4.2 Vereinigtes Königreich

4.2.1 Das britische IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens

In Großbritannien wurde 1990 mit dem Computer Misuse Act (CMA) die Grundlage zur strafrechtlichen Verfolgung von Cyberkriminalität gelegt. Im Gegensatz zur deutschen Entwicklung des Computerstrafrechts wurde im Vereinigten Königreich aber durch einen Angriff auf das interaktive Videotextangebot der British Telecom deutlich, dass die Beschützer-Rolle im Zeitalter der Vernetzung neu definiert werden musste. Robert Schifreen und Stephen Gold waren Ende 1984 in das Prestel-System der BT eingedrungen und hatten dabei auch Zugriff auf den persönlichen Posteingang von Prinz Philip. Von diesem Account aus verschickten sie Mails, die dazu führten, dass Angestellte der BT auf den Angriff aufmerksam wurden. Im April 1985 wurden sie identifiziert und unter dem Forgery and Counterfeiting Act 1981 angeklagt. Sie wurden in erster Instanz zu geringen Geldstrafen verurteilt (Murray, 2016, S. 358 f.). Beide entschieden sich jedoch dazu, das Urteil anzufechten und wurden in der Folge freigesprochen, da das Gesetz nicht die erforderliche Grundlage für eine Verurteilung liefere. Diese Entscheidung wurde im April 1988 durch das House of Lords bestätigt (House of Lords, 1988).

Vor diesem Hintergrund veröffentliche die Law Commission im August 1988 ein Working Paper, das die neuen Probleme der Computerkriminalität eingehend diskutierte, Regulierungsdefizite des bestehenden Rechts aufwarf und verschiedene Reformoptionen aufzeigte.[7] Hierbei wurde auch auf Erfahrungen in anderen Staaten (darunter Deutschland) sowie auf die Entwicklungen in der OECD verwiesen (The Law Commission, 1988, S. 109-128). Die Kommission identifizierte zwar legislativen Handlungsbedarf beim unbefugten Zugriff auf Computersysteme – ein Problem, das durch den Angriff von Schifreen und Gold offengelegt wurde – diskutierte die Möglichkeiten einer Kriminalisierung aber auch kritisch.

Die Etablierung eines neuen Straftatbestandes zum Eindringen in Computersysteme wurde unter anderem deshalb kritisch gesehen, weil ein Zugriff nicht in gleichem Maße als Verletzung der Persönlichkeitsrechte interpretiert wurde, wie in Deutschland:

7 Bereits 1987 hatte die Scottish Law Commission ein Working Paper zur Regulation von Computerstraftaten publiziert. Da das schottische Rechtssystem noch stärker auf dem Fallrecht beruht, war diese Kommission etwas skeptischer, was eine gesetzliche Neuregelung anging. Die Möglichkeit das Recht durch neue Fälle und die richterliche Auslegung weiterzuentwickeln schien aus dieser Perspektive noch nicht gänzlich ausgeschöpft (Wasik, 2010, S. 402).

> »No general right of privacy exists in English law even in the law of tort, and while obtaining unauthorised access to a computer may appear to be akin to the tort of trespass, such behaviour is not generally subject to criminal sanction without some further aggravating feature. Information is not property in English law [...] and it is no offence, as such, to read someone else's correspondence or files.« (Ebd., S. 81)

Die Beschützer-Rolle fand in der Folge eine deutlichere Referenz (Schutz für wen?) zum wirtschaftlichen Schutzgut, als auch zur physischen Sicherheit. Dem Working Paper folgte ein offener Konsultationsprozess in dem sowohl die Zivilgesellschaft als auch Wirtschaftsunternehmen zu Stellungnahmen aufgefordert waren. Ziel der Kommission war es, einen Eindruck von der empirischen Dringlichkeit des Problems zu erhalten, um dann fundierte Empfehlungen auszusprechen. Nach Auswertung der Rückmeldungen gelangte die Kommission im Oktober 1989 zu der Einschätzung, dass Hacking ein akutes wirtschaftliches und sicherheitspolitisches Problem geworden war und dass legislative Maßnahmen daher angebracht waren (The Law Commission, 1989, S. 6).

Dem Papier folgte 1989 der Vorschlag, drei neue Straftatbestände in einem Gesetz zu etablieren. Im Gegensatz zur deutschen Entwicklung wurde die Beschützer-Rolle in Großbritannien bereits in dieser Phase auch durch verstärkte sicherheitspolitische Erwägungen geprägt. Diese Dynamik zeigte sich in Verweisen auf Vorfälle, in denen Personen durch falsch programmierte Fertigungsanlagen physisch verletzt wurden (ebd., S. 3). Ähnlich wie in Deutschland wurde die Beschützer-Rolle aber auch durch wirtschaftliche Erwägungen, wie bspw. hohe Kosten zur Wiederherstellung der Systeme, ermöglicht (ebd., S. 6). Die Kommission erkannte die Regelungsnotwendigkeit aber nicht, weil Informationen als besonders schützenswert erachtet wurden, sondern, um die Integrität der Systeme und deren Funktionsfähigkeit zu wahren:

> »[...] the main argument in favour of a hacking offence does not turn on the protection of information, but rather springs from the need to protect the integrity and security of computer systems from attacks from unauthorised persons seeking to enter those systems.« (The Law Commission, 1988, S. 7)

Der Entwurf für den Computer Misuse Act wurde durch den Konservativen Abgeordneten Michael Colvin in das Unterhaus eingebracht. Auch er wies explizit darauf hin, dass das Gesetz nicht in erster Linie Informationen schützen sollte, sondern die Integrität der Systeme. Dieser Fokus blieb nicht ohne Kritik (insbesondere mit Blick auf Gesundheitsdaten), im Unterhaus wurde daher explizit hervorgehoben, dass, wenn der unberechtigte Zugang für weitere strafbare Handlungen genutzt würde, bspw. zur Informationsgewinnung und Erpressung, dies unter Section 2 ebenfalls erfasst sei (House of Commons, 1990b, S. 1138).

Der Fokus der Beschützer-Rolle auf folgenreiche Cyberangriffe findet Ausdruck in der expliziten Ablehnung eines Hacker-Privilegs, das die deutsche Regierung zunächst noch anerkannte. Im Gegensatz zur deutschen Beschützer-Rolle fand die britische einen der ersten Referenzpunkte (Schutz vor wem?) daher nicht im technisch interessierten Freizeithacker, sondern sanktionierte alle unbefugte Zugriffe (The Law Commission, 1988, S. 12). Dieser Standpunkt wurde im Parlament geteilt und fand Eingang in das Gesetz, auch wenn die Frage einer Überkriminalisierung debattiert wurde, wurden HackerInnen doch prinzipiell als gefährlich betrachtet, so dass deren Verhalten stets als strafbar erachtet wurde (House of Commons, 1990b, S. 1147). Diese Referenz auf potenziell folgenreiche Angriffe zeigte sich auch in den debattierten Szenarien, die bspw. Angriffe auf Krankenhäuser, militärische Einrichtungen oder Verkehrsleitsysteme umfassten (House of Commons, 1990b; House of Lords, 1990).

Die Kommission empfahl die Etablierung von drei neuen Straftatbeständen, die dann in den Computer Misuse Act übernommen wurden: »1. Unauthorised access to computer material. 2. Unauthorised access with intent to commit or facilitate commission of further offences. 3. Unauthorised modification of computer material« (The Stationery Office, 1990, Sections 1, 2, 3). Aus der Ablehnung einer/s potenziell wohlwollenden Hackerin/s und der daraus folgenden Referenz (Schutz vor wem?) auf gefährliche AngreiferInnen folgte auch, dass der Computer Misuse Act in Section 14 neue Kompetenzen zur Beschlagnahme und Durchsuchung bereits für den eigentlich als Ordnungswidrigkeit (summary offences) eingestuften Tatbestand »Unauthorised access to computer material« definierte (ebd., Section 14). Diese Ausweitung der Befugnisse der Strafermittlungsbehörden wurde im House of Commons besonders kritisch diskutiert, letztlich aber mehrheitlich akzeptiert (House of Commons, 1990b; House of Lords, 1990).

In der parlamentarischen Debatte wurde zur Rechtfertigung der neuen Regelungen, wie in der Kommission, wiederholt auf die wirtschaftlichen Kosten der Computerkriminalität, die steigenden Fallzahlen sowie die vermutlich hohe Dunkelziffer verwiesen (House of Commons, 1990b, S. 1134 bzw. 1143). Auch WirtschaftsvertreterInnen (bspw. der Arbeitgeberverband CBI) betonten unter Bezugnahme hierauf die Regulierungsnotwendigkeit (House of Commons, 1990a, S. 1291). Ähnlich wie in Deutschland wurde auch hier von VertreterInnen unterschiedlicher Parteien auf die rasante Verbreitung der Technik und damit die wachsende gesellschaftliche Bedeutung hingewiesen:

> »Government computerisation has made us all a great deal more vulnerable, as has company computerisation. The City of London money markets, Lloyd's and all sorts of financial organisations that have made Britain financially great and far advanced depend upon computers.« (House of Commons, 1990b, S. 1154)

Insgesamt wurde der Gesetzesentwurf daher überparteilich unterstützt. Dies wurde auch dadurch begünstigt, dass er als *private member's bill* eingebracht wurde (ebd., S. 1158). Es wurde aber auch kritisiert, dass die Regierung nicht selbst einen Vorschlag zur Regulierung vorgelegt hatte. Im Gegensatz zur Entwicklung in Deutschland, in der die (unterschiedlichen) Regierungen die Entwürfe maßgeblich vorangetrieben haben, war die Etablierung der Beschützerrolle in Großbritannien Ergebnis parlamentarischen Regulationsstrebens.

Wie bereits angedeutet, zeigt sich hier ein Unterschied zu der Entwicklung in Deutschland. Wie in Deutschland lag die Referenz (Schutz für wen?) zwar auf dem Schutz ökonomischen Wohlstands. Die Rolle als Wohlstandsmaximierer wirkte somit katalytisch auf die Etablierung der Beschützer-Rolle. Im Unterschied zu Deutschland stand in Großbritannien aber bereits in der Frühphase nicht das Verhalten von FreizeithackerInnen zur Debatte. Diskussionen befassten sich vielmehr bereits zu diesem Zeitpunkt mit physischen Folgen von Cyberangriffen, sodass die Referenz der Rolle (Schutz vor wem) von Beginn an eine andere war.

Da in Großbritannien erst vergleichsweise spät über eine Kriminalisierung von Computerstraftaten debattiert wurde (auch im Vergleich zu Deutschland), wurde die Etablierung der Beschützer-Rolle in stärkerem Maße durch internationale Erwartungen begünstigt. Die Abgeordneten befürchteten, dass das Vereinigte Königreich ohne eine Kriminalisierung der Computerstraftaten international zum Rückzugsort für HackerInnen werden könnte (ebd., S. 1135). Es galt also internationale Reputationsverluste aufgrund einer fehlenden bzw. defizitären Beschützer-Rolle zu vermeiden. Der internationale Rollenbezug wurde dabei auch durch die Devolution des Vereinigten Königreichs und potenziell unterschiedliche Regelungen selbst befördert (House of Lords, 1990, S. 231).

Die internationale Ausrichtung ist auch deshalb bemerkenswert, weil damit verbunden die Rolle als Garant liberaler Grundrechte einen zusätzlichen Bezugspunkt hat, nämlich auf der neu entstehenden Infrastruktur. Zum Zeitpunkt der Gesetzesverabschiedung wurde in Großbritannien bereits auf die Notwendigkeit eines international koordinierten Vorgehens verwiesen, um auch langfristig ein freies Internet zu gewährleisten:

> »Without legislation that is agreed internationally, to the effect that unauthorised access is a crime, there is a real danger that owners of computer network systems will be encouraged to erect ring fences of security around their systems. One has in mind university systems that are useful for sharing information and data. Without the law to convict unauthorised users of those systems, there is a danger that the systems will be less open and less available and that society will suffer as a result.« (House of Commons, 1990b, S. 1159)

Die Beschützer-Rolle ist in diesem Kontext also auch durch die Rolle als Garant liberaler Grundrechte begünstigt. Die Referenz (Schutz für wen?) liegt aber nicht

nur auf dem Schutz der eigenen Wirtschaft bzw. Bevölkerung, sondern auch auf dem Erhalt des freien Netzes. Dies ist besonders bemerkenswert, da das globale Internet zu dieser Zeit noch nicht in seiner späteren Form erkennbar war. Es ist damit auch die internationale Rollenausrichtung, die für die britische Etablierung der Beschützer-Rolle bedeutend war. Sie weist von Beginn an stärkere extraterritoriale bzw. internationale Bezüge auf.

Ferner adressierte die britische Rolle bereits im Jahr 2000 terroristische Gefahren, während die deutsche Beschützer-Rolle eine terroristische Referenz (Schutz vor wem?) erst später, nach den Anschlägen des 11. Septembers, fand. Mit dem Terrorism Act 2000 wurden explizit auch solche Cyberangriffe unter Strafe gestellt, die darauf ausgerichtet waren »to interfere with or seriously to disrupt an electronic system« (The Stationery Office, 2000c, Section 1(2)(e)). Mit bis zu zehn Jahren Freiheitsstrafe war auch das Strafmaß im Vergleich zu Deutschland deutlich höher, wo zu dieser Zeit die Referenz zu Terrorismus noch nicht gesetzlich hergestellt wurde. Diese Ausrichtung der britischen Beschützer-Rolle wurde durch die Bezugnahme auf historische Erfahrungen, insbesondere mit dem irischen Terrorismus, erleichtert. Die Referenz ist damit auf den domestischen Terrorismus bezogen und findet sich in verschiedenen Debatten sowohl auf Seiten der Regierung als auch in beiden Kammern des Parlaments (House of Commons, 1999a, 2000a; House of Lords, 2000). Der Bezug zum historischen Selbst als Opfer terroristischer Anschläge ermöglichte damit bereits früher eine sanktionsbewährtere Beschützer-Rolle, die auch domestisch weniger herausgefordert wurde als in Deutschland (The Stationery Office, 2000c).

4.2.2 Kryptopolitik

Auch in Großbritannien wurde Mitte der 1990er Jahre eine Debatte um die Regulation von Verschlüsselung geführt. In diesem Kontext wiesen VertreterInnen der Tory-Regierung, ähnlich wie in der Bundesrepublik, darauf hin, dass die Ermittlungsbehörden durch starke Verschlüsselung nicht in ihrer Arbeit eingeschränkt werden dürften. Es galt also die Funktionsfähigkeit der Beschützer-Rolle zu gewährleisten. Eine Regelung müsse daher darauf zielen »to preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism« (Department of Trade and Industry, 1997).

Nach interministeriellen Konsultationen veröffentlichte das Department for Trade and Industry 1996 ein Strategiepapier, das die Pläne der Regierung skizzierte. Die Beschützer-Rolle, die in diesen ersten Entwürfen dargelegt wurde, war deutlich von der amerikanischen Rolle inspiriert. Die Regierung beabsichtigte ein System aus gewerblichen Trusted Third Partys (TTPs) zu installieren, die die Verschlüsselung staatlich lizenziert übernehmen sollten. Die TTPs sollten gesetzlich dazu verpflichtet werden, eine Schlüsseldublette zu verwahren,

um diese den Sicherheitsbehörden zu Ermittlungszwecken zur Verfügung stellen zu können. Wie die amerikanische Administration, wollte auch die britische Regierung an Exportbeschränkungen für Verschlüsselungslösungen festhalten, die keine Key-Recovery-Funktionalität beinhalteten (ebd.). Ferner wurde darüber debattiert, dass auch die Schlüssel, die nicht bei TTPs hinterlegt waren, verfügbar sein sollten (House of Commons, 1999c). Um Zugriff auf die Schlüssel zu erhalten, die nicht bei britischen TTPs hinterlegt würden, sollten internationale Abkommen zur Kooperation bei der Strafverfolgung geschlossen werden (Trade and Industry Select Committee, 1999).

Im Gegensatz zur Bundesrepublik wurde in Großbritannien ein umfassendes und potenziell globales Key-Escrow-System von der Tory-Regierung nicht abgelehnt (ebd.). Zwar wurde eine amerikanische Dominanz und die extraterritoriale US-Beschützer-Rolle in diesem Kontext ebenfalls kritisch gesehen. Dies hatte aber keine strikte Ablehnung der Key-Recovery zur Folge, sondern führte zu Debatten darüber, wie ein solches System besser ausgestaltet werden könne. Stimmen aus der Regierung befürworteten daher grundsätzlich Lösungen zur Schlüsselhinterlegung auch unter Verweis auf deren potenziell positive Effekte für die wirtschaftliche Entwicklung. Nur mit einer (globalen) Schlüsselinfrastruktur könne auch das Vertrauen der Unternehmen und KundInnen in die Verschlüsselung der GeschäftspartnerInnen erhalten werden (Hickson, 1997, S. 584).

Kritik erfuhren diese Pläne aus der Wirtschaft und Zivilgesellschaft, auch Teile der zu diesem Zeitpunkt oppositionellen Labour Party lehnten das Vorhaben als zu weitreichend ab. Nur wenige Stimmen unterstützten die Pläne der Regierung ohne substanzielle Einschränkungen (Trade and Industry Select Committee, 1999). Die KritikerInnen warfen der Regierung unter anderem vor, mit einer Schwächung der Verschlüsselung nicht nur Wirtschaftsgeheimnisse zu gefährden, sondern auch weitreichende Überwachungsmöglichkeiten zu schaffen (Akdeniz, 1997; Hickson, 1997). Die Ablehnung erfolgte also vornehmlich im domestischen, nicht im internationalen Rollenspiel als Abgrenzung zur USA. Dies hilft zu verstehen, warum britische Regierungen international immer wieder die Regulation von Kryptographie offen diskutiert haben.

Als bei den Wahlen 1997 die konservative Regierung von John Major durch die Labour-Administration von Tony Blair ersetzt wurde, hielt die neue Regierung nach dem Wahlsieg trotz voriger Kritik an den Plänen zur Key-Recovery fest. Im Unterschied zur Vorgängerregierung sollten die Regelungen aber nicht mehr verpflichtend sein, sondern auf freiwilliger Kooperation mit den TTPs basieren (Trade and Industry Select Committee, 1999).

Im Vorwort einer Analyse unterschiedlicher Möglichkeiten zum Umgang mit dem Problem, konstatierte der neue Premierminister Tony Blair: »there is already evidence that criminals, such as paedophiles and terrorists, are using encryption to conceal their activities. […] If powers of interception and seizure are rende-

red ineffective by encryption, all society will suffer« (Cabinet Office, 1999, S. i). Ähnlich wie in Deutschland wurde damit auf die potenziellen Beschränkungen der Beschützer-Rolle verwiesen, die dazu führen würden, dass Strafverfolgung nicht mehr effektiv gewährleistet werden könne. Anders als in der Bundesrepublik führte aber die ausbleibende Referenz auf ein negatives historisches Selbstbild und die damit verbundenen Bedenken zu liberalen Freiheitsrechten dazu, dass die Regelung zur Schlüsselhinterlegung mit Plänen zu einem neuen Electronic Communications Act im Vereinigten Königreich für fünf Jahre implementiert wurden (The Stationery Office, 2000a). Deutliche Kritik aus der Wirtschaft und aus dem Parlament sorgten aber dafür, dass die Regelung – anders als von der Vorgängerregierung geplant – freiwillig war und dass weitere sicherheitspolitische Maßnahmen zum Umgang mit Verschlüsselung aus dem Gesetz gestrichen wurden (Trade and Industry Select Committee, 1999).

Stimmen, die darauf hinwiesen, dass sich die Politiken der internationalen Partner mit Blick auf Key-Escrow verändert hatten, dass die OECD-Guidelines dazu aufriefen NutzerInnen die freie Wahl der Verschlüsselung zu überlassen und die daher dafür plädierten, die Regelungen auch nicht auf freiwilliger Basis in Kraft zu setzen, konnten sich zunächst nicht durchsetzen. Wie in Deutschland wurde die Kritik auch hier unter Verweis auf die beiden Rollen als Wohlstandsmaximierer (von Akteure aus der Wirtschaft) und Garant liberaler Grundrechte (von Bürgerrechtsbewegungen und VertreterInnen der technischen Community) artikuliert (House of Commons, 1999b; Trade and Industry Select Committee, 1999).

Die Abgeordneten im Ausschuss für Handel und Industrie brachten ihre Enttäuschung über die Position der Regierung offen zum Ausdruck: »We are disappointed, however, that the Government should still hold a candle for key escrow and key recovery. […] We can foresee no benefits arising from Government promotion of key escrow or key recovery technologies« (Trade and Industry Select Committee, 1999, S. VIII – 90.). Grundsätzlich machten die Parlamentarier deutlich, das sie mit der Kooperation zwischen Regierung und Wirtschaft mit Blick auf Verschlüsselung nicht zufrieden waren und dass sie die Schuld dafür bei der Regierung sahen (ebd., S. VIII – 105.).

Auch wenn die Kritik nicht dafür gesorgt hat, dass das freiwillige System aus TTPs aufgegeben wurde, hat der Widerstand verschiedener Akteure doch dazu geführt, dass die Regelung zur freiwilligen Schlüsselhinterlegung mit einem fünfjährigen Verfallsdatum (sunset clause) versehen wurde, 2006 wurde die Regel endgültig ausgesetzt (House of Commons, 1999b). Die Regierung begründete die endgültige Abkehr von einer verpflichtenden Schlüsselhinterlegung dann auch mit den Bedenken, diese könnten die Internetwirtschaft in Großbritannien nachhaltig schädigen, insbesondere da die internationale Konkurrenz nicht durch derartige Arrangements beeinträchtigt worden war (House of Commons, 2000d, S. 775).

Die Rolle als Garant liberaler Grundrechte wirkte damit weniger begrenzend auf die Beschützer-Rolle als in Deutschland. Auch aufgrund der besonderen Beziehung zu den USA, wurde der Vorstoß der amerikanischen Regierung nicht rundum abgelehnt. Da die Referenz zu einem negativen historischen Selbst ebenfalls ausblieb, konnte die britische Regierung in der Folge immer wieder eine restriktivere Verschlüsselungspolitik verfolgen. Am folgenreichsten war letztlich die Kontestation der WirtschaftsvertreterInnen, die mit Bezug zur Rolle als Wohlstandsmaximierer, die besondere Bedeutung von Verschlüsselung für das Netz als Wirtschaftsraum herausstellte und betonte, dass starke Kryptografie für ein vertrauensvolles Verhältnis der Wirtschaftssubjekte essenziell sei. Den Wettbewerbsnachteil einer freiwilligen Schlüsselhinterlegung gab die Regierung daher auf. Sie suchte aber nach neuen Möglichkeiten die Beschützer-Rolle aufrechtzuerhalten.

Da es sich bei den Vorschriften im Electronic Communications Act um freiwillige Regelungen handelte, wurde für den Umgang mit Verschlüsselung der im Jahr 2000 verabschiedete Regulation of Investigatory Powers Act (RIPA) bedeutend – insbesondere, als die Sunset Clause 2006 zum Auslaufen der freiwilligen Regeln für Kryptographiedienstleister führte. Mit RIPA wurden einige der sicherheitspolitischen Maßnahmen etabliert, die bereits zuvor debattiert wurden, aber aufgrund des Drucks aus Parlament und Wirtschaft nicht mit dem Electronic Communications Act reguliert wurden. Um den Strafverfolgungsbehörden Zugriff auf verschlüsselte Kommunikation zu ermöglichen, ohne dabei Kritik für die Unterminierung von Kryptographie im Allgemeinen zu erfahren, wurde mit RIPA die Möglichkeit geschaffen, von Verdächtigen sanktionsbewährt die Herausgabe der privaten Schlüssel zu fordern. In den Debatten zu RIPA wurde der Konflikt zwischen den Rollen Wohlstandsmaximierer, Garant liberaler Grundrechte und Beschützer erneut deutlich (ebd.).

Auch die Regierungsseite erkannte die Probleme einer Unterminierung von Verschlüsselung an, sah es aber dennoch als unabdingbar, andere Möglichkeiten zur erzwungenen Schlüsselherausgabe zu etablieren. Die Regierung argumentierte, dass die neuen Regelungen nur dazu dienten, bereits existierende Kompetenzen im Angesicht technischer Entwicklungen zu erhalten. Es ging aus ihrer Sicht also nicht um den Ausbau der Beschützer-Rolle. Ferner versicherte Innenminister Jack Straw, dass die Ermittlungsbehörden nur Zugriff auf Schlüssel von rechtmäßig abgefangenen Daten verlangen könnten. Die Beschützer-Rolle wurde aus Sicht der Regierung durch die Rolle als Garant liberaler Grundrechte angemessen begrenzt. Die Forderung, den Ermittlungsbehörden die Möglichkeit zu geben, Schlüssel unter Androhung von Zwangsmaßnahmen zu fordern, wurde grundsätzlich auch von Teilen des Parlaments anerkannt (Trade and Industry Select Committee, 1999, S. VIII – 98.). Auch wenn es kritische Stimmen aus der Wirtschaft gab, stimmte auch der Ausschuss für Handel und Industrie der

Einschätzung zu, wonach die Befugnis zur Schlüsselherausgabe eine wichtige Kompetenz der Ermittlungsbehörden sei (House of Commons, 2000d, S. 775).

Allerdings machte die Opposition auch auf Probleme aufmerksam. Abgeordnete wiesen darauf hin, dass die Strafe für die Nichtherausgabe des Schlüssels möglicherweise geringer sein könnte als das Strafmaß für das verfolgte Delikt und dass daher ggf. eher Strafen für die Zurückhaltung der Schlüssel akzeptiert würden, als mit den Ermittlungsbehörden zu kooperieren. Ferner betonten sie, dass NutzerInnen nicht dafür belangt werden dürften, wenn Schlüssel automatisch geändert würden. Auch die Unschuldsvermutung würde durch die Regeln »auf den Kopf gestellt«, da Verdächtige nachweisen müssten, den Schlüssel nicht zu besitzen bzw. zu kennen. Weiterhin erschien es problematisch, von Beschuldigten Informationen zu verlangen, die sie selbst belasten könnten (Trade and Industry Select Committee, 1999, S. VIII). Punkte, die in der Debatte im Unterhaus wiederholt aufgegriffen und kritisiert wurden (House of Commons, 2000d). Allerdings ohne Erfolg, die Regierung etablierte mit RIPA die Möglichkeit, die Herausgabe von privaten Schlüsseln zu fordern, sofern Ermittlungsbehörden auf rechtmäßigem Wege an verschlüsselte Daten gelangten. Andernfalls drohten Freiheitsstrafen von bis zu zwei Jahren. War die nationale Sicherheit oder Kinderpornographie betroffen, reichte das Strafmaß bis zu fünf Jahren (Parliamentary Office of Science and Technology, 2006; The Stationery Office, 2000b). Part III Section 49 von RIPA sollte es Ermittlungsbehörden aus Gründen der nationalen Sicherheit, zur Strafverfolgung (bzw. -vereitelung) oder im Interesse des ökonomischen Wohlergehens des Vereinigten Königreichs ermöglichen, die Herausgabe von privaten Schlüsseln bzw. die lesbare Form der verschlüsselten Daten zu fordern. Die Betroffenen konnten ferner dazu verpflichtet werden, die Anordnung geheim zu halten. Von Kommunikationsdienstleistern verlangte RIPA, die Möglichkeiten zum Abfangen von Kommunikationsinhalten vorzuhalten und daher Verschlüsselung zu entfernen, sofern diese von den Communication Service Providern (CSP) selbst implementiert wurde (Severson, 2017, S. 6f.). Die Definition von CSPs ist dabei im Vereinigten Königreich umfassender als in Deutschland. Während in Deutschland Telekommunikationsdienstleister von Telemedien unterschieden werden, kennt die britische Rechtslage diese Differenzierung nicht. Damit werden bspw. auch Betreiber von Messengerdiensten erfasst und die Beschützer-Rolle ist dementsprechend umfassender (Home Office, 2015a, S. 6). Außerdem ist die Beschützer-Rolle in Großbritannien enger mit der Rolle als Wohlstandsmaximierer verbunden. Hierdurch entstehen auch katalytische Wechselwirkungen, wenn es bspw. um die Schlüsselherausgabe zum Erhalt des ökonomischen Wohlergehens des Vereinigten Königreiches geht.

Die neuen Regelungen wurden letztlich von einer überparteilichen Mehrheit als angemessen beurteilt. Sogar die oppositionellen Liberal Democrats konstatierten, dass es Umstände gebe, in denen derartige Kompetenzen zur Entschlüsselung

notwendig seien, um Schaden von der britischen Bevölkerung abzuwenden und die Sicherheit zu gewährleisten: »it would be a very serious omission to have no means of intercepting and reading encrypted communications between dangerous criminals embarking on a very serious crime, or between people attempting to threaten the lives of the people of this country« (House of Commons, 2000b, S. 1206).

Aufgrund der vorgetragenen Kritik, wurde Part III allerdings bei der Verabschiedung des Gesetzes noch außer Kraft gesetzt und sollte zu einem späteren Zeitpunkt aktiviert werden, sofern die zunehmende Nutzung von Verschlüsselung zu einem maßgeblichen Problem der Strafverfolgungsbehörden werden würde. Dass dieser Fall irgendwann eintreten würde, betonte der Innenminister bereits bei den ersten Parlamentsdebatten:

> »The gloomy prognosis, though, is that whatever is done, law enforcement will take a hit over encryption. [...] Introducing the measures in part III is the least that we can do to minimise the effect of that hit. They form an important part of the package of measures that we are putting in place if we are to have any hope of dealing successfully with the threat from the criminal use of encryption.« (House of Commons, 2000d, S. 777)

Aus Sicht der Regierung war der kritische Punkt im Juni 2006 erreicht. Die Administration kündigte daher Konsultationen zur Aktivierung der Befugnisse an. Die Pläne, dass die Regierung die Einführung der sogenannten Section 49 Notices erwog, führte bei Bürgerrechtsbewegungen zu vehementer Kritik (EDRi, 2006). Das Innenministerium rechtfertigte die Konsultationen und letztlich die Aktivierung der neuen Befugnisse damit, dass die Ermittlungsbehörden immer häufiger auf verschlüsselte Daten stießen und dass deren Arbeit hierdurch signifikant beeinträchtigt würde. Neben Kriminalität verwies das Innenministerium wiederholt auf die Gefahr terroristischer Aktivitäten, die unter dem Deckmantel von Verschlüsselung potenziell unentdeckt bleiben könnten. Aus Sicht der Regierung wurde dieses Problem zwischen 2003 und 2006 immer deutlicher, sodass zwingender Handlungsbedarf bestand, da die Funktion der Beschützer-Rolle nicht mehr gewährleistet werden konnte (Home Office, 2006, S. 3). Die Konsultationen mit VertreterInnen aus Wirtschaft, Zivilgesellschaft und Wissenschaft führten, trotz anhaltender Kritik, dazu, dass die entsprechenden Befugnisse im Oktober 2007 in Kraft gesetzt wurden (Home Office, 2007).

Der praktische Umgang mit diesen neuen Kompetenzen führte in der Folge immer wieder zur Kontestation der Regierung. Insbesondere der offensive Umgang mit den neuen Befugnissen sorgte schnell für Kritik. Die ErmittlerInnen nutzten die Kompetenzen aus Sicht der KritikerInnen bereits bei vergleichsweise geringen Anschuldigungen. So wurden bspw. gegen Tierschutz-AktivistInnen

oder psychisch Kranke Haftstrafen verhängt, da sie sich weigerten mit den Behörden zu kooperieren (Brunst, 2012, S. 336f.). Auch der Fall eines jungen Hackers, der im Sommer 2014 versucht hatte Zugriff auf eine Webseite zu erlangen und der die Polizei von Newcastle durch Scherzanrufe störte, wurde durch eine Section 49 Notice zu sechs Monaten Freiheitsstrafe verurteilt, da er sich weigerte die Schlüssel für seine kryptierte Festplatte preiszugeben. Auch dies wurde aus den Reihen der Netzgemeinde und von Bürgerrechtsbewegungen kritisiert. Einer der weiteren Hauptkritikpunkte war, dass die Anordnungen zur Schlüsselherausgabe nicht durch RichterInnen ausgesprochen werden mussten, sondern durch entsprechende Beamte der Ermittlungsbehörden (GCHQ, MI6, MI5, die Polizei und die National Crime Agency) (Vice, 2014).

Diese Kritik wurde mit dem Investigatory Powers Act (IPA) 2016 aufgegriffen. Das Gesetz sah erstmalig eine richterliche Befugnis für die Anordnung zur Schlüsselherausgabe vor.[8] Zwar blieben die Befugnisse unter Part III Section 49 weitgehend erhalten, mit dem Investigatory Powers Commissioner (IPC) etablierte die Regierung aber eine neue Kontrollinstanz, die die Praxis der Ermittlungsbehörden überwachen und regelmäßig Bericht erstatten sollte. Dies war aber die einzige Beschränkung der Beschützer-Rolle. Denn auch aufgrund der durch Terroranschläge in Paris erweiterte der IPA die Einsatzmöglichkeiten für Anordnungen zur Schlüsselherausgabe. Waren diese zuvor nur dann möglich, wenn ErmittlerInnen auf rechtmäßigem Weg (lawful interception) verschlüsselte Inhaltsdaten abgegriffen hatten, war der Einsatz durch den IPA auch dann möglich, wenn Behörden verschlüsselte Metadaten nutzten (Severson, 2017, S. 8).

Die Erweiterung exekutiver Kompetenzen wurde dabei maßgeblich durch die Anschläge auf die Redaktion von Charlie Hebdo im Januar 2015 in Paris ermöglicht. In diesem Kontext setzte sich der britische Premierminister David Cameron wiederholt dafür ein, nicht überwachbare Kommunikationsräume nicht zu dulden:

> »whether it has been about looking at letters, or about fixed telephone communications or mobile communications, we have always believed that, in extremis, on the production of a signed warrant from the Home Secretary, it should be possible to look at someone's communications to try and stop a terrorist outrage. The decision we have to take is: are we prepared to allow in future, as technology develops, safe spaces for terrorists to communicate? The principle I think we should adopt is that we are not content for that to happen, and as a result we should look to legislate accordingly.« (House of Commons, 2015b, S. 862)

8 Die neue gesetzliche Regelung wurden maßgeblich durch die Snowden-Enthüllungen ermöglicht.

Mit dieser Position sorgte Cameron international für Aufsehen, da in diesen Aussagen eine Forderung nach dem Verbot oder der substanziellen Schwächung von Verschlüsselung gesehen wurde (The Guardian, 2015b). KritikerInnen sahen in der Stellungnahme den einseitigen Versuch, die Beschützer-Rolle über Gebühr auszudehnen, ohne dabei die Implikationen für die Rollen als Wohlstandsmaximierer und Garant liberaler Grundrechte zu berücksichtigen.

Auch wenn der Premierminister nach heftiger Kritik darauf hinwies, dass er nicht beabsichtige, Verschlüsselung zu verbieten, blieben die Vorschläge zu einem restriktiveren Umgang umstritten. Bei der Vorstellung des IPA wies Innenministerin Theresa May aber explizit darauf hin, dass die Regierung nicht plane Verschlüsselung zu verbieten, sondern, dass sie darin auch ein wichtiges Werkzeug für die funktionierende Onlinewirtschaft sowie den Datenschutz der BürgerInnen sah. Dennoch seien die neuen Kompetenzen notwendig, um den sicherheitspolitischen Gefahren auch weiterhin effektiv begegnen zu können (House of Commons, 2015e, S. 975). Die Regierung erkannte damit die Bedenken der KritikerInnen an und wies selbst auf die Spannungen zwischen den drei Rollen hin. Die Exekutive ging davon aus, mit dem neuen Gesetz eine gute Balance zwischen den Rollen gefunden zu haben.

Durch den IPA wurde den zuständigen MinisterInnen, nach richterlicher Prüfung, die Möglichkeit eingeräumt, durch sogenannte »technical capability notices« die Entfernung technischer Schutzmaßnahmen gegenüber CSPs zu veranlassen (Science and Technology Committee, 2016, S. 16). Aufseiten der Bürgerrechtsbewegungen sorgte diese Praxis für erhebliche Kritik. Privacy International sah darin »an indirect attack on end-to-end encryption« (ebd., S. 16). Diese Sorge teilten auch andere NGOs. Sie befürchteten, dass durch die Vorgaben eine Verbreitung von Ende-zu-Ende-Verschlüsselung unterbleiben würde, da die Anbieter einer solchen Aufforderung zur Entschlüsselung nicht mehr nachkommen könnten, weil die Schlüssel direkt zwischen den NutzerInnen ausgetauscht werden. Eine verlangsamte Verbreitung von Ende-zu-Ende-Verschlüsselung habe sowohl negative Effekte für die Privatheit der Kommunikation als auch auch für den Wirtschaftsstandort (ebd., S. 17f.). Auch der mit dem Gesetz betraute Parlamentsausschuss teilte die Sorge über potenziell schädliche Effekte für die Verbreitung von Ende-zu-Ende-Verschlüsselung:

> »The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so.« (UK Government, 2016b, S. 50)

Das Parlament forderte von der Regierung ferner klarzustellen, dass diese nicht beabsichtige, Hintertüren in Verschlüsselung vorzuschreiben oder die Technologie

grundlegend zu schwächen. Ferner wiesen die Abgeordneten darauf hin, dass die gesetzlichen Regelungen mit dem britischen und europäischen Datenschutz konform sein müssten (UK Government, 2016b, S. 50 bzw. 92).

Die Administration erkannte einige dieser Punkte an und stellte in diesem Kontext klar, dass CSPs nur die Verschlüsselung aufheben mussten, die sie selbst zur Verfügung gestellt bzw. implementiert hatten (ebd., S. 80). Ein expliziter Bezug zur Ende-zu-Ende-Verschlüsselung blieb aber aus. Mit Blick auf den Vorwurf, die Exekutive unterminiere Verschlüsselung im Allgemeinen, wiesen RegierungsvertreterInnen wiederholt darauf hin, dass bereits RIPA Telekommunikationsanbieter dazu verpflichtet hatte, Verschlüsselung zu entfernen soweit sie von den Dienstleistern selbst zur Verfügung gestellt wurde und dass der IPA diese Kompetenzen nicht erweitert habe (UK Government, 2016e). Die neuen Regelungen wurden dennoch von KritikerInnen als eine umfassende Kompetenzerweiterung gedeutet, da die Unternehmen noch unter RIPA nur dabei mitwirken mussten, Daten zu entschlüsseln, nachdem Ermittlungsbehörden diese rechtmäßig erhoben hatten. Durch den IPA jedoch wurde von den Dienstleistern verlangt prophylaktisch Kapazitäten zur Entschlüsselung vorzuhalten. Dies wurde wiederholt als ein Angriff auf Verschlüsselung im Allgemeinen gesehen, da die Unternehmen bspw. Hintertüren in ihren Produkten platzieren müssten (Severson, 2017, S. 10f.).

Zur Begrenzung der Beschützer-Rolle kam es damit nur mit Bezug zur Rolle als Wohlstandsmaximierer, da eine Überforderung der Dienstleister durch eine grundsätzliche Pflicht zur Entschlüsselung drohte.

Hervorzuheben ist ferner, dass die Regierung in diesem Kontext beanspruchte, Technical Capability Notices zur Dekryptierung auch für Unternehmen im Ausland erlassen zu können. Damit ging die teilweise extraterritoriale Geltung der Beschützer-Rolle einher, sofern britische Sicherheitsbelange berührt wurden (ebd., S. 9). Diese expansive Kompetenzaneignung wurde von zahlreichen (vornehmlich amerikanischen) Internetunternehmen kritisch gesehen (Science and Technology Committee, 2016, S. 18f.). Auch im Parlament wurde darauf hingewiesen, dass Unternehmen durch diese Regelungen in Konflikte zwischen widersprüchlichen gesetzlichen Regelungen verstrickt werden könnten (House of Commons, 2016b, S. 917). Aber auch nach dem Konsultationsprozess gab die Regierung diese Bestrebungen der Entterritorialisierung nicht auf. Die Regierung präzisierte im finalen Gesetzestext aber die Anforderungen, die mit einer extraterritorialen technical capability notice verbunden sind. So ist bei der Anordnung, wie auch im domestischen Gebrauch, zunächst abzuwägen, »whether it is reasonably practicable for a telecommunications operator« einer solchen Forderung nachzukommen (The Stationery Office, 2016, Section 85 (4)). Ferner ist bei ausländischen Unternehmen die Rechtslage im jeweiligen Land zu berücksichtigen und ob es für das Unternehmen möglich ist, der Anordnung folge zu leisten,

ohne dabei Gesetze zu verletzen (ebd., Section 85 (4)(a)(b)). Die britische Regierung trug damit die domestische Beschützer-Rolle nach außen und versuchte ihr mit dem IPA zumindest teilweise extraterritoriale Wirkung zu verschaffen.

Von vielen KritikerInnen aus dem Parlament wurden die Einschränkungen aber als zu undefiniert und kaum überprüfbar gesehen (Severson, 2017). Das Parlament vertrat in diesem Kontext aber keine eindeutig kritische Position, denn im legislativen Prozess wurde durch Abgeordnete einerseits darauf hingewiesen, dass die extraterritorialen Befugnisse prinzipiell problematisch sein könnten, andererseits forderten die MPs auch, die Möglichkeiten zum internationalen Datenaustausch zu verbessern (UK Government, 2016b, S. 63 bzw. 89).[9] Daher konnte die Regierung ihre Position im Gesetzestext letztlich verwirklichen und die Beschützer-Rolle teilweise über die territorialen Grenzen hinweg erweitern. Die Regierung griff dabei auch die Forderung nach internationaler Kooperation auf und betonte mit Blick auf die Rolle als Garant liberaler Grundrechte, dass es in diesem Kontext zunächst darauf ankomme, mit internationalen PartnerInnen grundlegende Regeln zum Datenaustausch festzulegen, die auch einen hohen Schutz der Privatsphäre der BürgerInnen gewährleisteten (ebd., S. 63).

Weitere VertreterInnen aus der Netzcommunity sahen in den Bestrebungen auch eine verzweifelte staatliche Reaktion auf die Weigerung Apples im Fall des Attentäters von San Bernardino ein verschlüsseltes iPhone zu entschlüsseln (Naked Security, 2019). Ferner wurde die im IPA definierte Praxis auch in einem wissenschaftlichen Gutachten kritisiert, das der UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in Auftrag gegeben hatte. In dieser Studie wurde bemängelt, dass die Vorgaben zu vage gehalten waren und dass die Regelungen als Verpflichtung zum Einsatz von Hintertüren interpretiert werden könnten. Ferner problematisierte die Untersuchung, dass Großbritannien damit zu einem negativen Vorbild für andere Staaten geworden sei – bspw. China (United Nations Human Rights Special Procedures, 2018). Die Einführung gesetzlicher Restriktionen für Verschlüsselung

9 Die Forderungen nach einem verbesserten internationalen Datenaustausch erfolgte unter Verweis auf den Mord an Lee Rigby durch zwei islamistische Terroristen. Der Fall steht aber nicht unmittelbar mit der Verschlüsselungsproblematik in Verbindung. Dennoch löste er umfassende Kritik an Facebook aus, weil Informationen über die Täter und deren Pläne nicht frühzeitig an die britischen Sicherheitsbehörden übermittelt worden waren. In diesem Zusammenhang entwickelte sich im Vereinigten Königreich eine Debatte darüber, inwiefern Betreiber sozialer Medien dazu verpflichtet seien, die eigenen Seiten nach Anzeichen für terroristische Planungen zu durchsuchen und proaktiv Maßnahmen zu ergreifen (The Telegraph, 2014). Im Bericht des Intelligence and Security Committees wurde das extraterritoriale Defizit von RIPA explizit problematisiert (Intelligence and Security Committee, 2014e, S. 141f.).

könnte so Autokratien inspirieren und dazu genutzt werden, diese Praktiken zu legitimieren.

Damit wurde auch auf internationaler Ebene Kritik vorgetragen, die die britische Regierung aber bereits domestisch nicht daran gehindert hatte, Dienstleister dazu zu verpflichten, Möglichkeiten zur Entschlüsselung vorzuhalten. Die britische Exekutive hat in der Folge wiederholt versucht andere Staaten von dieser Praxis zu überzeugen und dabei im Kreis der 5-Eye-Staaten die meisten Fortschritte erzielt. Die Gruppe ruft seit mehreren Jahren regelmäßig zu einem restriktiveren Umgang mit Verschlüsselung auf.

Die deutlich kritischere Position gegenüber Verschlüsselung, die domestisch etabliert werden konnte, ermöglichte der britischen Regierung auch im Außenverhalten einen offensiveren Umgang mit der Thematik. Insbesondere zu dem Zeitpunkt als auch innenpolitisch über den IPA verhandelt wurde und nachdem sich eine Erweiterung der Beschützer-Rolle realisierte hatte, intensivierte die britische Regierung auch international ihre Bemühungen, Verschlüsselung stärker zu reglementieren. Im Rahmen der Five-Eyes problematisierte die britische Regierung zusammen mit den Partnerstaaten nach 2016 wiederholt die verschlüsselte Kommunikation. In einem gemeinsamen Kommuniqué machten die RegierungsvertreterInnen 2016 deutlich, dass sie Verschlüsselung zwar als wichtig für die Bürgerrechte im digitalen Zeitalter ansahen, aber gleichzeitig befürchteten, dass die Technik die Strafverfolgungsbehörden zunehmend bei ihrer Arbeit beeinträchtigen könnte (U.S. Department of Homeland Security, 2016). Die Regierungen befürchteten ein unausgeglichenes Verhältnis zwischen einem liberalen und unregulierten Internet und den nationalen Beschützer-Rollen, das maßgeblich durch die Verschlüsselung erzeugt werde.

Diese Sorgen wurden ein Jahr später konkreter formuliert und von Versuchen begleitet, zusammen mit den entsprechenden Dienstleistern, Möglichkeiten zum Umgang mit diesem Problem zu finden (Government of Canada, 2017). Die technische Community war aber nicht zu einer umfassenden Kooperation mit den Regierungen bereit, da sie die Einschätzung vertrat, dass eine Schwächung von Verschlüsselung die IT-Sicherheit des gesamten Netzes gefährden könnte und so sowohl aus bürgerrechtlicher als auch wirtschaftlicher Sicht nicht angemessen sei. Die Regierungen der 5-Eyes mussten auch 2018 eine mangelnde Kooperationsbereitschaft der Digitalwirtschaft akzeptieren. Führende UnternehmensvertreterInnen hatten es abgelehnt, an Gesprächen über die terroristische oder kriminelle Nutzung von Onlinekommunikationsräumen teilzunehmen (Australian Government, 2018).

Da die Bestrebungen des Geheimdienstverbundes in der Netzgemeinde nicht aufgegriffen wurden, formulierten die 5-Eyes 2018 eigene Prinzipien zur Verschlüsselung. Hierin vertraten die Regierungen die Position, dass:

> »Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution. Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute.« (Ebd.)

Die Regierungen akzeptierten in ihrer Erklärung, dass es Fälle geben könne, in denen eine Entschlüsselung technisch unmöglich sei. Dies sollten aber Ausnahmen bleiben und um dies zu gewährleisten, riefen sie die Internetunternehmen zur freiwilligen, nationalen wie internationalen Kooperation mit den Ermittlungsbehörden auf. Die Unternehmen sollten in diesem Kontext freiwillig eigene Konzepte zur Überwachung von Kommunikation erarbeiten. Weiterhin betonten sie, dass der Zugriff auf kryptierte Daten nur unter Einhaltung rechtsstaatlicher Prozesse und unter Wahrung der bürgerlichen Freiheitsrechte erfolgen dürfe. Sie verliehen damit den Bestrebungen Ausdruck, die Beschützer-Rolle durch die Rolle als Garant liberaler Grundrechte einzuhegen.

Zum Abschluss machten die Regierungen aber auch deutlich, dass sie Einschränkungen ihrer sicherheitspolitischen Handlungsfähigkeit aufgrund technischer Hürden nicht dauerhaft tolerieren würden:

> »Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.« (Ebd.)

Eine Position, die die britische Regierung domestisch bereits mit dem IPA eingenommen hatte. 2019 erneuerten die fünf angelsächsischen Regierungen ihre Forderungen nach mehr Kooperation mit der Wirtschaft. Allerdings wiesen sie auch darauf hin, dass andere Unternehmen gezielt nur solche Technologien einsetzten, die sie selbst nicht mehr entschlüsseln könnten. Dieses Vorgehen wurde von den Regierungen als fahrlässig und riskant für die Gesellschaften gesehen (UK Government, 2019c, S. 2f.). Auch auf Ebene der Vereinten Nationen wies die britische Regierung immer wieder auf die Risiken hin, die aus ihrer Sicht mit einer weitgehenden Verbreitung nicht dekryptierbarer Verschlüsselung einhergeht (UK Government, 2017b).

Ebenfalls Ende 2018 hatten Vertreter des GCHQ in einem Lawfare-Gastbeitrag zwar betont, dass Verschlüsselung sowohl aus wirtschaftlicher als auch bürgerrechtlicher Perspektive bedeutend sei und dass Eingriffe nur unter strengen Auflagen durchgeführt werden dürften. Der IPA biete aus ihrer Sicht »world class oversight«, um diese Maßnahmen zu kontrollieren (Levy und Robinson, 2018). Um mit Verschlüsselung umzugehen, ohne sie zu brechen, brachten sie den Vorschlag ein,

bspw. bei Ende-zu-Ende verschlüsselten Messengern Nachrichtendienste als unsichtbare dritte Partei in die Kommunikation zwischen Verdächtigen einzubinden und so ein Abhören möglich zu machen. Dies könnten die Betreiber der Dienste ohne Probleme implementieren und die Verschlüsselung werde hierdurch nicht systematisch unterminiert (Levy und Robinson, 2018). Im Mai 2019 reagierten VertreterInnen der Netzgemeinde, Wissenschaft und Wirtschaft in einem offenen Brief auf diese Vorschläge. Sie betonten, dass der Vorschlag sowohl bürgerrechtlich als technisch problematisch sei. Eine Implementierung des »ghost protocols« unterminiere das Vertrauen in Authentifizierungsprozesse wodurch grundlegend infrage gestellt wäre, mit wem kommuniziert würde. Weiterhin müssten sämtliche Applikationen angepasst werden, um zu verhindern, dass die mitlesende Partei für KommunikationsteilnehmerInnen sichtbar würde. Hierdurch könnten neue Sicherheitslücken entstehen, die dann alle NutzerInnen beträfen (Access Now, 2019).

Aus der Netzgemeinde gab es vehemente Kritik an all diese Forderungen. Die Electronic Frontier Foundation sah in den Bestrebungen der 5-Eyes einen Export der britischen Überwachungspolitik und eine Aushöhlung der Bürgerrechte im Netz (EFF, 2017). In einem offenen Brief an die RegierungsvertreterInnen formulierten 83 Bürgerrechtsorganisationen und VertreterInnen der Netzgemeinschaft aus verschiedenen Ländern ihre Kritik an den Forderungen. Sie riefen die Staaten dazu auf:

> »[…] to protect the security of your citizens, your economies, and your governments by supporting the development and use of secure communications tools and technologies, by rejecting policies that would prevent or undermine the use of strong encryption, and by urging other world leaders to do the same.« (Human Rights Watch, 2017, S. 1)

Pläne, wodurch Hintertüren in Verschlüsselung vorgesehen werden müssten, waren aus Sicht der UnterzeichnerInnen schädlich für die Sicherheit im Netz allgemein. Diese Ansicht bekräftigten die KritikerInnen mit dem utilitaristischen Hinweis, dass Verschlüsselung sehr viel mehr Positives als Negatives ermögliche und dass Kriminelle und Terroristen im Extremfall immer auf Software zurückgreifen könnten, die außerhalb des Einflussbereichs der 5-Eye-Staaten liege (ebd., S. 2). Der Verweis aus der Netzgemeinde, dass das Netz selbst ein schützenswertes Gut sei und dass die staatliche Beschützer-Rolle ein sicheres Netz durch Eingriffe in Verschlüsselung oder das Zurückhalten von Schwachstellen unterminiere, wurde in verschiedenen Kontexten cybersicherheitspolitischer Debatten angeführt. Diese Bezüge blieben aber folgenlos, da die Regierung das Netz selbst als Schutzgut nicht prinzipiell anerkannte, sondern die Beschützer-Rolle auf die nationalen Systeme bezogen blieb.

Wie bei der Etablierung des domestischen Rechtsrahmens, zeigt sich auch in diesem Kontext, dass der britischen Regierung aufgrund ausbleibender Kontestationen eine umfassendere Rollenübernahme erleichtert wurde. In der domestischen Sphäre zeigt sich das daran, dass die Herausforderungen mit Verweis auf die Rolle als Garant liberaler Grundrechte nicht so folgenreich waren wie in der Bundesrepublik – auch aufgrund eines ausbleibenden negativen historischen Selbstbezugs. Die britische Regierung konnte daher stets eine striktere Kryptopolitik verfolgen als das deutsche Pendant. Diese ermöglichte auch eine verschlüsselungskritischere Rollenübernahme nach außen, die dort bei den signifikanten Anderen im 5-Eye-Verbund anschlussfähig war. Die Bestrebungen der Gruppe, eine technische Begrenzung der Beschützer-Rolle durch die rasche Verbreitung von (Ende-zu-Ende-)Verschlüsselung zu vermeiden, wurden stets durch die britische Regierung unterstützt.

4.2.3 Internationalisierung: Strafrechtliche Harmonisierung

Wie die Bundesrepublik, gehörte auch das Vereinigte Königreich 2001 zu den ersten Unterzeichnern der Convention on Cybercrime des Europarates. Forderungen nach internationaler Kooperation zur Bekämpfung von Cyberkriminalität wurden in Großbritannien aber bereits in den frühen 1990er Jahren laut.

> »Of couse [sic!], computer crime is often international crime. It is all very well for us to have an effective law in Britain, but we must ensure that similar laws exist in other major countries. The really serious criminal activities are likely to be netted through international co-operation across frontiers rather than by laws which are limited to activities in Britain.« (House of Commons, 1990b, S. 1147)

Die Limitationen einer territorial gebundenen Beschützer-Rolle wurden in diesem Kontext bereits früh problematisiert. Die Regierung erkannte in der Konvention dann einerseits eine Möglichkeit, die britischen Ambitionen im Kampf gegen Cyberkriminalität international zu dokumentieren und andererseits von der verbesserten Kooperation der unterzeichnenden Staaten zu profitieren (Foreign & Commonwealth Office, 2011). Ferner wurde die Konvention als Mittel zum Schutz der Digitalwirtschaft gesehen, da auf diesem Weg das Vertrauen der VerbraucherInnen gestärkt werden könne (Ofcom, 2009). Die internationale Harmonisierung der Beschützer-Rolle wurde damit durch das katalytische Zusammenspiel mit der Rolle als Wohlstandsmaximierer ermöglicht.

Ratifiziert wurde die Konvention aber erst 2011 als mit dem Police & Justice Act 2006 und dem Serious Crime Act 2007 alle erforderlichen Vorgaben umgesetzt waren (Foreign & Commonwealth Office, 2010). Mit diesen Gesetzen wurde einerseits die Strafbarkeit für DoS-Angriffe etabliert und andererseits das Strafmaß

für den Zugriff auf IT-Systeme angeglichen. Die gesetzliche Weiterentwicklung wurde dabei aber nur begrenzt durch die internationalen Vorgaben der Konvention und des Rahmenbeschlusses 2005/222/JI ermöglicht (Home Office, 2004). Zunächst wurden Ergänzungen des CMA durch domestische Entwicklungen angestoßen.

Da der Computer Misuse Act eine direkte Reaktion auf den Angriff von Schifreen und Gold war, adressierte er zunächst nicht alle Teilaspekte der IT-Sicherheit. Insbesondere die Strafbarkeit der Beeinträchtigung der Verfügbarkeit von Daten war zunächst noch nicht im Gesetz angelegt. Diese Regulierungslücke wurde durch den Terrorism Act 2000 für terroristische Vergehen geschlossen (The Stationery Office, 2000c). Für kriminelle Angriffe blieb das Defizit aber bestehen. Bereits 2002 wurde zwar im Parlament eine Erweiterung des CMA um DoS-Angriffe debattiert, der Vorschlag (der wieder als private member's bill eingebracht wurde) konnte aber keine Mehrheit im Parlament finden und blieb daher folgenlos (House of Lords, 2002a). Dies ist bemerkenswert denn zu diesem Zeitpunkt war Großbritannien bereits Unterzeichner der Europaratskonvention on Cybercrime. Die daraus folgende Notwendigkeit, auch DoS-Angriffe unter Strafe zu stellen, wurde auch im House of Lords betont. Ferner war absehbar, dass der Rahmenbeschluss 2005/222/JI empfehlen würde, ein Vergehen für derartige Vorfälle einzuführen. Bei einer Begutachtung des CMA durch das Internet Crime Forum der All Party Internet Group wurden diese Aspekte wiederum aufgeworfen (Home Office, 2004). Auch im Parlament wurde in diesem Kontext darüber diskutiert. Letztlich führten diese Debatten aber nicht unmittelbar zu einer gesetzlichen Anpassung (House of Lords, 2002b, S. 981). Während der Rahmenbeschluss bzw. die Europaratskonvention in Deutschland gesetzliche Anpassungen ermöglicht hat, wurde die britische Beschützer-Rolle durch einen domestischen Vorfall weiterentwickelt.

Im Jahr 2004 wurde deutlich, dass für Kriminelle die DoS-Regulationslücke nach wie vor offen stand. Ein Angeklagter wurde in erster Instanz für den massenhaften Versand von E-Mails und die daraus resultierende Überlastung eines Mailservers freigesprochen, da das Gericht in diesem Verhalten kein Vergehen nach dem Computer Misuse Act erkannte. Mit Blick auf kriminelle DoS-Angriffe bestand daher noch immer Regulierungsbedarf (Fafinski, 2006). Mit dem Police and Justice Act wurde dieses Defizit adressiert und ein neuer Straftatbestand im CMA etabliert, der auch die Beeinträchtigung von IT-Systemen unter Strafe stellte und damit auch den Anforderungen aus der Europaratskonvention und dem EU-Rahmenbeschluss gerecht wurde. Wie in Deutschland, schuf auch die britische Regierung in diesem Zuge einen Tatbestand für die Bereitstellung von Software, die Angriffe gegen Computersysteme ermöglicht (The Stationery Office, 2006, Section 3 bzw. 3a).

Während der Rahmenbeschluss 2005/222/JI noch zu keinen größeren Anpassungen der Beschützer-Rolle führte, wurde die Richtlinie 2013/40/EU umfassend

im Parlament diskutiert, da die Regierung beschlossen hatte, sich in diesem Kontext der EU-Regelung anzuschließen (opt-in) (House of Commons, 2011a, S. 1051).[10] Die Notwendigkeit internationaler Kooperation wurde in dieser Debatte besonders betont, »because the problem is an international one and online criminals do not respect international borders« (ebd., S. 1051). Der Opt-In wurde in diesem Kontext als Ausdruck des britischen Bemühens gesehen, den internationalen Kampf gegen Cyberkriminalität entschlossen zu führen. Ferner würden auf diesem Weg potenzielle Rückzugsorte für Kriminelle verschlossen, da alle Mitgliedsstaaten einen gesetzlichen Mindeststandard einhalten müssten (ebd., S. 1051). Die Regierung konstatierte daher:

> »The aims of the directive are consistent with the aims of the Government in protecting our country, our economy, our businesses and our citizens from those who seek to misuse the online environment.« (Ebd., S. 1052)

Diese Postion wurde im Parlament auch von den Abgeordneten der Opposition geteilt, die das Vorhaben grundsätzlich unterstützten. Allerdings wiesen KritikerInnen darauf hin, dass die britische Regierung die Entscheidung zum Opt-in zu spät getroffen habe und dass dadurch die Gestaltungsmöglichkeiten für Großbritannien begrenzt seien. Ferner wurde betont, dass eine europaweite Regulierung zwar wünschenswert sei, dass diese aber der Kooperation mit anderen Commonwealth-Staaten oder den USA nicht im Wege stehen dürfe. Die britische Regierung dürfe durch die Richtlinie nicht in ihrer Souveränität eingeschränkt werden, weitere Abkommen zu schließen (ebd., S. 1055 f.). Für die britische Regierung war es also bedeutsam, die Beschützer-Rolle möglichst unabhängig zu definieren. Die EU wurde zwar als wichtiger signifikanter Anderer anerkannt und die Richtlinie 2013/40/EU wurde übernommen. Es war aber stets bedeutsam, dass die Kooperation mit anderen Partnern hierdurch nicht negativ beeinflusst würde. Die souveräne Verfügung über die eigene Beschützer-Rolle sorgt damit dafür, dass diese aus britischer Sicht nicht delegiert werden kann.

Während in Deutschland ein weitgehend unkontrollierter Datenaustausch von digitalen Beweismitteln, wie er derzeit in der EU im Rahmen eine E-Evidence-Richtlinie debattiert wird, aufgrund der begrenzenden Wirkung der Rolle als Garant liberaler Grundrechte kritisch gesehen wird, begann die Regierung des Vereinigten Königreichs offensiv damit über extraterritoriale Abhör- und Entschlüsselungsanordnungen zu verhandeln. Insbesondere mit den USA wurde in diesem Kontext über erleichterte Kooperationsmodi gesprochen, die nicht auf

10 Mit dem Vertrag von Amsterdam 1997 hat sich die britische Regierung das Recht zusichern lassen, darüber zu entscheiden, ob sich das Vereinigte Königreich Regelungen im Bereich Freedom, Security and Justice unterwirft (opt-in) oder nicht (opt-out). Diese Regelung besteht auch nach dem Vertrag von Lissabon weiter (House of Commons, 2011b).

den mitunter langfristigen Wegen der Rechtshilfeverträge beruhen (Washington Post, 2016).

Hier zeigt sich, dass die domestisch weniger stark herausgeforderte Beschützer-Rolle in Großbritannien auch im Außenverhalten eine expansivere Rollenübernahme ermöglicht. Der fehlende Kontestationsmechanismus des negativen historischen Selbstbezugs sowie die Referenz (Schutz vor wem?) auf den domestischen Terrorismus erlaubte der britischen Regierung domestisch bereits früher höhere Strafmaße, eingreifendere Ermittlungsbefugnisse und weitreichendere Maßnahmen nach außen zu fordern. Dies wird bei dem folgenden Blick auf die Etablierung der domestischen Beschützer-Rolle deutlich. Weiterhin hat die Regierung, aufbauend auf die domestische Beschützer-Rolle, Kooperationen mit den USA geschlossen.

4.2.4 Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle

Die britische Regierung begann schon früher als die deutsche damit, die Beschützer-Rolle mit offensiven Mitteln zur Strafverfolgung auszustatten. Dies führte aufgrund der historischen Erfahrungen mit Terrorismus aber zu weniger intensiven Kontestationsprozessen, so dass die Regierung die Rolle einfacher stabilisieren konnte.

Mit dem Police Act 1997 wurde im Vereinigten Königreich bereits früh die Grundlage dafür gelegt, Polizeibehörden den Zugriff auf IT-Systeme zu gewähren. Section 93 erlaubt den ErmittlerInnen »interference with property or with wireless telegraphy […]« (The Stationery Office, 1997). Diese Befugnis war anwendbar, wenn zur Prävention oder Aufklärung schwerer Straftaten andere Ermittlungsmethoden nicht ausreichend waren. In den Debatten um den Police Act standen die digitalen Ermittlungsmethoden aber noch nicht im Zentrum der Aufmerksamkeit. Dennoch verwies die britische Regierung zur Legitimierung von Eingriffen in IT-Systeme immer wieder auf diese Regelung (UK Government, 2016c).[11] Im Parlament rekurrierte die Regierung zur Rechtfertigung des Police Acts explizit auf die gesellschaftliche Bedrohung durch (domestischen) Terrorismus. Diese Referenzen wurden auch von vielen Abgeordneten der Opposition geteilt.

> »We know from reading newspapers, watching television and listening to the radio how an increasing threat of crime affects the lives of more and more of our citizens. At the same time, there is no doubt that we have to be conscious

11 Während die Praxis des polizeilichen Eingriffs in IT-Systeme im Police Act 1997 noch als property interference bezeichnet wurde, änderte sich die Bezeichnung später zu *Equipment Interference*.

> of the return of a terrorist threat to this country.« (House of Commons, 1997, S. 379)

Diese Bedenken bezüglich terroristischer Gefahren wurden auch im House of Lords wiederholt geäußert und zur Rechtfertigung der neuen Kompetenzen herangezogen (House of Lords, 1997, S. 412 bzw. 426). Die Anordnung der property interference oblag dabei leitenden BeamtInnen der Strafverfolgungsbehörden, sodass eine richterliche Kontrolle nicht vorgesehen war. Dies sorgte insbesondere bei Bürgerrechtsbewegungen für Kritik. Eine frühe Referenz (Schutz vor wem?) auf den domestischen und internationalen Terrorismus ermöglichte es der britischen Regierung aber schon früh, polizeiliche Befugnisse zum Eingriff in IT-Systeme zu etablieren. Der Widerstand gegen diese neuen Ermittlungsmethoden fokussierte sich hauptsächlich darauf, die Bürgerrechte angemessen zu schützen (House of Commons, 1997, S. 387 bzw. 392). Allerdings wurde in den Debatten nicht über die informationstechnischen Möglichkeiten der neuen Befugnisse debattiert, sodass deren Implikationen erst wesentlich später öffentlich bekannt wurden. Denn erst zwanzig Jahre nach Verabschiedung des Police Acts bekannte die Regierung, dass Polizeibehörden unter dieser Ermächtigung Eingriffe in IT-Systeme vornahmen.

Im Gegensatz zu Deutschland wurde der Analogieschluss aus der bestehenden polizeilichen Praxis auch nicht substanziell herausgefordert und durch Gerichte untersagt. Bürgerrechtsorganisationen wiesen in einer intensiven Debatte um staatliches Hacking 2016 (s.u.) aber auf die problematische Rechtsgrundlage hin und vertraten die Position, dass ein polizeiliches Eingreifen in IT-Systeme durch den Police Act nicht gedeckt sei (Liberty, 2016b, S. 5). Wie in Deutschland trat auch in Großbritannien die Beschützer-Rolle in Spannung mit der Rolle als Garant liberaler Grundrechte. Durch den anderen historischen Selbstbezug als Opfer von Terrorismus wurden die Maßnahmen aber nicht grundlegend hinterfragt bzw. abgelehnt.

1999 konstatierte die Regierung unter Tony Blair, dass die rasche technologische Entwicklung die bestehenden Regelungen zum Abfangen von Kommunikation vor neue Herausforderungen stelle. »This revolution in communications technology is one of the imperatives for change in the law« (UK Government, 1999, Foreword). In einem Konsultationspapier argumentierte die Regierung, dass TerroristInnen und Kriminelle die neuen Möglichkeiten nutzten und dass daher eine Novellierung insbesondere des Interception of Communications Act 1985 (IOCA) nötig sei. Das Innenministerium identifizierte Handlungsbedarf bspw. mit Blick auf den wachsenden E-Mailverkehr, der effizienter bei den Internet Service Providern (ISP) abgefangen werden könne und der nicht notwendigerweise über einen Public Telecommunication Operator geleitet wird. Folglich sollten auch ISPs zur Kooperation beim Abfangen von Daten verpflichtet werden. Hierfür war aber eine

Neufassung des Gesetzes nötig (UK Government, 1999, S. 14 bzw. 17). Die Regierung beabsichtigte damit die Regelungen des IOCA signifikant zu erweitern:

> »The intention is to provide a single legal framework which deals with all interception of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted. This means that the scope of the Bill will be wider than that of the Interception of Communications Act 1985 [...]« (Ebd., S. 16)

Der Innenminister betonte in diesem Kontext aber stets auch, dass hierbei die Bürgerrechte gewahrt werden würden (ebd.).

Vor diesem Hintergrund etablierte die Regierung mit dem Regulation of Investigatory Powers Act 2000 (RIPA) neue Regelungen, die den Polizeibehörden das Abfangen von Kommunikationsinhalten erlaubten. RIPA regelte Kompetenzen in sechs unterschiedlichen Bereichen neu: »the interception of communications; the acquisition of communications data; intrusive surveillance; directed surveillance; the use of covert human intelligence sources; and demands for decryption« (House of Commons, 2000d, S. 768). Neben den bereits debattierten Kompetenzen zur Entschlüsselung, waren mit Blick auf Informationstechnik und das Internet die Maßnahmen zum Abfangen von Kommunikation einschlägig, da es sich hierbei um Praktiken handelte, die besonders mit Blick auf die neuen Kommunikationswege etabliert wurden. Hierbei handelte es sich um Eingriffe in die Kommunikationsübertragung, die die Inhalte für Strafverfolgungsbehörden zugänglich macht (The Stationery Office, 2000b, Section 2 (2)).

Section 5(3) von RIPA erlaubte der/dem zuständigen MinisterIn mit Verweis auf drei Gründe, Anordnungen zum Abfangen von Kommunikation zu erlassen: die Nationale Sicherheit, die Aufklärung oder Verhinderung schwerer Kriminalität sowie den Erhalt des wirtschaftlichen Wohlergehens des Vereinigten Königreichs. Die/Der MinisterIn muss hierbei abwägen, ob die Maßnahme verhältnismäßig ist und ob die Informationen nicht auch auf anderem Weg erlangt werden könnten. Über die Anordnung oder die Beendigung der Maßnahme ist sodann ein/e Surveillance Commissioner zu informieren. Diese/r prüft die Anordnung und gibt sie frei, sofern sie/er sie für rechtmäßig hält. Beantragen können solche interception warrants die LeiterInnen der Geheimdienste sowie der übergeordneten Polizeibehörden bzw. des Zolls und National Criminal Intelligence Service (ebd., Section 6 (2)). Um die Kommunikationsinhalte abzufangen, können durch die Anordnungen auch Dritte (die Telekommunikationsanbieter) zur Kooperation verpflichtet werden. Sie sind dazu verpflichtet, alle Maßnahmen zu ergreifen, die »reasonably practicable« sind (ebd., Section 11 (6)). Ferner werden die Unternehmen verpflichtet, den Inhalt sowie die Existenz der Überwachungsanordnung geheim zu halten (ebd., Section 19 (3)).

In diesem Kontext zeigt sich erneut die enge, katalytische Verbindung zwischen der Beschützer-Rolle und der Rolle als Wohlstandsmaximierer. Denn die Eingriffsrechte beziehen sich nicht nur auf sicherheitspolitische Erwägungen, sondern können auch aus wirtschaftlichen Gründen erfolgen.

Die durch die/den MinisterIn ausgestellten Anordnungen zum Abfangen der Kommunikation wurden vom neu etablierten Interception of Communications Commissioner geprüft. Dieser wurde durch den Premierminister bestellt und musste zuvor ein hohes juristisches Amt bekleidet haben (ebd., Section 57). Zusätzlich etablierte RIPA mit dem Investigatory Powers Tribunal (IPT) ein neues Gericht, das die mit dem Gesetz verbundenen Kompetenzen und deren Angemessenheit mit Blick auf die Bürgerrechte überwachen sollte (ebd., Section 65).

Die Regierung verwies zur Rechtfertigung der Neuregelungen durch RIPA neben den neuen Gefahren der kriminellen und terroristischen Nutzung der neuen Kommunikationswege auch darauf, dass das Gesetz keine grundsätzlich neuen Befugnisse schaffe, sondern lediglich bestehende Regeln zusammengeführt würden, um dem technischen Wandel angemessen begegnen zu können. Ferner profitiere hiervon auch der Grundrechtsschutz der betroffenen BürgerInnen. Mit RIPA werde auch den Vorgaben des Human Rights Acts 1998 entsprochen. Wiederholt versicherte Home Secretary Jack Straw, dass eine angemessene Balance zwischen den Kompetenzen der Ermittlungsbehörden und den Bürgerrechten hergestellt werde (House of Commons, 2000d, S. 767).[12]

Eine Überarbeitung der bestehenden Regelungen war aus Sicht der Regierung aber unter anderem zur Bekämpfung von Geldwäsche, Menschenhandel, Pädophilie, Zigarettenschmuggel und anderen Delikten notwendig (ebd., S. 768). Prinzipiell stimmte die Tory-Opposition der Einschätzung der Regierung zu, dass der IOCA angesichts technischer Entwicklungen überarbeitet werden müsse, um die Sicherheit der britischen Bevölkerung nach wie vor zu gewährleisten. Auch die Erweiterung der Beschützer-Rolle auf die Überwachung der neuen Kommunikationswege wurde akzeptiert (ebd., S. 778). Die Liberal Democrats unterstützten das Gesetz letztlich ebenfalls. Auch sie wiesen auf die besonderen Gefahren hin, die durch die Verbreitung der Informationstechnik ermöglicht würden und betonten die Verantwortung des Parlaments, die britischen BürgerInnen zu schützen:

12 1998 wurde der Human Rights Act (HRA) beschlossen, um die Rechte aus der Europäischen Menschenrechtskonvention in britisches Recht zu übertragen. Der HRA stellt aber auch sicher, dass Akte der Primärgesetzgebung nicht durch Urteile außer Kraft gesetzt werden können. Gerichten bleibt nur die Formulierung einer Erklärung der Inkompatibilität, die aber keine Auswirkung auf die bestehenden britischen Gesetze hat (The Stationery Office, 1998). Der HRA wurde wiederholt kritisiert und immer wieder wurde auch über eine britische Bill of Rights als Alternative bzw. Ergänzung debattiert (House of Lords und House of Commons, 2008).

> »[…] we must ensure that serious threats to the physical safety of the people of this country, whether from criminals, hostile powers or terrorists, can be countered by the judicious and regulated use of such powers. We must do so in a way that does not disrupt an industry that has great earning power for the country and potential for the future.« (House of Commons, 2000b, S. 1206)

Diese Einschätzung teilten auch die meisten Labour-Abgeordneten. Die Referenz auf Terrorismus bzw. die Anschlagsfolgen, die Großbritannien bereits erfahren hat, wurden überparteilich geteilt. In diesem Kontext wurde ferner betont, dass die britische Bevölkerung kein Verständnis dafür aufbringen würde, wenn die erforderlichen Maßnahmen zur Prävention solcher Angriffe nicht ergriffen würden (bspw. House of Commons, 2000d, S. 784f.).

Der Ausbau der Beschützer-Rolle wurde daher maßgeblich durch das historische Selbst ermöglicht. Sowohl Regierung als auch Opposition fürchteten im Falle erneuter Terroranschläge, dafür verantwortlich gemacht zu werden, diese nicht verhindert zu haben.

RIPA erfuhr aber von Seiten der Zivilgesellschaft und von VertreterInnen der Internetwirtschaft Kritik. Wirtschaftliche Einwände gegen das neue Gesetz betonten, dass durch die Neuregelung auch kleinere ISPs zur Kooperation beim Abhören von Kommunikation verpflichtet seien. Dies könne mit empfindlichen Kosten verbunden sein, die die Unternehmen nur schwer tragen könnten (ebd., S. 779 f.). Kritik an den potenziellen Kosten und entsprechende Forderungen nach Kompensation für die betroffenen Unternehmen wurde sowohl von Branchenverbänden als auch Tory-Abgeordneten formuliert (House of Commons, 2000c).

Von den Liberal Democrats wurde wiederholt negativ hervorgehoben, dass keine transparente und unabhängige richterliche Kontrolle der Maßnahmen vorgesehen wurde (House of Commons, 2000b, S. 1206). Zwar wurde mit dem IPT ein neues Kontrollgremium etabliert, das die zuvor für unterschiedliche Behörden zuständigen Kontrollinstanzen ersetzte (das Interception of Communications Tribunal, das Security Service Tribunal und das Intelligence Services Tribunal), bemängelt wurde aber die Intransparenz und insbesondere der Umstand, dass keine Auskünfte zu Überwachungsmaßnahmen veröffentlicht werden sollten. Auch dass unter dem Freedom of Information Act 2000 keine weiteren Informationen angefordert werden konnten, wurde in diesem Kontext kritisiert (JUSTICE, 2000). Die Regierung argumentierte, dass Offenlegungen dazu führen könnten, tatsächlich Überwachte zu warnen und so Maßnahmen zu gefährden:

> »It is logically a difficult position to explain to individuals, and it is difficult for people to understand that they may make a complaint to the tribunal […] that they may be being intercepted even though it is not possible to tell them whether they are being intercepted. Because it is secret, people are bound to

> be suspicious, but—to repeat the point [...] the powers are operated in a strong ethical and legal framework.« (House of Commons, 2000d, S. 774)

Letztlich führte die Sorge vor Terroranschlägen mit Verweis auf die historischen Erfahrungen dazu, dass RIPA rasch durch das Parlament verabschiedet wurde. Das Gesetz wurde in der Folge wiederholt zum Ziel bürgerrechtlicher Kritik. Erst als durch die Enthüllungen von Edward Snowden 2013 staatliche Überwachungspraktiken öffentlich bekannt wurden, kam es zu einer Überarbeitung der Regelungen. 2014 wurde auch eingehend darüber diskutiert, dass die Regelungen genutzt wurden, um gezielt journalistische Quellen zu identifizieren und abzuhören (The Guardian, 2014c). Aus rollentheoretischer Perspektive transportierte diese Kritik den Vorwurf, die Exekutive habe die Beschützer-Rolle im Geheimen deutlich überdehnt. Unter diesem wachsenden domestischen wie internationalen Druck, legte die Regierung den Investigatory Powers Acts 2016 (IPA) vor.

Mit dem IPA wurde explizit über die Thematik staatlichen Hackens diskutiert. In diesem Kontext bekannte die britische Regierung auch erstmals, dass staatliche Eingriffe in IT-Systeme zu den gängigen Ermittlungspraktiken der Polizeibehörden zählten. Der IPA sollte den kurz nach den Snowden-Veröffentlichungen erlassenen Data Retention and Investigatory Powers Act 2014 ablösen, der aufgrund einer sunset-clause auszulaufen drohte. Mit dem IPA etablierte die Regierung neue Kompetenzen der Strafverfolgungsbehörden unter dem Begriff *Equipment Interference* erstmals explizit und sorgte dafür, dass die Regelungen aus dem Police Act nur noch eingeschränkt für den Eingriff in Computersysteme genutzt werden konnten (The Stationery Office, 2016, Section 14). Zur Rechtfertigung der Eingriffe verwies die Regierung darauf, dass aufgrund des technischen Wandels und insbesondere der voranschreitenden Nutzung von Verschlüsselung, Informationen nur noch auf diesem Weg zugänglich seien:

> »Equipment interference plays an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption. It can sometimes be the only method by which to acquire the data.« (UK Government, 2016b, S. 23)

Diese jetzt explizit gemachte und durch den IPA gestützte Praxis sorgte im Rahmen eines öffentlichen Konsultationsprozesses für erhebliche Kritik. KritikerInnen wiesen darauf hin, dass die neuen Befugnisse nicht nur in Form eines Code of Conduct formuliert werden sollten, sondern dass es einer eigenen gesetzlichen Grundlage für derart invasive neue Kompetenzen geben sollte. Ferner bemängelten Bürgerrechtsbewegungen, dass der Eingriff in Systeme grundlegend die IT-Sicherheit unterminiere (Home Office, 2015c). Auch Bemühungen der Polizei, Schadsoftware auf dem freien Markt zu erstehen und sich damit bei der Aus-

übung der Beschützer-Rolle von Unternehmen wie Hacking Team abhängig zu machen, wurden scharf kritisiert (Liberty, 2016b, S. 5).

Im Gegensatz zur deutschen Politik, ist die Beschützer-Rolle in Großbritannien in diesem Kontext weniger spezifisch. Während in Deutschland zwischen den unterschiedlich intrusiven Praktiken der Online-Durchsuchung bzw. Quelle-TKÜ. unterschieden wird, gibt es im Vereinigten Königreich nur Regeln zur Equipment Interference. Allerdings gibt es auch hier Unterschiede in den Anordnungsanforderungen je nachdem, ob es sich um »live« mitgeschnittene oder gespeicherte Daten handelt. Für Kommunikation, die auf dem Transportweg abgefangen werden soll, bedarf es einer eigenen interception warrant (Home Office, 2018a, S. 12). Equipment Interference darf auch zur Überwachung eingesetzt werden. Das beinhaltet »monitoring, observing or listening to a person's communications or other activities, or recording anything that is monitored, observed or listened to.« (ebd., S. 13)

Die Regierung definierte die Kompetenzen zur Equipment Interference im IPA folgendermaßen:

> »Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information from equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment.« (Ebd., S. 10)

Equipment Interference umfasst damit eine Reihe verschiedener Praktiken, die es den Ermittlungsbehörden (im Geheimen) erlauben, Zugriff auf gespeicherte Daten zu erlangen. Sie reichen vom physischen Zugriff bis zur Ausnutzung von Softwareschwachstellen. In diesem Kontext sicherte die Regierung aber auch zu, dass die neuen Kompetenzen mit dem 1998 verabschiedeten Human Rights Act konform gestaltet würden (ebd., S. 10f.). Im Gegensatz zu den Geheimdiensten ist es den Polizeibehörden bspw. nur erlaubt targeted Equipment Interference einzusetzen. Den Geheimdiensten steht daneben die umfassendere bulk Equipment Interference offen (ebd., S. 67).

Mit dem IPA wurde den Ermittlungsbehörden die Befugnis zur Equipment Interference zur Aufklärung und Prävention schwerer Kriminalität erteilt. Ferner erlaubt der IPA den Polizeien den Eingriff, wenn dadurch der Tot oder die physische bzw. mentale Gesundheit von Personen geschützt werden kann (ebd., S. 24). Die Anordnung der Equipment Interference obliegt bei den Polizeibehörden einer/einem leitender/n Beamtin/en (law enforcement chief). Außer in besonders dringenden Fällen ist zudem die vorherige Genehmigung durch einen Judicial Commissioner nötig. Besonders akuter Handlungsbedarf liegt vor, wenn bspw. eine unmittelbare Gefahr für Leib und Leben besteht oder wenn für die Informationsbeschaffung nur ein kleines Zeitfenster offen ist. Die Anordnung muss

aber spätestens nach drei Werktagen durch einen Judicial Commissioner überprüft und bestätigt werden (ebd., S. 51). Wenn zur Ausübung der Beschützer-Rolle die staatlichen Kapazitäten nicht ausreichen und daher ein Telekommunikationsdienstleister zur Kooperation verpflichtet wird, bedarf es einer ministeriellen Anordnung (ebd., S. 48). Bei der Genehmigung der Equipment Interference muss stets abgewogen werden, ob die gleichen Informationen nicht auch durch weniger invasive Maßnahmen gewonnen werden können. Nur wenn dies nicht der Fall ist, ist die Maßnahme gerechtfertigt (ebd., S. 45).

Ähnlich wie in Deutschland sind die besonders invasiven Maßnahmen der Beschützer-Rolle damit an besonders schützenswerte Güter (Leib und Leben) gebunden und durch demokratische Kontrollinstanzen eingehegt. Auf diesem Weg versuchte die britische Regierung die Balance zwischen der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte zu gewährleisten.

Die explizite Legitimierung der Equipment Interference wurde aber im öffentlichen Konsultationsprozess besonders durch Bürgerrechtsbewegungen kritisiert. Privacy International wies, wie viele andere[13], darauf hin, dass die neuen Regelungen sehr weitreichende Folgen für die IT-Sicherheit haben könnten. Insbesondere die Unterstützung durch Telekommunikationsdienstleister sei in hohem Maße problematisch, da es in diesem Kontext denkbar sei, dass diese als Sicherheitsupdates getarnte Hintertüren in ihre Software integrieren könnten, um den staatlichen Anordnungen Folge zu leisten. Dies sei sowohl bürgerrechtlich bedenklich, da viele NutzerInnen persönlichste Daten auf IT-Systemen speicherten als auch aus wirtschaftlicher Sicht abzulehnen, da hierdurch auch Hintertüren für Kriminelle offen blieben: »This weakening of systems leads to sacrificing the security of the communications that we all rely on for banking, commerce and other everyday transactions […]« (Privacy International, 2015b).

Auch VertreterInnen der Wirtschaft sahen die neuen Befugnisse als zu weitreichend. Der Industrieverband techUK verwies in einer Stellungnahme ebenfalls darauf, dass es problematisch sei, Unternehmen dazu zu verpflichten, Schwachstellen in die eigenen Produkte zu integrieren. Die WirtschaftsvertreterInnen sahen in dieser Praxis auch erhebliche Probleme bezüglich der Haftung für Schäden, die durch diese Hintertüren bei anderen Kunden (auch im Ausland) entstehen könnten (techUK, 2015).

Die Regierung rechtfertigte die neuen Befugnisse vor dem Parlament unter Verweis auf die veränderte Gefahrensituation in der das Risiko eines Terroranschlags jederzeit gegeben sei. TerroristInnen nutzten zu ihrer Koordination und zur Vorbereitung von Anschlägen immer häufiger das Internet (House of Com-

13 Ähnlich wie Privacy International argumentierten Big Brother Watch (2015), die Electronic Frontier Foundation (2015) und Liberty (2016).

mons, 2016c). Equipment Interference sei in diesem Bereich oftmals die einzige Möglichkeit diese Gefahren aufzuspüren und zu bekämpfen.

> »It allows the security and intelligence agencies to keep pace with terrorists and serious criminals, who increasingly use sophisticated techniques to communicate, to evade detection in dark places, and to plan and plot what they do. Equipment interference has been instrumental in disrupting credible threats to life, including those against UK citizens.« (Ebd., S. 5)

Die Einschätzung, dass die Regierung die Möglichkeit haben müsse, auf Informationen auf IT-Systemen zuzugreifen, wurde auch von der Opposition nicht grundsätzlich in Abrede gestellt. Ferner wurden auch die etablierten Kontrollen und die Abwägung mit bürgerrechtlichen Bedenken weitgehend für ausreichend erachtet (House of Commons, 2016c, S. 6f.).

Die Abgeordneten erkannten damit im Gegensatz zu den AktivistInnen kein Defizit bei der Rolle als Garant liberaler Grundrechte. Das Argument, der Staat unterminiere durch die Beschützer-Rolle die Sicherheit im globalen Netz wurde wiederum nicht aufgegriffen bzw. akzeptiert. Der nationale Rahmen blieb Referenzpunkt (Schutz für wen?) der Beschützer-Rolle.

Es waren letztlich die aus der Rolle als Wohlstandsmaximierer folgenden Bedenken zur Beeinträchtigung der wirtschaftlichen Wettbewerbsfähigkeit, die den zuständigen Parlamentsausschuss dazu veranlassten, die Regierung aufzufordern, die praktische Anwendung der neuen Befugnisse genau zu überwachen und ggf. zu überarbeiten:

> »As ever, the fight against serious crime should be appropriately balanced with the requirement to protect and promote the UK's commercial competitiveness. We believe the industry case regarding public fear about 'equipment interference' is well founded.« (House of Commons, 2016d, S. 21)

In Großbritannien war also nicht die Rolle als Garant liberaler Grundrechte maßgeblich für die Einschränkung bzw. Kontrolle der exekutiven Kompetenzen, sondern die Rolle als Wohlstandsmaximierer. Da zusätzlich zum teilweise katalytischen Zusammenwirken der beiden Rollen im britischen Fall auch ein Bezug zum historischen Selbst als Opfer von Terrorismus hergestellt wird, ist der Exekutiven die Übernahme einer umfassenderen, weniger kontestierten Beschützer-Rolle im Bereich der polizeilichen Strafverfolgung möglich.

Diese umfassendere Beschützer-Rolle überträgt sich auch auf die internationale Ebene. Die extraterritoriale Qualität der Beschützer-Rolle zeigt sich im Anspruch ausländische Dienstleister zur Entschlüsselung zu verpflichten. Im Gegensatz zur Bundesrepublik hat das Vereinigte Königreich mit dem Crime (Overseas Production Orders) Act 2019 die Voraussetzungen dafür geschaffen, dass,

nach Abschluss eines internationalen Abkommens, britische Strafverfolgungsbehörden ohne den Weg über gegenseitige Rechtshilfe direkt an Diensteanbieter im Zielland herantreten und die Herausgabe von Daten verlangen können (The Stationery Office, 2019).

Aus Sicht der Regierung war dieser neue Weg und die damit verbundene Extraterritorialisierung der Beschützer-Rolle notwendig geworden, da die bestehenden Prozesse der Rechtshilfe mit einer Dauer von bis zu zwei Jahren nicht ausreichten, um akuten Gefahren durch schwere Kriminalität und Terrorismus zu begegnen. Hinzu komme, dass Daten immer häufiger im Ausland gespeichert seien und dass die domestischen Regelungen somit nicht mehr angemessen seien. Bereits in den ersten parlamentarischen Beratungen des Gesetzentwurfs ließ die Regierung keinen Zweifel daran, dass das erste Abkommen mit den USA geschlossen werden solle, da dort die Mehrheit wichtiger Diensteanbieter beheimatet sei (House of Commons, 2018b, S. 587f.). Dieses Abkommen wurde im Oktober 2019 geschlossen und umfasst nicht nur die Herausgabe von gespeicherten Meta- und Inhaltsdaten, sondern ermöglicht britischen Strafverfolgungsbehörden auch die Anordnung von unmittelbaren Abhörmaßnahmen zum Abfangen laufender Kommunikation, wobei US-BürgerInnen gegen alle Abfragen geschützt sind (UK Government, 2019a, S. 4f.). Bürgerrechtsorganisationen kritisierten diese neuen Regelungen und sahen darin ein beginnendes »Race to the Bottom« mit Blick auf die liberalen Grundrechte (EFF, 2019).

Auf internationaler Ebene äußert sich die weniger herausgeforderte Beschützer-Rolle in Großbritannien folglich auch in offeneren Kooperationen. Die Referenz der Beschützer-Rolle (Schutz für wen?) auf das nationale Gemeinwesen bleibt jedoch erhalten, da die jeweils eigenen StaatsbürgerInnen besonders geschützt werden.

4.3 Zwischenfazit

Die Analyse der Cybersicherheitspolitik im Bereich der Kriminalitätsbekämpfung zeigt einige Ähnlichkeiten aber auch deutliche Unterschiede zwischen den beiden Untersuchungsstaaten. In beiden Fällen wurde die Beschützer-Rolle zuerst durch ein katalytisches Zusammenspiel mit der Rolle als Wohlstandsmaximierer ermöglicht. In beiden Fällen wurde die Beschützer-Rolle damit zuerst mit Bezug auf das Referenzobjekt (Schutz für wen?) Wirtschaft etabliert. Die Kontestation einer zu weitgehenden Beschützer-Rolle erfolgte in beiden Staaten unter Verweis auf die wirtschaftlichen Folgen einer zu umfassenden Regulierung vornehmlich durch VertreterInnen der Wirtschaft sowie des Parlaments. In Deutschland war die Beschützer-Rolle zunächst auch dadurch begrenzt, dass FreizeithackerInnen nicht kriminalisiert werden sollten. Diese Beschränkung gab es in Großbritannien