erlaubt hätte. Damit wäre ein System etabliert worden, in dem vermutlich ein wesentlicher Teil aller Zweitschlüssel bei US-Unternehmen hinterlegt worden wären. Dieses Szenario wurde auch durch die Enquete-Kommission des deutschen Bundestags äußerst kritisch gesehen:

1 Diese Systeme der Schlüsselhinterlegung werden oft auch als Key-Escrow bezeichnet und standen in der innenpolitischen amerikanischen Debatte um die Kontrolle von Kryptographie im Zentrum der Kritik. Die Regierung hatte mit dem Clipper-Chip 1993 einen Ansatz verfolgt, der einen staatlichen Zugriff auch auf verschlüsselte Daten ermöglicht hätte, da eine Schlüsseldublette bei der Regierung gespeichert worden wäre. Dies wurde domestisch heftig kritisiert und nachdem ein Informatiker 1994 einen Fehler im Design gefunden hatte, wurden die Pläne schließlich verworfen (Kehl, Wilson und Bankston, 2015).

> »Mit diesem Exportregime geht es der US-Regierung im Ergebnis vor allem darum, einen weltweiten Standard für Kryptoverfahren zu etablieren, der – unabhängig von der technischen Ausgestaltung im einzelnen – den unbemerkten Zugriff von US-Regierungsstellen auf den Klartext verschlüsselter Informationen auch ausländischer Nutzer von US-Produkten erlaubt.« (Deutscher Bundestag, 1998a, S. 67)

Entsprechend der Globalität des Internets, wäre damit auch eine umfassende internationale Einflussmöglichkeit für die USA entstanden. Die USA hätten dann mit dem Internet auch ihre eigene Beschützer-Rolle global verbreitet. Die Bestrebungen wurden so als Versuch interpretiert, die innenpolitisch geschwächte Beschützer-Rolle zu internationalisieren und dadurch zu kompensieren. Die Bundesregierung vertrat daher auch international die Position, dass der »Versuch, US-Politik in das Ausland zu exportieren, nicht akzeptabel sei« (ebd., S. 67).

Diese Einwände wurden mit dem Verweis auf die potenziellen Einschränkungen bzw. nachteiligen Effekte für die eigene Strafverfolgung begründet, da das amerikanische Modell »Spielräume anderer Regierungen zur Gestaltung einer eigenen Kryptopolitik« beschränke (ebd., S. 68). Außerdem äußerte die Enquete-Kommission Bedenken darüber, »daß die vertrauliche Datenkommunikation deutscher Nutzer dem Zugriff ausländischer Instanzen außerhalb des Geltungsbereichs deutscher Gesetze und unkontrolliert durch deutsche Gerichte ausgesetzt« werde (ebd., S. 67). Der globale Handlungsraum sollte also nicht neuen Regeln folgen, sondern wieder territorial rückgebunden werden. Deutsche Gerichte sollten über deutsche BürgerInnen urteilen.

Die restriktiven Exportregeln der USA hatten ferner auch direkte Auswirkungen auf die Beschützer-Rolle der Bundesregierung selbst. Auch wenn das 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) Verschlüsselungsprodukte aus den USA skeptisch beurteilte (Deutscher Bundestag, 1996, S. 4), nutzte die Verwaltung der Bundeswehr doch seit 1994 Lotus Notes, das durch die Exportkontrollgesetze der USA nur mit einer schwachen Verschlüsselung ausgestattet war. Um der NSA den Zugriff auf die Kommunikation zu erleichtern, wurden von einem Schlüssel mit einer Länge von 64 Bit die ersten 24 Bit mit dem öffentlichen Schlüssel der NSA verschlüsselt, »so daß die NSA letztendlich nur 40 Bit entschlüsseln« musste (Deutscher Bundestag, 1999, S. 3). Auch dieser Umstand hat möglicherweise zum deutschen Widerstand gegen die Pläne der USA beigetragen. Eindeutig ist, dass die Politik der US-Regierung als problematisch für die deutsche Wirtschaft gesehen wurde.

> »Als besondere Bedrohungsform kommt hinzu, daß Key Recovery für Wirtschaftsspionage durch Geheimdienste genutzt werden kann. Außerdem kann eine zentrale Hinterlegungsstelle selbst Ziel von Angriffen werden. Dieses Risiko wäre dann besonders evident, wenn es jemals zu dem von den USA vorge-

schlagenen weltweiten Key-Recovery-System käme.« (Deutscher Bundestag, 1998a, S. 33)

Mit diesem Argument warf die Enquete-Kommission auch ein zentrales Dilemma bei der Kontrolle von Kryptographie auf. Wenn Hintertüren oder Zweitschlüssel für Verschlüsselung geschaffen werden, besteht immer die Möglichkeit, dass ein/eine Dritte/r diese Schwachstellen findet und ausnutzt. In diesem Fall würde nicht nur riskiert, dass die USA selbst ihre Position ausnutzen könnten, sondern auch Kriminelle, Terrororganisationen oder andere Akteure könnten potenziell unbemerkt von einer solchen Lösung profitieren.

Als die US-Regierung versuchte im Rahmen des Wassenaar-Abkommens durchzusetzen, dass nur noch Produkte mit Key-Recovery-Funktion exportiert werden sollten, wurde das unter anderem durch den Widerstand der deutschen Regierung verhindert. Die Bundesregierung trug damit auch zur Liberalisierung des internationalen Krypto-Marktes bei. Sie setzte sich in der Folge auch dafür ein, die EG-Dual-Use-Verordnung für Verschlüsselungsprodukte zu lockern (Brunst, 2012, S. 335). Dies folgte einem internationalen Trend, der sich auch in den am 27. März 1997 verabschiedeten »Guidelines for Cryptography Policy« der OECD widerspiegelt, die ebenfalls einen liberalen Umgang mit Verschlüsselungsprodukten empfahlen (OECD, 1997).

Das synergetische Zusammenwirken der Rollen Wohlstandsmaximierer, Garant liberaler Grundrechte und Beschützer führten dazu, dass die Bundesregierung auf internationaler Ebene die Bestrebungen der USA ablehnten. Die Regierung erkannte zwar ebenfalls die sicherheitspolitischen Probleme, die mit einer Verbreitung von Verschlüsselung einhergingen, wollte aber eine global ausgedehnte Beschützer-Rolle der USA nicht akzeptieren. Die Kontestation der amerikanischen Bemühungen ergab sich sowohl aus wirtschaftlichen als auch bürgerrechtlichen Erwägungen. Aus Sicht des Wohlstandsmaximierers war das Risiko, amerikanischen Behörden durch die Hinterlegung von Zweitschlüsseln potenziell Zugriff auf deutsche Wirtschaftsgeheimnisse einzuräumen, nicht hinnehmbar. Auch mit Blick auf die privaten Kommunikationsinhalte deutscher BürgerInnen wurde dies kritisch gesehen. Zu diesen Bedenken kam noch eine partielle Abhängigkeit der eigenen Beschützer-Rolle hinzu. Da das deutsche Militär amerikanische Software verwendete, wurde die Fähigkeit zum Schutz eigener, sensibler Kommunikation unterminiert. Auf internationaler Ebene wirkten so alle drei Rollen synergetisch auf eine Kontestation der amerikanischen Bemühungen hin und ermöglichten eine liberale Verschlüsselungspolitik.

Die deutsche Skepsis gegenüber einer Regulierung von Verschlüsselung war aber nicht nur durch Vorbehalte gegen einen wachsenden Einfluss der USA geprägt. Kritik wurde auch gegen eine deutsche Aushöhlung kryptographischer Verfahren vorgebracht. Diese Position wurde sowohl innerhalb der Regierungskoali-

tion als auch von Akteuren der Zivilgesellschaft vertreten. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) konstatierte bspw. eine Regulation von Kryptographie stelle »bisherige Grundrechtsprinzipien auf den Kopf«, da auch beim Verfassen von Briefen Chiffren zulässig seien und die Aufgabe der Dekryptierung allein bei den Behörden liege (FIfF, 1997). Die Forderung des Innenministers, die Schlüssel verfügbar zu hinterlegen käme, so der Vorwurf, der Aufforderung gleich, nur noch leicht lesbare Standardbriefe zu verfassen: derartiges habe »in Deutschland noch keine Diktatur gefordert« (ebd.).

Auch innerhalb der Koalition und zwischen den Ressorts waren die Vorschläge des Innenministers nicht unumstritten. Sowohl der Koalitionspartner FDP als auch der Bundeswirtschaftsminister lehnten die Regulation von Verschlüsselung ab. Daher wurden 1997 auch keine Maßnahmen zur Restriktion von Verschlüsselung in das neue Informations- und Telekommunikationsdienste-Gesetz (IuKDG) integriert. Der FDP-Justizminister Schmidt-Jorzig brachte bei der ersten Lesung des neuen IuKDG gegen eine umfassende Kryptoregulation nicht nur wirtschaftliche Argumente vor, sondern betonte ferner die Bedeutung der Verschlüsselung für die Wahrung der Bürgerrechte denn »[…] sie schafft die technische Voraussetzung dafür, daß die Idee des Postgeheimnisses in die Zukunft übertragen werden kann.« (Deutscher Bundestag, 1997b, S. 15395). Ferner verband er die Verschlüsselungsthematik mit dem freien Informationsaustausch im Internet. In diesem Zusammenhang verwies er auf die historischen Erfahrungen der Bundesrepublik:

> »Die Informationsfreiheit war schon immer eine Schutzimpfung gegen die Diktatur. Nicht umsonst – ich will es so drastisch sagen, damit wir die Wichtigkeit dieser Dimension voll im Blick haben – hatte schon Goebbels das Hören von Feindsendern unter Strafe gestellt. Wieviel machtloser sind Diktaturen, wenn man und seit man per Mausklick alle Nachrichten, alle Informationen weltweit empfangen kann?« (Ebd., S. 15395)

Auch die 1996 unter Führung des Innenministeriums (BMI) gegründete Task Force Kryptopolitik, gelangte zu der Einschätzung, dass Verschlüsselungsprodukte frei verfügbar sein sollten (Deutscher Bundestag, 1997a, S. 10). Die innenpolitische Krypto-Debattte wurde schließlich im Jahr 1999 beigelegt, als das Wirtschafts- und Innenministerium die »Eckpunkte der deutschen Kryptopolitik« vorlegten und damit die Position der Regierung definierten. Mit diesem Dokument legte die Regierung fest, dass sie nicht beabsichtige, »die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken« (Bundesregierung, 2001, S. 11). Begründet wurde dies mit der Bedeutung von Verschlüsselung für den »Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen« (ebd., S. 11). Diese Entscheidung wurde sowohl von der Wirtschaft als auch von BürgerrechtsaktivistInnen positiv aufgenommen. Im Rahmen der 58. Datenschutzkonferenz

begrüßten bspw. die Datenschutzbeauftragten des Bundes und der Länder ausdrücklich die Entscheidung der Bundesregierung und betonten dass der Einsatz von Kryptographie ein wesentlicher Bestandteil zum Schutz personenbezogener Daten sei (Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit, 1999).

Die Bundesregierung vereinbarte aber, die Situation zwei Jahre später erneut zu debattieren und zu evaluieren, ob die Strafermittlung durch Verschlüsselung maßgeblich eingeschränkt werde. Hierzu wurde der Arbeitskreis Innere Sicherheit und Verschlüsselung gegründet. Beteiligt waren das BMI, das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV), der Generalbundesanwalt, das Zollkriminalamt sowie das BSI (Bundesregierung, 2001, S. 3). Der Arbeitskreis kam 2001 zu dem Ergebnis, dass die Arbeit der Ermittlungs- und Sicherheitsbehörden durch den Einsatz von Verschlüsselung »noch nicht (nachhaltig) beeinträchtigt« sei (ebd., S. 7). Die Eckpunkte der deutschen Kryptopolitik blieben daher unangetastet. In der Folge wurde zwar immer wieder über die Beschränkung von Kryptographie bzw. über die Zugriffsmöglichkeiten staatlicher Stellen debattiert (insbesondere nach Terroranschlägen), die Regierung erklärte aber zuletzt 2015, dass die Eckpunkte nach wie vor gültig seien (Deutscher Bundestag, 2015c, S. 4).

Innenpolitisch wurde die Bundesregierung immer wieder mit Verweis auf ihre Rolle als Garant liberaler Grundrechte herausgefordert. Stimmen, die auf die besondere Funktion von Verschlüsselung in einer demokratischen Gesellschaft hinwiesen, kamen gleichermaßen aus Zivilgesellschaft, Parlament und Teilen der Regierung. Diese Bestrebungen wirkten besonders beschränkend auf die Beschützer-Rolle bzw. eine Unterminierung von Verschlüsselung, da sie mit den negativen historischen Selbstbildern der Bundesrepublik verknüpft wurden. Durch diese domestischen Kontestationsprozesse wurde folglich ebenfalls eine liberale Verschlüsselungspolitik ermöglicht.

4.1.3 Internationalisierung: Strafrechtliche Harmonisierung

Das Internet ermöglichte es Kriminellen aber nicht nur verschlüsselt zu kommunizieren, sondern es brachte auch die Möglichkeit, problemlos über Landesgrenzen hinweg zu operieren. Hierdurch entstanden für die Strafverfolgung nicht nur technische Probleme der Attribution von Angriffen, sondern auch Fragen der internationalen Kooperation. Hinzu kam, dass die Referenz zum jugendlichen Hacker in der Mitte der 1990er Jahre zunehmend kritisch gesehen wurde. Der deutsche Innenminister Kanther betonte, dass zu diesem Zeitpunkt die meisten Cyberangriffe kommerziell motiviert waren:

> »Immer noch geistert durch die Diskussion das Bild vom jungen oder gar jugendlichen Computerfreak, der – im Grunde spielerisch veranlagt – einfach Spaß am Tüfteln hat: Codeknacken als moderne Version von Superhirn. Doch das Idyll vom jugendlichen Übermut im IT-Zeitalter ist nüchtern betrachtet eine Illusion. Längst stehen wirtschaftliche Motive beim kriminellen IT-Einsatz im Vordergrund.« (Bundesregierung, 1996, S. 4)

Mit diesem veränderten AngreiferInnentyp nahm auch die Notwendigkeit der internationalen Kooperation zu, da die Schäden durch Cyberangriffe wuchsen. Die internationale Kooperation zur Bekämpfung von Cyberkriminalität wurde in verschiedenen institutionellen Kontexten seit Beginn der 1990er Jahre debattiert bspw. innerhalb der UN (1990). Im Rahmen des Europarates wurde mit der Convention on Cybercrime das erste und bislang einzige verbindliche internationale Regelwerk zur Bekämpfung von Cyberkriminalität etabliert. Das im November 2001 verabschiedete Übereinkommen sieht eine Harmonisierung des Strafrechts, internationale Kooperation (etwa bei der Rechtshilfe) sowie eine Angleichung der Ermittlungsbefugnisse aller Vertragsparteien vor (Council of Europe, 2001a). Die deutsche Regierung hat die Konvention unmittelbar nach der Öffnung gezeichnet, ratifiziert wurde sie im März 2009 (Council of Europe, 2019). Der zusammen mit dem Übereinkommen veröffentlichte Explanatory Report skizziert die problematisch gewordene Situation so:

> »Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments.« (Council of Europe, 2001b, S. 2)

Vor diesem Hintergrund wurde seit 1996 an einem Übereinkommen gearbeitet. Mit der Einsicht, dass es eines internationalen Abkommens zur wirksamen Bekämpfung der Internetkriminalität bedürfe, ist auch die Einschätzung verbunden, dass es letztlich doch die Nationalstaaten sind, die diesen neuen Raum entsprechend ihrer Territorialität ordnen sollen.

Die Bundesregierung hat die Bestrebungen zur internationalen Harmonisierung der gesetzlichen Regelungen sowohl im Rahmen des Europarates als auch innerhalb der Europäischen Union stets nachdrücklich unterstützt. Sie vertrat damit die auch international verbreitete Auffassung, dass durch den globalen Handlungsraum Bedarf bestand, die nationalen Beschützer-Rollen anzugleichen, um zu gewährleisten, dass Straftaten überhaupt als solche erkannt und verfolgt werden konnten. Konkret sah die Regierung in neuen Regelungen zur internationalen Bekämpfung von Computerkriminalität die Möglichkeit, dem Trend entgegenzuwirken, »im Internet die unterschiedlichen nationalen Rechtsnormen aus-

zunutzen, um sich der Strafermittlung und/oder -verfolgung zu entziehen bzw. diese zu behindern« (Deutscher Bundestag, 2001, S. 3). Dass ein bestimmtes Verhalten in einem Staat legal, in einem anderen aber illegal war, stellte in einem entgrenzten Raum ein neues Problem dar.

Um dem zu begegnen, definierte die Convention on Cybercrime in den Artikeln 2 bis 13 verschiedene zu harmonisierende Straftatbestände. Mit dem Rahmenbeschluss 2005/222/JI folgte die EU weitgehend der Konvention des Europarates und etablierte die Straftatbestände innerhalb der Union. In dem Dokument nimmt der Rat der Europäischen Union direkt Bezug auf »die von internationalen Organisationen und insbesondere vom Europarat geleisteten Arbeiten zur Angleichung des Strafrechts« (EU, 2005, S. 67). Im Gegensatz zur Convention on Cybercrime enthielt der Rahmenbeschluss aber keine Vorgaben für die Befugnisse der Ermittlungsbehörden (ebd.).[2] Mit diesen Regelungen wurde festgelegt, welche neuen Verhaltensweisen durch die Exekutiven sanktioniert werden sollten.

Viele der in diesen Dokumenten beschriebenen Delikte waren in Deutschland bereits durch das 2. WiKG strafbar geworden. Daher folgte aus diesen Bestimmungen in Deutschland nur begrenzter Änderungsbedarf. Die strafrechtlichen Anpassungen wurden 2003 bzw. 2007 mit dem 35. und dem 41. Strafrechtsänderungsgesetz umgesetzt (Bundesgesetzblatt, 2003, 2007). Innenpolitisch wurde der neu geschaffene § 202c besonders kritisch diskutiert. Der als Hackerparagraph bekanntgewordene Abschnitt stellt auch die Erstellung sowie die Verbreitung von Hackertools unter Strafe. Aus Sicht der Wirtschaft kriminalisierte die Regierung damit auch die Tätigkeiten von SicherheitsforscherInnen, die zwangsläufig mit Software zur Identifikation von Schwachstellen arbeiten müssten. Die Kritik wurde dabei bspw. vom Branchenverband BITKOM und SAP vorgebracht (Deutscher Bundestag, 2007b, S. 10290f.). Der Chaos Computer Club (CCC) sah durch den verschärften Straftatbestand gar »den IT-Standort Deutschland« gefährdet (CCC, 2008). Der Rechtsausschuss des Bundestages teilte diese Einschätzungen allerdings nicht (Deutscher Bundestag, 2007a). Eine Klage vor dem Bundesverfassungsgericht (BverfG) blieb ebenfalls erfolglos (Bundesverfassungsgericht, 2009).

Außerdem wurde durch die Änderungen der direkte wirtschaftliche Bezug in § 303b gestrichen. Diese Neuregelung zeigt, dass durch die neuen potenziellen Angreifer in Verbindung mit der fortschreitenden Vernetzung (insbesondere kritischer Infrastrukturen) eine neue Gefahrensituation entstanden war. Daher wurde für § 303b (Computersabotage) eine Höchststrafe von zehn Jahren Freiheitsstrafe vorgesehen, »falls durch einen Angriff die Versorgung der Bevölkerung mit

2 Der Rahmenbeschluss wurde 2013 durch die Richtlinie 2013/40/EU ersetzt. Auch hier wird direkt auf die Convention on Cybercrime rekurriert und das Ziel verfolgt, dass alle EU-Mitgliedsstaaten das Abkommen ratifizieren (EU, 2013, S. 9).

lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt« würde. Hier zeigt sich deutlich die national wie international gestiegene Gefahreneinschätzung, die eine Erweiterung der Sanktionsmittel der Beschützer ermöglichte. Im Zuge der Harmonisierung wurde ferner der neue Tatbestand Abfangen von Daten geschaffen (§ 202b). Im Zuge der Anpassungen fiel weiterhin das sogenannte Hacker-Privileg aus § 202a StGB, das das bloße Eindringen in Computersysteme noch nicht unter Strafe stellte. Auch dies wurde durch die neuen Charakteristiken der AngreiferInnen ermöglicht.

Neben Vorgaben zur Gestaltung des Strafrechts und zur internationalen Kooperation enthält die Convention on Cybercrime auch Regelungen zu Ermittlungsbefugnissen der Sicherheitsbehörden. In den Artikeln 14 bis 21 beschreibt das Übereinkommen die Kompetenzen, über die Staaten bzw. die Ermittlungsbehörden der Staaten verfügen sollten, um Computerkriminalität effektiv verfolgen zu können. Von besonderer Bedeutung für die deutsche Politik sind hier die Artikel 19 und 21. Artikel 19(1) schreibt den Vertragsparteien vor, die Ermittlungsbehörden in die Lage zu versetzen:

> »a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können, in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zunehmen.« (Bundesgesetzblatt, 2008a, S. 1256)[3]

Artikel 21 bezieht sich auf den direkten Mitschnitt gegenwärtiger Kommunikation, die Staaten müssen Sicherheitsbehörden die rechtlichen Möglichkeiten einräumen,

> »inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und b) einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten, i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.« (Ebd., S. 1258)

3 Im Folgenden wird auf die deutsche Übersetzung des Textes zurückgegriffen, die am 10. November 2008 im Bundesgesetzblatt veröffentlicht wurde.

Mit diesen Vorschriften verständigten sich die Exekutiven auf Maßnahmen, die sie zur Erfüllung ihrer Schutzfunktionen für notwendig und angemessen hielten.[4] Es war aber in Deutschland bereits abzusehen, dass es gegen einige Bestimmungen substanziell Widerstand geben würde (heise.de, 2001a,b). Auch juristische Analysen bezweifelten, dass bspw. Maßnahmen nach Artikel 19 der Konvention durch § 102 der deutschen Strafprozessordnung (StPO) gedeckt waren (Spannbrucker, 2004, S. 188f.).

In dieser Phase wurde die Beschützer-Rolle und damit verbunden die Sanktionspotenziale deutlich ausgebaut. Diese Expansion der Kompetenzen wurde maßgeblich durch eine doppelte Veränderung der Rollenreferenz ermöglicht. Einerseits verschob sich der Fokus des Schutzgutes weiter von der Wirtschaft, ein Trend, der bereits in der Frühphase begonnen hatte und sich hier fortsetzte. Da IT zunehmend zu einer zentralen Infrastruktur wurde, löste sich die Beschützer-Rolle etwas vom wirtschaftlichen Schutzgut und fokussierte sich auf die kritischen Infrastrukturen. Mit dieser Verschiebung der Referenz (Schutz für wen?) ging eine neue Gefahreneinschätzung einher, da es nun auch darum ging, die Gesellschaft vor potenziellen physischen Folgen von Cyberangriffen zu schützen. Dies wurde auch durch die zweite Verschiebung der Referenz (Schutz vor wem?) noch deutlicher. Mit Blick auf die AngreiferInnen ging es nun nicht mehr um FreizeithackerInnen, sondern um zunehmend professionalisierte Kriminelle. Das Zusammenspiel aus verändertem Schutzgut (kritische Infrastrukturen) und neuen AngreiferInnen ermöglichte so einen Ausbau der Beschützer-Rolle. Es kam zwar zu Kontestationen mit Verweis auf wirtschaftliche Implikationen, bspw. für die IT-Sicherheitsforschung. Diese blieben vor dem Hintergrund der neuen Lageeinschätzung allerdings folgenlos.

Auf internationaler Ebene war die ausgedehnte Beschützer-Rolle anschlussfähig, da auch andere Staaten ähnliche Politiken verfolgten. Eine Harmonisierung strafrechtlicher Regulationen wurde damit durch kompatible Beschützer-Rollen ermöglicht. Eine weitgehende Kooperation erwuchs hieraus allerdings nicht. Dies lag unter anderem an folgenden domestischen Kontestationsprozessen in der Bundesrepublik, die es der Regierung bislang schwer gemacht haben, die eigene Beschützer-Rolle stabil zu etablieren sowie an der Rolle als Garant liberaler Grundrechte, die eine Delegation oder Teilung der Beschützer-Rolle schwierig macht.

4 Im Text der Konvention wird wiederholt darauf hingewiesen, dass das »Gleichgewicht gewahrt werden muss zwischen den Interessen der Strafverfolgung und der Achtung der grundlegenden Menschenrechte« (Bundesgesetzblatt, 2008a, S. 1244).

4.1.4 Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle

Besonders intensiv wurde die domestische Auseinandersetzung in der Bundesrepublik als die Regierung damit begann, die Beschützer-Rolle mit offensiven Fähigkeiten zum (physischen) Schutz vor Gefahren aus der »analogen Welt« auszustatten. Dieses Vorgehen führte zu massiven Kontestationsprozessen, da dies von der parlamentarischen Opposition und VertreterInnen der Zivilgesellschaft als unangemessener Ausbau der Rolle gesehen wurde.

Auch wenn Hintertüren in Verschlüsselung international wie domestisch durch die Regierung abgelehnt wurden, etablierte sie innenpolitisch dennoch für Strafverfolgungsbehörden die Möglichkeit, Internetkommunikation abzuhören. Damit hat sie ihre Beschützer-Rolle deutlich erweitert. Sie folgte damit später auch dem internationalen Konsens der Convention on Cybercrime. Die Regierung hat dazu eine Reihe von Maßnahmen ergriffen, die innenpolitisch besonders durch die Wirtschaft und Bürgerrechtsbewegungen herausgefordert wurden. Im Mai 1995 verabschiedete das Bundeskabinett bspw. die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) (Bundesgesetzblatt, 1995).

Da der Staat selbst die sicherheitsrelevanten Kommunikationsmittel nicht mehr betrieb, sollten die Anbieter von Kommunikationsdienstleistungen bereits vor Markteintritt dazu verpflichtet werden, technische Möglichkeiten zu schaffen, gesetzlichen Verpflichtungen zur Überwachung nachzukommen, sodass keine Lücken entstünden (Bundesregierung, 1996, S. 5). Denn »die Belange von Polizei und Justiz, und das heißt unsere eigenen Sicherheitsinteressen [dürften; Anm. d. Verf.], nicht außer acht bleiben« (ebd., S. 6f.). Die neuen Zugriffsmöglichkeiten wurden von Innenminister Kanther mit der raschen technischen Entwicklung und der Privatisierung des Marktes begründet. Die FÜV wurde 2002 durch die Telekommunikations-Überwachungsverordnung (TKÜV) ersetzt, die auch konkrete Bestimmungen zum Umgang mit verschlüsselter Kommunikation enthielt. In §8(3) der TKÜV legte die Regierung fest, dass Anbieter, sofern sie die Kommunikation selbst durch Verschlüsselung schützten, diese vor dem Erstellen der Überwachwungskopie entfernen mussten (Bundesgesetzblatt, 2002). Auf Grundlage des G-10-Gesetzes, der §§ 100a, 100b der StPO und §§ 39 bis 43 des Außenwirtschaftsgesetzes regelte die TKÜV die technische Überwachung im Fernmeldeverkehr (ebd.). Sie erlaubte damit dem Verfassungsschutz, den Bundes- sowie Landespolizeien, dem Zoll und dem BND Maßnahmen zur Telekommunikationsüberwachung (TKÜ). Die Verordnungen wurden zwar von verschiedenen Seiten kritisiert, blieben letztlich aber in Kraft. Begründet wurde diese Reform der FÜV durch den Verweis auf die Gefahr terroristischer Angriffe, die im Netz vorbereitet werden könnten.

> »Viele der schädlichen Programme und gezielten Angriffe gehen zunehmend auf das Konto organisierter Kriminalität und terroristischer Angreifer. Das Hauptmotiv ist nicht mehr wie bei den so genannten Script-Kiddies der Wunsch, an Bekanntheit zu gewinnen, sondern es geht darum, aus den Angriffen finanziellen Nutzen zu ziehen oder volkswirtschaftlichen Schaden anzurichten.« (Bundesministerium des Innern, 2005, S. 4)

Das Ausmaß der innenpolitischen Kontestation erreichte 2006 einen Höhepunkt, als sich eine intensive Debatte um die konkrete Nutzung von digitalen Ermittlungsmethoden entfaltete. Um mit der technischen Entwicklung schrittzuhalten, hatte die Bundesregierung den Strafverfolgungsbehörden zwei (Software-)Instrumente zur Verfügung gestellt: die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung. Beide Maßnahmen sollten dazu beitragen, dass Ermittlungen nicht durch technische Hürden, wie Verschlüsselung, unmöglich gemacht werden. Die Maßnahmen unterscheiden sich in ihrer Eingriffstiefe in die Grundrechte deutlich. Die Quellen-TKÜ zielt darauf ab, Kommunikation vor der Verschlüsselung abzufangen und diese ohne eine Schwächung von Verschlüsselung abhörbar zu machen. Sie ist damit, die auf dem Endgerät der Betroffenen softwaregestützte Fortsetzung der TKÜ. Die Online-Durchsuchung ermöglicht den Behörden dagegen ein Gerät komplett zu durchsuchen (Brodowski und Freiling, 2011, S. 143-152). Beides sind Kompetenzen, die in der Convention on Cybercrime angelegt sind (Artikel 19 bzw. 21). Auch wenn den Exekutiven viel Spielraum bei deren Implementierung bleibt. Die Bundesregierung rechtfertigte diese Maßnahmen im »Programm zur Stärkung der Inneren Sicherheit« und konstatierte, dass es für Ermittlungsbehörden in Zeiten der Digitalisierung notwendig sei, Endgeräte auch ohne direkten physischen Zugriff überwachen zu können (Deutscher Bundestag, 2006).

Unter Verweis auf die Bürgerrechte wurde die exekutive Beschützer-Rolle in der Folge substanziell herausgefordert. Im Februar 2006 ordnete ein Ermittlungsrichter beim Bundesgerichtshof an, dass eine Software zur Informationsgewinnung eingesetzt werden dürfe. Konkret ging es um ein Verfahren des Generalbundesanwaltes, das im Rahmen des Verdachts auf die Gründung einer terroristischen Vereinigung geführt wurde. Der Ermittlungsrichter erlaubte den Behörden unter Verweis auf § 102 der StPO den Einsatz eines digitalen Ermittlungswerkzeugs.

> »Zur verdeckten Ausführung dieser Maßnahme wird den Ermittlungsbehörden gestattet, ein hierfür konzipiertes Computerprogramm von außen auf dem Computer des Beschuldigten zu installieren, um die auf den Speichermedien des Computers abgelegten Daten zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen.« (Bundesgerichtshof, 2006b)

Diese Einschätzung wurde allerdings durch einen anderen Ermittlungsrichter infrage gestellt. Dieser entschied im Dezember des gleichen Jahres, dass die Online-Durchsuchung nicht durch die Regelungen der StPO gedeckt seien. § 102 StPO biete nicht den ausreichenden Rahmen, diese Maßnahme zu rechtfertigen. Auch einen weiten Analogieschluss, um analoge Ermittlungsmethoden auf die digitale Sphäre anwenden zu können, lehnte der Ermittlungsrichter ab. Er sei zu weitreichend als, dass dies ohne eigene gesetzliche Regelung möglich wäre (Bundesgerichtshof, 2006a).

Der Generalbundesanwalt legte gegen diesen Beschluss Einspruch ein. Im Januar 2007 entschied der BGH aber: »Die ›verdeckte Online-Durchsuchung‹ ist mangels einer Ermächtigungsgrundlage unzulässig. Sie kann insbesondere nicht auf § 102 StPO gestützt werden« (Bundesgerichtshof, 2007). Diese Einschätzung barg einige Risiken für die Bundesregierung, denn angeblich hatte der Bundesinnenminister dem Bundesamt für Verfassungsschutz schon 2005 per Dienstanweisung erlaubt, verdeckt Computer nach Informationen zu durchsuchen. Dem Urteil des BGH folgte noch im gleichen Jahr ein Gutachten des Wissenschaftlichen Dienstes des Bundestags, das die Rechtmäßigkeit der Online-Durchsuchung ebenfalls kritisch beurteilte (Wissenschaftlicher Dienst des Bundestages, 2007). Trotz dieses Urteils und der Einschätzung zahlreicher ExpertInnen, versuchte die nordrhein-westfälische Landesregierung dem Landesverfassungsschutz, die Online-Durchsuchung durch ein neues Gesetz zu ermöglichen. Dies führte zu einer Klage vor dem Bundesverfassungsgericht. In einem wegweisenden Urteil am 27. Februar 2008 definierte das BverfG das »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« (Bundesverfassungsgericht, 2008). In diesem Urteilt entschied das Gericht:

> »Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.[5] […] Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.« (Ebd.)

5 »Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.«

Die entsprechenden Regelungen des nordrhein-westfälischen Verfassungsschutzgesetzes waren damit ungültig und auch der Praxis der Bundesregierung war die Rechtmäßigkeit abgesprochen worden. Diese Entscheidung wurde sowohl von Bürgerrechtsbewegungen als auch der Internetwirtschaft begrüßt. Während Wirtschaftsvertreter die Bedeutung des Urteils für das Vertrauen der NutzerInnen in Onlinedienstleistungen hervorhoben, betonten die Bürgerrechtsbewegungen die Wirkung der Entscheidung auf die Wahrung der Grundrechte im digitalen Zeitalter (Spiegel, 2008).

Die Regierung verabschiedete noch im gleichen Jahr des BverfG-Urteils ein neues Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, das dem BKA mit § 20k die Online-Durchsuchung unter Richtervorbehalt ermöglichte (Bundesgesetzblatt, 2008b). Das Gesetz war zuvor nicht nur von der Opposition und Bürgerrechtsbewegungen, sondern auch von der SPD abgelehnt worden. Die SPD hatte im Gesetzgebungsprozess aber noch einige Anpassungen am Entwurf erreicht, die ihre mehrheitliche Zustimmung letztlich sicherte. Die Kritik aus der Zivilgesellschaft war aber ungebrochen. Die Regierung rechtfertigte die neuen Befugnisse bspw. mit den Erfahrungen der sogenannten Sauerland-Gruppe, die Anschläge in Deutschland geplant hatte und dabei auch Verschlüsselung zur Sicherung von Informationen nutzte. Die Online-Durchsuchung sei daher »bei der Terrorbekämpfung unverzichtbar« (Deutscher Bundestag, 2008, S. 19833).

Außerdem wurde wiederholt darauf verwiesen, dass das Gesetz dem Urteil des BVerfG Rechnung trage. Das neue Gesetz entspreche »Punkt für Punkt den Vorgaben, die uns Karlsruhe gemacht hat« (ebd., S. 19834). Die Opposition kritisierte das Gesetz zum einen mit Blick auf die Kompetenzausweitung im Bereich der Gefahrenabwehr. Das BKA erhalte Kompetenzen, die bisher in den Landeskriminalämtern angesiedelt waren, so entstehe »ein deutsches FBI« (ebd., S. 19835). Das Gesetz schwäche das Trennungsgebot zwischen Polizeien und Geheimdiensten und ebne den Weg in den Überwachungsstaat (ebd., S. 19838). Auch Bürgerrechtsbewegungen kritisierten das Gesetz mit ähnlichen Argumenten scharf. Weiterhin kritisierten sie, dass das neue Gesetz den Schutz besonders sensibler BerufsträgerInnen nicht ausreichend berücksichtige. Dies führte dazu, dass unter anderem von zwei FDP-Politikern, zwei Journalisten, dem Präsidenten der Bundesärztekammer und einem Psychologen beim BVerfG Verfassungsbeschwerde eingereicht wurde (Zeit, 2009).

Im April 2016 entschied das BVerfG, dass Teile des BKA-Gesetzes verfassungswidrig seien. Prinzipiell stellte das Gericht zwar fest:

> »Die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen ([…] Online-Durchsuchungen, Telekommunikationsüberwachungen, […]) ist zur Abwehr von Gefahren des internationalen

> Terrorismus im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar.« (Bundesverfassungsgericht, 2016b)

Allerdings waren die Befugnisse nicht spezifisch genug gestaltet und die juristische Kontrolle nicht ausreichend gewährleistet, so dass das Gericht die betreffenden Regelungen (darunter § 20k zur Online-Durchsuchung) für grundgesetzwidrig erklärte, aber der Regierung bis zum 30. Juni 2018 Zeit ließ, eine neue Regelung zu finden. Im Juni 2017 trat bereits das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes in Kraft (Bundesgesetzblatt, 2017b). Auch diese Neufassung wurde unter anderem aufgrund der Regelungen zur Online-Durchsuchung kritisiert. Der Deutsche Anwaltsverein konstatierte sogar (bereits vor der Verabschiedung des Entwurfs), der neue § 49, der die Online-Durchsuchung regelte, falle hinter den alten § 20k zurück, da nun eine Durchsuchung schon möglich wurde, wenn »bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt« (Deutscher Anwaltverein, 2017a, S. 5).

Für eine weitere Welle der Kontestation sorgte die Verabschiedung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens im Sommer 2017. Mit diesem Gesetz hatte die Regierung den Einsatz von Quellen-TKÜ und Onlinedurchsuchung nochmals ausgeweitet (Bundesgesetzblatt, 2017a). Mit § 100b etablierte die Regierung die Online-Durchsuchung in der StPO. Damit rückte die Maßnahme aus dem Bereich der Gefahrenabwehr (BKA-Gesetz) in die Strafverfolgung (Roggan, 2018). Die Regierung argumentierte, dass diese neuen Fähigkeiten zur Gewährleistung der Schutzfunktion essenziell seien. Besonders mit Blick auf Ende-zu-Ende verschlüsselte Messenger entstünden vermehrt Hürden bei der Strafverfolgung:

> »Traf man sich vor 20 Jahren noch in einer Wohnung, um kriminelle oder terroristische Aktivitäten zu planen, kann man sich heutzutage in einem Chatroom treffen. Der Gesetzgeber muss hierauf eine Antwort finden. Strafverfolger dürfen Kriminellen nicht hinterherhinken. […] Besonders schwierig wird es für die Ermittler, wenn es um Datenmaterial geht, das durch sogenannte Messengerdienste ausgetauscht wurde. Wenn Behörden keinen Zugriff auf diese Daten haben, entstehen in der Folge Räume, in denen Strafverfolgung unmöglich ist.« (Deutscher Bundestag, 2017d, S. 24586)[6]

6 Immer wieder wurde in diesem Kontext auf die Nutzung von (Ende-zu-Ende-verschlüsselten) Messengerdiensten (bspw. WhatsApp oder Signal) verwiesen, die keine Telekommunikationsdienstleister im Sinne des Telekommunikationsgesetzes sind, sondern Telemedien. Diese Telemedien unterliegen daher auch nicht den entsprechenden Anforderungen und sind somit nicht verpflichtet TKÜ-Maßnahmen der TKÜV umzusetzen. Sie wären bei einer Ende-

Die neuen Regeln waren aus Sicht der Regierung nur eine Anpassung an die neuen Kommunikationsmöglichkeiten (ebd., S. 24588, ebenso 24592). Es könne »nicht sein, dass nur die eine Seite, dass nur Terroristen und Kriminelle vom technischen Fortschritt profitieren« (ebd., S. 24591). Außerdem folge die Regierung mit dem Gesetz den rechtsstaatlichen Grundsätzen (ebd., S. 24591).

Für heftigen Widerspruch gegen die neuen Regeln sorgte einerseits, dass diese erst im Ausschuss und damit weitgehend ohne öffentliche Diskussion in die Gesetzesvorlage aufgenommen wurden, die dadurch einen völlig neuen Schwerpunkt erhalten habe. Diese Kritik wurde auch von Teilen der Regierung eingeräumt (ebd., S. 24585). Andererseits wiesen KritikerInnen auf den aus ihrer Sicht extensiven Strafenkatalog hin, der mit den Maßnahmen verfolgt werden sollte. Auch für die besonders intrusive Online-Durchsuchung waren aus ihrer Sicht zu viele Straftaten vorgesehen (Deutscher Anwaltverein, 2017b; heise.de, 2017b). Die Bundesbeauftragte für den Datenschutz sah in den Plänen der Regierung einen »klaren Verfassungsverstoß« und wies ebenfalls darauf hin, dass der 74 Paragraphen umfassende Katalog, der durch die Online-Durchsuchung verfolgt werden solle, deutlich zu groß sei (Bundesbeauftragte für den Datenschutz, 2017). Netzpolitik.org sah in dem Gesetz das »krasseste Überwachungsgesetz der Legislaturperiode« (Netzpolitik.org, 2017). Der Geschäftsführer des Branchenverbands BITKOM warnte davor, durch übermäßige Eingriffe in die IT-Sicherheit, das Vertrauen der NutzerInnen in die Dienste zu untergraben (heise.de, 2017a). Der CCC sah in den Vorschlägen eine Gefahr für die Innere Sicherheit, da sowohl für die Quellen-TKÜ als auch für die Online-Durchsuchung Sicherheitslücken ausgenutzt werden müssten, die ggf. auch von Dritten gefunden werden könnten (CCC, 2017).

Auch im Bundestag stießen die Pläne der Regierung auf deutliche Kritik. Die Opposition sah in den neuen Befugnissen, wie auch der CCC, eine Gefahr für die IT-Sicherheit. Das Geheimhalten von Sicherheitslücken berge immer das Risiko, dass Dritte diese nutzten. Außerdem seien die Maßnahmen »noch weitgehender als der große Lauschangriff aus den 90ern« und ein unverhältnismäßiger Eingriff in die Grundrechte (Deutscher Bundestag, 2017d, S. 24586f.). Der Umfang des Strafenkatalogs wurde ebenfalls von verschiedenen Fraktionen als zu umfassend kritisiert (ebd., S. 24587, ebenso 24589).

All diese Einwände führten erneut zu Beschwerden vor dem BVerfG. AktivistInnen von Digitalcourage e.V., die FDP, die Gesellschaft für Freiheitsrechte und die Humanistische Union reichten 2018 ihre Klagen ein. Sie argumentierten, das Gesetz greife unverhältnismäßig und zu unbestimmt in die intimsten Lebensbereiche der BürgerInnen ein und untergrabe die Bürgerrechte (Gesellschaft für Freiheitsrechte, 2018; ZDF, 2018).

---

zu-Ende-Verschlüsselung aber ohnehin unbrauchbar. Der Einsatz staatlicher Spähsoftware wurde daher als angemessene Reaktion vorgeschlagen.

Mit den Bestrebungen, die Beschützer-Rolle entsprechend der neuen Gefahreneinschätzung aus professionalisierten AngreiferInnen und besonders sensiblen Schutzgütern offensiv auszubauen, löste die Bundesregierung eine anhaltende Welle domestischer Kontestationsprozesse aus. Diese stützten sich maßgeblich auf die Rolle als Garant liberaler Grundrechte, auf die die Bundesregierung wiederholt hingewiesen wurde. Maßnahmen wie die Online-Durchsuchung oder die Quellen-TKÜ wurden sowohl von der Zivilgesellschaft als auch der parlamentarischen Opposition scharf kritisiert. Durch Klagen vor dem Bundesverfassungsgericht wurde die Regierung gezwungen, beim Einsatz dieser Maßnahmen zurückhaltender zu sein und sie besser zu kontrollieren. Das Zusammenspiel der unterschiedlichen GegenrollenträgerInnen ermöglichte es, dass die Regierung noch immer keine endgültig stabile Beschützer-Rolle etablieren konnte. Die Kontestation war so folgenreich, da sie sich auf Urteile des Verfassungsgerichts stützen konnten und die Regierung damit autoritativ zur Ausbalancierung der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte veranlassen konnte. Die Kontestationen gegen eine Erweiterung der Beschützer-Rolle waren am Ende des Untersuchungszeitraumes noch im Gange. Eine stabile Rollenbeziehung, die die Schutzfunktion und die Wahrung der Grundrechte ins Gleichgewicht bringt, war noch nicht gefunden.

Neben diesen Kontestationen mit Bezug zur Grundrechtskonformität der Online-Durchsuchung und der Quellen-TKÜ wurde in diesem Zeitraum parallel auch deutlich, dass die Bundesregierung technisch kaum in der Lage war, ihre Beschützer-Rolle alleine wahrzunehmen. Ausgangspunkt dieser Entwicklung war die öffentliche Diskussion um die Software zur Quellen-TKÜ. Der Chaos Computer Club deckte in einer technischen Analyse der Software auf, dass diese die gesetzlichen Maßgaben nicht erfüllte. Die Funktionalität der Software, die vermutlich von bayerischen ErmittlerInnen verwendet wurde, war nicht nur auf das Abfangen von Kommunikation vor der Verschlüsselung beschränkt, sondern ermöglichte die umfassendere Überwachung des infizierten Gerätes (CCC, 2011). Die Bundesregierung musste in diesem Kontext eingestehen, dass sie den Quellcode, der auf Bundesebene verwendeten Software, nicht einsehen konnte, da dieser als Geschäftsgeheimnis bewertet wurde. Die vorgeschriebene Funktionalität konnte daher nur durch Anwendungstests überprüft werden (Deutscher Bundestag, 2011b, S. 5). Die Software wurde durch die Behörden bei der Firma DigiTask erworben und sorgte in der Folge für massive Kritik an der Bundesregierung (Deutscher Bundestag, 2012, S. 4). Die technische Überprüfung durch den CCC hatte nämlich auch ergeben, dass die Software Sicherheitslücken aufwies, die potenziell von Dritten ausnutzbar waren. Damit konnte der Einsatz zumindest theoretisch auch Kriminellen oder anderen den Zugriff auf die infizierten Rechner erlauben. Der Beschützer hätte also auch das Tor für Unbefugte geöffnet. Zudem zeigte die Analyse, dass die Kommunikation

mit dem Programm über Server in den USA verlief. Die Opposition sah daher die Möglichkeit, dass auch amerikanische Behörden evtl. mitlesen konnten. In der Folge wurde diese Software nicht mehr genutzt (ebd., S. 1f.). In Abstimmung zwischen den Behörden wurde 2012 eine »Standardisierende Leistungsbeschreibung« für die Software erarbeitet, die die Funktionen der Software definierte (Deutscher Bundestag, 2016d, S. 6).

Die Bundesregierung setzte dann auf die Entwicklung eigener Software, dies wurde aber wieder durch privatwirtschaftliche Akteure unterstützt (Bundesministerium des Innern, 2014b). Die Arbeit an diesen Werkzeugen wurde 2015 abgeschlossen. Allerdings wurde auf dem freien Markt zusätzlich eine Ersatzoption eingekauft (Süddeutsche Zeitung, 2014b). Öffentlich wurde darüber spekuliert, dass diese Anschaffung notwendig war, da die selbst entwickelte Software zur Quellen-TKÜ nicht über die notwendige technische Funktionalität verfügte, um in allen Anwendungsumfeldern verwendbar zu sein (Welt, 2016). Diese negative Erfahrung hat die Behörden dazu veranlasst, die nächste Softwaregeneration wieder auf dem freien Markt zu beziehen (Welt, 2018). Dieser Einkauf bei kommerziellen Anbietern hat der Regierung viel Kritik beschert, da diese Software bspw. auch an die Türkei verkauft und dort gegen Oppositionelle eingesetzt wurde. KritikerInnen argumentieren daher, die Bundesregierung befeuere die Nachfrage auf einem Markt, der potenziell bedenklich sei und die IT-Unsicherheit fördere, da er von Softwareschwachstellen lebe. Weiterhin könnten Autokratien, mit Verweis auf den demokratischen Kundenkreis, ihr eigenes Verhalten rechtfertigen (Süddeutsche Zeitung, 2018). Sie wiesen damit darauf hin, dass die Regierung durch den Einkauf von Überwachungssoftware international der Reputation als Garant liberaler Grundrechte schade.

Diese Erfahrung führte dazu, dass die Regierung begann, die eigenen technischen Fähigkeiten auszubauen. Trotz prinzipieller Kritik am staatlichen Hacking, das immer auch auf Schwachstellen in Software angewiesen ist und diese daher geheim hält, hat die Bundesregierung 2016 erste Pläne entwickelt, eine Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) einzurichten. Damit trennte die Bundesregierung den Bereich der offensiven Nutzung von Cyberfähigkeiten institutionell vom defensiv ausgerichteten BSI (Süddeutsche Zeitung, 2017).

Die Regierung plante, die Ermittlungsbehörden durch diese neue Institution in die Lage zu versetzen, ihre Aufgaben besser erfüllen zu können. Konkret »geht es um eine Anpassung der technischen Fähigkeiten an die aktuellen Herausforderungen der Kommunikationswelt« (Deutscher Bundestag, 2016d, S. 2). Mit dem Erlass vom 6. April 2017 wurde die neue Institution mit 400 Planstellen offiziell als Bundesanstalt im Geschäftsbereich des BSI etabliert. ZITiS selbst erhielt keine Eingriffsbefugnisse, sondern bietet dem BKA, dem BfV und der Bundespolizei technische Unterstützung mit Blick auf deren operative »IT-Fähigkeiten«

(Deutscher Bundestag, 2018d, S. 2). Eine Kernaufgabe ist dabei die Kryptoanalyse (ebd., S. 10).

Damit baute die Bundesregierung die Kapazitäten aus, die zur Umgehung von Verschlüsselung notwendig sind. Eine Entwicklung, die parallel auch auf europäischer Ebene bei Europol stattfand und dort ebenfalls durch die Bundesregierung unterstützt wurde (Deutscher Bundestag, 2018b). Der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich Wilfried Karl betonte in diesem Kontext aber, dass dies die Kryptopolitik der Bundesregierung nicht verändere:

> »Es gibt heute Verschlüsselungsmethoden, die mathematisch nicht zu brechen sind. Wir maßen uns nicht an, hierfür eine Lösung zu finden. Aber es gibt durchaus Möglichkeiten, mit entsprechender Hardware und schlauen Algorithmen sowie den entsprechenden Experten zu Ergebnissen zu kommen. Etwa, wenn eine Verschlüsselung nicht ordentlich implementiert wurde oder wenn Anwender Fehler gemacht haben. Wenn wir Methoden finden, dann stellen wir sie unseren Kunden zur Verfügung. Wir ändern übrigens nichts an der Kryptopolitik der Bundesregierung. Es geht hier nicht um eine Schwächung von Kryptoverfahren.« (Behörden Spiegel, 2018)

Neben der Umgehung von Verschlüsselung ging mit den Aufgaben von ZITiS auch einher, dass gefundene Schwachstellen in Software aus staatlichen Sicherheitsinteressen ggf. offengehalten werden. Im Gegensatz zu anderen Staaten (bspw. den USA oder dem Vereinigten Königreich), gab es aber noch kein definiertes Verfahren, durch das die Geheimhaltung oder Offenlegung von Sicherheitslücken geregelt wurde. Die Gestaltung dieses Entscheidungsprozesses war am Ende des Untersuchungszeitraumes noch im Gange. Die Regierung hat aber bekanntgegeben, dass ZITiS bis 2018 noch keine Schwachstellen aus externen Quellen eingekauft hatte (Deutscher Bundestag, 2018d, S. 13).

Die neue Institution wurde von Seiten der Netzgemeinschaft und der politischen Opposition scharf kritisiert. Ein Anlass für Kritik war bspw. der fehlende Kriterienkatalog zur Entscheidung über die Offenlegung von Sicherheitslücken (derartige Abwägungen werden zumeist als Vulnerabilities Equities Processes bezeichnet). Hierauf wurde bspw. durch den ehemaligen Datenschutzbeauftragten Peter Schaar oder durch Digitalcourage hingewiesen (Digitalcourage, 2017; heise.de, 2018a). Parlamentarisch wurde von der Linkspartei sogar gefordert, ZITiS wieder aufzulösen. Die neue Institution gefährde »die Datensicherheit und Grundrechte aller Bürgerinnen und Bürger« und verletze das »Trennungsgebot zwischen Polizei und Geheimdiensten« (Deutscher Bundestag, 2019).

Das Bestreben der Bundesregierung, die Beschützer-Rolle durch den Aufbau eigener technischer Fähigkeiten auszubauen und unabhängiger zu gestalten, ist wiederum herausgefordert worden. Auch wenn die Bundesregierung betonte,

dass sie an starker Verschlüsselung festhalte und keine Unterminierung der Technik anstrebe, bemängelte die Opposition, dass die Regierung die Rolle nicht klar genug definierte und bspw. keinen Prozess für die Offenlegung von Schwachstellen definierte. Mit dem Verweis auf das Trennungsgebot bezogen sich KritikerInnen wiederum auf das negative historische Selbst der Bundesrepublik.

Die domestischen Prozesse der Rollenkontestation, insbesondere mit Bezug auf die Rolle als Garant liberaler Grundrechte, begünstigten auch eine zurückhaltende außenpolitische Rollenübernahme der Bundesrepublik. Aktuelle Bestrebungen in der EU mit Regelungen zu digitalen Beweismitteln (E-Evidence) den Zugriff auf Daten in anderen Staaten jenseits internationaler Rechtshilfe zu erleichtern und Diensteanbieter direkt gegenüber externen Strafverfolgungsbehörden auskunftspflichtig zu machen, werden von der Bundesrepublik skeptisch beurteilt. In einem Brief an die Kommission äußerte die Regierung zusammen mit sieben weiteren EU-Mitgliedstaaten Bedenken mit Blick auf die extraterritoriale Geltung der Beschützer-Rolle. Die Bundesregierung bemängelte dabei, dass die vorgesehene Neuregelung den Empfängerstaaten keine Möglichkeit einräume, die externen Datenanfragen abzulehnen. Dies sei besonders vor dem Hintergrund einer fehlenden beiderseitigen Strafbarkeit problematisch, da so Ermittlungen möglich wären, die unter deutschem Recht nicht durchführbar wären. Ferner bedürfe es in einem solchen System Vorkehrungen zum Schutz der Bürgerrechte (Justizministerium, 2018).

Auch die Absicht zwischen EU und USA ein solches Abkommen zum erleichterten Zugriff auf Meta- und Inhaltsdaten zu etablieren, wurde von der Bundesregierung aufgrund bürgerrechtlicher Bedenken kritisch beurteilt. Die Bundesrepublik hat den Vorschlägen daher nicht zugestimmt, sie wurde aber von der Mehrheit im Rat überstimmt (heise.de, 2019). In einem von Netzpolitik.org veröffentlichten Hintergrundpapier äußerte die Bundesregierung besondere Bedenken gegen eine Ausweitung der EU-Regelungen mit den USA. Diese sehen im CLOUD Act nicht nur die Abfrage gespeicherter Daten vor, sondern auch den Zugriff auf laufenden Datenverkehr – also das unmittelbare Abfangen übertragener Kommunikation (Bundesregierung, 2019b, S. 3). Damit ist eine Facette der Beschützer-Rolle berührt, die die deutsche Bundesregierung für die eigenen Strafverfolgungsbehörden noch nicht stabil etablieren konnte.

Da die Bundesregierung die Beschützer-Rolle domestisch noch nicht sicher etablieren konnte, ist die extraterritoriale Teilung der Rolle derzeit kaum möglich. Die besonderen Bedenken und die damit verbundenen Kontestationsprozesse der domestischen Gegenrollenträger sorgen dafür, dass anderen Strafverfolgungsbehörden kein freier Zugriff auf die Daten deutscher Firmen gewährt wird.