die deutsche Staatsgewalt auch im Ausland an die Grundrechte gebunden ist. Das Gericht widersprach damit direkt der Interpretation der Bundesregierung. Dementsprechend forderten die RichterInnen die Regierung auf, das BND-Gesetz bis zum Ende des Jahres 2021 grundgesetzkonform zu gestalten (Bundesverfassungsgericht, 2020).

Mit dem neuen BND-Gesetz hat die Bundesregierung die Beschützer-Rolle entlang der enthüllten Praktiken gestaltet. Dies wurde einerseits durch die mit dem internationalen Terrorismus verbundene Gefahrenlage sowie durch die internationale Abhängigkeit ermöglicht. Der Rolle als Garant liberaler Grundrechte wurde aber durch neue Kontrollbefugnisse sowie das neue Unabhängige Gremium und die Stärkung des Parlamentarischen Kontrollgremiums ebenfalls entsprochen. Die Gegenrollenträger haben dies aber als unzureichend betrachtet und das Bundesverfassungsgericht hat die Bundesregierung zur Überarbeitung des Gesetzes verpflichtet.

5.2 Vereinigtes Königreich

5.2.1 Die Snowden-Enthüllungen: Die britische Regierung zwischen Kritik und Selbstbehauptung

Nach den Veröffentlichungen der Snowden-Enthüllungen geriet die britische Regierung durch die weltweite Berichterstattung in die Kritik. In den ersten Stellungnahmen verurteilten RegierungsvertreterInnen daher die Veröffentlichung der Dokumente als schädlich für die Gewährleistung der Sicherheit im Vereinigten Königreich und damit als unangemessene Beeinträchtigung der Beschützer-Rolle. Zudem führten sie aus Sicht der Regierung zu einer verzerrten öffentlichen Wahrnehmung der nachrichtendienstlichen Praktiken.

Außenminister William Hague betonte daher, dass die Regierung zwar daran interessiert sei, dafür zu sorgen, dass die BürgerInnen Vertrauen in die Arbeit der Nachrichtendienste und deren rechtmäßige Praktiken hätten, dass aber in diesem Kontext keine Informationen öffentlich werden dürften, die Kriminellen, TerroristInnen oder ausländischen Nachrichtendiensten Aufschluss über die Fähigkeiten des GCHQ offenbaren könnten. Um die Praktiken domestisch aufzuklären, wurden dem mit der Kontrolle der Nachrichtendienste betrauten Intelligence and Security Committee des Parlaments zusätzliche Informationen des GCHQ zur Verfügung gestellt (House of Commons, 2013c, S. 31). International verbat sich die Regierung jede Einmischung, so betonte Premierminister Cameron mit Blick auf die EU, dass die Regelungen geheimdienstlicher Praktiken alleinige nationalstaatliche Prärogative seien (UK Government, 2013c).

In dieser ersten Phase war die britische Regierung bemüht, die eigene Beschützer-Rolle gegen Kritik von innen und außen zu behaupten. Hierzu versuchte sie einerseits weitere Enthüllungen zu vermeiden und andererseits betonte sie die rechtsstaatliche Kontrolle der enthüllten Praktiken und damit die eigene Rolle als Garant liberaler Grundrechte sowie die Notwendigkeit geheimdienstlicher Aktivitäten. Durch den Druck zeigte sie auch die Bereitschaft, die Beschützer-Rolle etwas transparenter zu machen.

Bereits in der ersten parlamentarischen Debatte im Juni 2013 wurde von der Regierung sogar die Frage aufgeworfen, ob das GCHQ alle notwendigen Kapazitäten habe, um die Sicherheit bestmöglich zu gewährleisten. Der Außenminister gab schon in dieser Frühphase zu bedenken, dass die gesetzlichen Regelungen angesichts der technischen Entwicklung und der vielfältigen Gefahren (insbesondere des Terrorismus') ausgebaut werden müssten (House of Commons, 2013c, S. 41 bzw. 48). Immer wieder finden sich in den Debatten zudem Verweise auf die Vorgängerinstitution des GCHQ, die Government Code and Cypher School, die von einem Anwesen in Bletchley Park maßgeblich zur Entschlüsselung der deutschen Kommunikation im Zweiten Weltkrieg beitrug. Diese Referenz auf das positive historische Selbst des Nachrichtendienstes findet sich sowohl bei VertreterInnen der Regierung als auch der Opposition (ebd., S. 38f. ebenso 46).[3]

Auf internationaler Ebene vertrat die britische Regierung die Position, dass die Menschenrechte on- wie offline Gültigkeit hätten. RegierungsvertreterInnen machten aber auch deutlich, dass die enthüllten Überwachungsbestrebungen nicht substanziell begrenzt werden würden. Auf einer Konferenz in Seoul sagte Außenminister Hague nur wenige Monate nach Veröffentlichung der ersten Dokumente aus den Snowden-Files:

> »We do all face sophisticated and persistent threats in cyberspace from terrorists or organised criminals. We will not compromise on the United Kingdom's security or give free rein in cyberspace to those who wish to harm our country. With my full support our security and intelligence agencies will continue to address threats in cyberspace and to help our allies and partners to do the same – and the UK will remain at the centre of the debate on how we tackle those threats more effectively. But countries who seek to hide behind firewalls and erect artificial barriers on the internet will ultimately reduce their security, not enhance it.« (Foreign & Commonwealth Office, 2013a)

In diesem Kontext wurde auch betont, dass Staaten, die eine stärkere staatliche Kontrolle des Internets anstrebten, riskierten den digitalen Wirtschaftsraum

3 Die Referenzen zum positiven historischen Selbst des Nachrichtendienstes und dessen Einfluss auf die britische Cybersicherheitspolitik wurde durch den Verfasser kursorisch in einem Aufsatz dargestellt (Steiger, 2017).

nachhaltig zu beschädigen (ebd.). Auf diese Weise versuchte die britische Regierung den Vorwürfen zu begegnen, dass sie mit ihren Überwachungspraktiken selbst weitgehende Kontrolle ausübe und die Sicherheit anderer Staaten bzw. deren BürgerInnen unterminiere. Sie rechtfertigte die eigene Sicherheitspolitik mit aus ihrer Sicht legitimen Bedenken um die (physische) Sicherheit im Vereinigten Königreich und kritisierte zugleich die staatlichen Kontrollen autokratischer Staaten.

Weiterhin betonte die Regierung, dass die Nachrichtendienste stets im Einklang mit den gesetzlichen Regeln arbeiteten und dass damit der Schutz der Bürgerrechte gewährleistet sei. Rollentheoretisch gesprochen, bekräftigte die Regierung damit, dass es kein Defizit bei der Rolle als Garant liberaler Grundrechte gab. Zudem dürfe das GCHQ nur nach ministerieller Anweisung umfassende Überwachungsmaßnahmen ergreifen. Dies sorge insbesondere mit Blick auf die Überwachung britischer StaatsbürgerInnen für eine strenge Kontrolle. Der Prozess gewährleiste, dass der sicherheitspolitische Nutzen stets kritisch gegen die bürgerlichen Freiheitsrechte abgewogen werde. Zusätzlich dazu seien die Überwachungsanordnungen Gegenstand der Prüfung durch den/die Intelligence Services Commissioner und Interception of Communications Commissioner. Insgesamt verfüge das Vereinigte Königreich über eines der stärksten Kontrollsysteme für Nachrichtendienste (House of Commons, 2013c, S. 32 ebenso 38).

Zu diesen Kontrollen kam die positive Haltung gegenüber dem GCHQ, das nicht nur VertreterInnen der Regierung und des Dienstes selbst immer wieder betonten. Die positive Einstellung gegenüber den Nachrichtendiensten wurde in einer ersten Stellungnahme des britischen Premierministers David Cameron deutlich, in der er zur Rechtfertigung der enthüllten Praktiken auch die domestischen Erfahrungen mit Terrorismus aufgriff:

> »But we have every reason to be proud of our intelligences [sic!] services and the way in which they are properly constituted in this country. Since 2000, we have seen serious attempts at major acts of terrorism in Britain typically once or twice a year. […] This year alone, there were major trials related to plots including plans for a 7/7-style attack with rucksack bombs two plots to kill soldiers […]« (UK Government, 2013b)

Aus Sicht der Regierung bestand daher kein Anlass, die Nachrichtendienste in ihren Befugnissen zu beschränken, da die Gefahrenlage für das Vereinigte Königreich insbesondere aufgrund terroristischer Aktivitäten nach wie vor akut war. Die Referenz zum historischen Selbst als Opfer von Terroranschlägen findet sich in diesen Debatten ähnlich wie in den Debatten zu den polizeilichen Befugnissen.

Die Einschätzung wurde aber von Bürgerrechtsorganisationen sowie von Edward Snowden herausgefordert. Aus seiner Sicht waren die Befugnisse des britischen GCHQ sogar noch problematischer als die der amerikanischen NSA:

> »Their respect for the privacy right, their respect for individual citizens, their ability to communicate and associate without monitoring and interference is not strongly encoded in law or policy. And the result of that is that citizens in the United Kingdom and citizens around the world who are targeted by the United Kingdom [...] they're at a much greater risk than they are in the United States.« (The Guardian, 2014b)

Die Snowden-Enthüllungen illustrierten in diesem Zusammenhang umfassende Überwachungspraktiken des GCHQ, wie bspw. das Programm Tempora in dessen Kontext transatlantische Glasfaserkabel am Übergabepunkt in Bude angezapft und Kommunikation überwacht wurde (The Guardian, 2013a).

Aus rollentheoretischer Perspektive bemängelten die KritikerInnen eine noch umfassendere und schlechter kontrollierte britische Beschützer-Rolle. Aus ihrer Sicht bestand damit ein Defizit bei der Rolle als Garant liberaler Grundrechte. Außerdem zeigten die Enthüllungen, dass die britische Beschützer-Rolle auch offensiv gegen Partnerstaaten gerichtet war.

Die Snowden-Enthüllungen offenbarten, dass die britische Regierung auch vor dem Hacken in verbündeten Staaten nicht zurückschreckte. Zwischen 2010/11 und 2013 infiltrierte das GCHQ die Systeme des belgischen Telekommunikationsdienstleisters Belgacom. Die als Operation Socialist bezeichnete Maßnahme diente dazu, dem Nachrichtendienst Zugriff auf Informationen insbesondere zu Kommunikationsvorgängen in Afrika und dem Mittleren Osten zu gewähren. Außerdem sollte der Zugriff dann ggf. über Belgacom auf andere Unternehmen ausgedehnt werden. Das GCHQ attackierte damit nicht nur ein Unternehmen im einem EU-Mitgliedsstaat, sondern auch einen wichtigen Dienstleister europäischer Institutionen sowie der NATO. Die belgische Regierung kam nach der Analyse des Angriffs 2018 in einem geheimen Papier zu der Einschätzung, dass der Angriff durch den britischen Geheimdienst ausgeführt wurde und vermutlich durch den Außenminister genehmigt worden war. Öffentlich machte die belgische Regierung diese Erkenntnisse aber nicht über offizielle Kanäle (heise.de, 2014; Spiegel, 2014b; The Guardian, 2018).

Die britische Regierung ging in der Folge zur Behauptung der Beschützer-Rolle offensiv gegen den Guardian vor, der die Dokumente von Edward Snowden erhalten hatte und die Berichterstattung in Großbritannien maßgeblich vorantrieb. Im Juli 2013 wurden JournalistInnen veranlasst, die Festplatten mit den Snowden-Dokumenten physisch zu zerstören. Andernfalls drohte die Regierung mit rechtlichen Konsequenzen (The Guardian, 2013b). Ein Vorgehen das von Bürgerrechtsorganisationen als schwerwiegender Eingriff in die Pressefreiheit scharf kritisiert wurde (Amnesty International, 2013) und auch von Mitgliedern des Unterhauses skeptisch bewertet wurde (House of Commons, 2013e, S. 350f.). Das Vorgehen wurde von Premierminister Cameron aber explizit gerechtfertigt:

> »As I said, we have a free press and it is very important that the press feels it is not pre-censored in what it writes. The approach we have taken is to try to talk to the press and explain how damaging some of these things can be. That is why The Guardian destroyed some of the information on disks it had, although it has now printed further damaging material. I do not want to have to use injunctions, D notices or other, tougher measures [...]« (House of Commons, 2013d, S. 666f.)[4]

Die Abwägung zwischen der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte war aus Sicht der Regierung damit eindeutig formuliert. Die freie Presseberichterstattung durfte die Beschützer-Rolle nicht unterminieren. Zu diesen Maßnahmen der Selbstbehauptung gehörte auch die kurzfristige Verhaftung und Durchsuchung von David Miranda[5] am Flughafen Heathrow im August 2013. Die Rechtmäßigkeit des Vorgehens wurde später auch gerichtlich bestätigt (The Guardian, 2014a). Das resolute Vorgehen gegen die britischen Medien wurde von internationalen JournalistInnen-Verbänden als flagranter Verstoß gegen die Pressefreiheit interpretiert (Committee to protect Journalists, 2013).

Die Veröffentlichungen der Snowden-Dokumente sorgten aber auch in Großbritannien für Kritik von BürgerrechtsaktivistInnen (Liberty, 2013). Drei britische Bürgerrechtsorganisationen reichten in der Folge, zusammen mit weiteren internationalen NGOs, eine Klage vor dem Investigatory Powers Tribunal (IPT) ein, dem mit der juristischen Bewertung geheimdienstlicher Praktiken betrauten Gremium. Konkret vertraten die KlägerInnen die Ansicht, dass die enthüllten Überwachungsmaßnahmen gegen die Artikel 8 bzw. 10 der Europäischen Menschenrechtskonvention verstießen (Investigatory Powers Tribunal, 2014).

Neben der prozeduralen Kontrolle der Nachrichtendienste verwiesen RegierungsvertreterInnen zur Entkräftung der Kontestationen immer wieder auf die Benevolenz des GCHQ und auf die positiven historischen Erfahrungen mit dem Dienst sowie mit der Kooperation mit der NSA, die seit den 1940er Jahren maßgeblich für die Sicherheit beider Nationen gewesen sei. Während in der deutschen Debatte häufig die einseitige Abhängigkeit von den USA betont wurde, wurde das Verhältnis zwischen dem Vereinigten Königreich und den USA von britischer Seite symmetrisch wahrgenommen und die Reziprozität der Beziehung akzentuiert (House of Commons, 2013c, S. 43). Auf internationaler Ebene wurde die Übernahme einer expansiven Beschützer-Rolle daher erleichtert, da das GCHQ auch

4 Mittels D Notice, mittlerweile DSMA Notice, kann die britische Regierung Medien darum bitten, bestimmte Informationen aus sicherheitspolitischen Gründen nicht zu publizieren. Die Entscheidung über die Veröffentlichung obliegt aber nach wie vor den Redaktionen (Defence and Security Media Advisory Committee, 2020)

5 Dem Lebensgefährten von Glenn Greenwald, der maßgeblich an der Veröffentlichung der Snowden-Dokumente beteiligt war.

weiterhin auf Augenhöhe mit der NSA kooperieren und als technisch versierter Partner wahrgenommen werden sollte.

Diese Kooperation sei nach wie vor für beide Seiten essenziell und die Prinzipien der Zusammenarbeit stünden auch nach Jahrzehnten nicht zur Disposition, sondern sollten weiter ausgebaut werden (House of Commons, 2013c, S. 45 bzw. 49). Die Regierung bestritt in diesem Kontext auch, dass das GCHQ durch den Austausch mit der NSA an Daten gelangt sei, die es laut britischem Recht nicht erheben dürfe (ebd., S. 32f.). Das unterschiedliche Schutzniveau für britische und amerikanische StaatsbürgerInnen durch die NSA wurde von der Opposition zwar problematisiert, die Kooperation allerdings nicht substanziell in Frage gestellt (ebd., S. 39 ebenso 43).

Im Gegensatz zu Deutschland, wo die Beschützer-Rolle als abhängig von der amerikanischen gesehen wurde, sah die britische Regierung eine Kooperation auf Augenhöhe. Außerdem verwies die Exekutive auf die positiven Erfahrungen der Kooperation mit den USA. Zudem betonte sie die Notwendigkeit einer starken Beschützer-Rolle. Die Regierung zeigte sich immer wieder stolz auf die Leistungen des Nachrichtendienstes und deren Fähigkeiten. In diesem Zusammenhang verwiesen RegierungsvertreterInnen wiederholt auch auf das positive historische Selbst des CGHQ und insbesondere die Erfolge während des Zweiten Weltkriegs. Diese positive Einstellung gegenüber dem Nachrichtendienst wurde auch von der parlamentarischen Opposition weitgehend geteilt.

Die Regierung betonte, die Arbeit der Nachrichtendienste sei in einer zunehmend komplexen Sicherheitslage von zentraler Bedeutung für die Gewährleistung der Sicherheit in Großbritannien:

> »There is no doubt that secret intelligence, including the work of GCHQ, is vital to our country. It enables us to detect threats against our country ranging from nuclear proliferation to cyber attack. Our agencies work to prevent serious and organised crime, and to protect our economy against those trying to steal our intellectual property. They disrupt complex plots against our country, such as when individuals travel abroad to gain terrorist training and prepare attacks. They support the work of our armed forces overseas and help to protect the lives of our men and women in uniform [...]« (Ebd., S. 33)

Die oppositionelle Labour Party verteidigte ebenfalls die Arbeit der Nachrichtendienste und verwies auf deren einwandfreien Leumund. Auch die Opposition betrachtete es als wichtiger, die gesetzlichen Vorgaben transparent zu kommunizieren und ggf. anzupassen, um das öffentliche Vertrauen zu stärken. Eine Veränderung der enthüllten Praktiken wurde dagegen kaum gefordert (ebd., S. 34-36).

Konservative Abgeordnete bezeichneten die Enthüllungen gar als »non-story«, die Selbstverständlichkeiten nachrichtendienstlicher Kooperation zwischen Ver-

bündeten unnötig problematisiere. Ferner vertraten VertreterInnen der Tories die Ansicht, dass sich das Vereinigte Königreich bereits in einem »cyber-war« befände und dass den Diensten aufgrund der besonderen Gefahr durch kinetisch folgenreiche Cyberangriffe weitgehende Freiheiten eingeräumt werden sollten (ebd., S. 43 bzw. 45). Auch Abgeordnete der Liberal Democrats konnten bspw. die Aufregung der deutschen Bundesregierung über die Überwachung des Mobiltelefons der Bundeskanzlerin nicht nachvollziehen und betrachteten die Reaktion entweder als Ausdruck tiefer Naivität oder als bloßes öffentliches Manöver (House of Commons, 2013e, S. 362).

Die Ausrichtung der Beschützer-Rolle und deren Umfang wurde im Vereinigten Königreich damit nicht so kritisch beurteilt wie in Deutschland. Während die enthüllten Praktiken in Deutschland als unangemessen empfunden wurden, teilten in Großbritannien viele PolitikerInnen die Ansicht, dass die Arbeit der Nachrichtendienste in dem veröffentlichten Umfang nicht grundsätzlich falsch seien. Dies wurde sowohl durch die als brisant empfundene Gefahrenlage als auch durch das historisch begründete Vertrauen in den Nachrichtendienst ermöglicht.

Zusätzlich zu den essenziellen sicherheitspolitischen Funktionen wurde den Praktiken des GCHQ auch zentrale Bedeutung für die Erreichung wirtschaftlicher Ziele zugesprochen, bspw. bei der offensiven Aufdeckung und Verfolgung von Steuerkriminalität und Wirtschaftsspionage (ebd., S. 356). Ein potenter Nachrichtendienst komplementiert aus dieser Sicht auch die Rolle als Wohlstandsmaximierer. Die Beschützer-Rolle hatte im Gegensatz zu Deutschland damit auch eine katalytisch wirkende Bezugnahme zu wirtschaftlichen Schutzobjekten über den defensiven Wirtschaftsschutz hinaus, die auch eine offensivere Rollenübernahme rechtfertigte.

Zwei Monate nach den ersten Enthüllungen gab das Intelligence and Security Committee (ISC) eine Bewertung zu den veröffentlichten Dokumenten ab. Im Mittelpunkt der parlamentarischen Untersuchung stand der Vorwurf, das britische GCHQ habe im Rahmen der Kooperation mit der NSA durch das PRISM-Programm Zugriff auf Daten britischer StaatsbürgerInnen erlangt, ohne über die dazu notwendigen Berechtigungen zu verfügen. Nach ihrer Untersuchung attestierten die Abgeordneten dem GCHQ, dass die Kooperation im Rahmen der gesetzlichen Regelungen erfolgt sei und dass für die Überwachungsmaßnahmen Anordnungen der zuständigen MinisterInnen vorlagen. Alle Maßnahmen seien durch RIPA 2000 und den Intelligence Services Act 1994 gedeckt gewesen. Die in der Presse geäußerten Verdachtsmomente seien daher unbegründet. Die MPs äußerten aber Bedenken, ob das gesetzliche Regelwerk, das die Auslandsüberwachung regelte, angesichts der technischen Entwicklungen noch angemessen sei. Diese Problematik wurde ferner durch den Interception of Communications Commissioner (IOCCO) untersucht (Intelligence and Security Committee, 2013a,

S. 2).[6] Die Regierung begrüßte diese Entlastung des Nachrichtendienstes explizit und betonte, dass die Überwachungspraktiken stets geltendem Recht entsprächen und angemessener demokratischer Kontrolle unterworfen seien (Foreign & Commonwealth Office, 2013b).

Mit dieser Einschätzung stützte das zuständige parlamentarische Kontrollorgan die Position der Regierung. Auch aus Sicht der Abgeordneten gab es keine systematische Überdehnung der Beschützer-Rolle zu Lasten der Rolle als Garant liberaler Grundrechte.

Im Oktober 2013 kam es zu ersten Kontestationsprozessen durch den kleinen Koalitionspartner gegen einen Ausbau der Überwachungsmaßnahmen. Abgeordnete der Liberal Democrats befürchteten, das Vereinigte Königreich befände sich auf einem Pfad, der »schlafwandlerisch« in einen ausgeprägten Überwachungsstaat führe und in dem die Balance zwischen Sicherheit und Freiheit nicht mehr gewahrt werde. Allerdings wurde auch von den skeptischen Abgeordneten nicht die Notwendigkeit oder Benevolenz der Nachrichtendienste infrage gestellt (House of Commons, 2013e, S. 333).

Mit Blick auf wirtschaftliche Schäden verwiesen britische Abgeordnete auf Deutschland. Überwachungskritische Stimmen aus dem Lager der Liberal Democrats betonten, dass durch die enthüllten Praktiken wirtschaftliches Vertrauen unterminiert werde und dass in Deutschland bereits Konzepte zur Wahrung der digitalen Souveränität (Schengen-Routing) debattiert würden (ebd., S. 338). Die Liberal Democrats forderten daher, wie das ISC, eine grundlegende Evaluation des bestehenden Rechtsrahmens (insbesondere RIPA 2000) – ein Anliegen, das auch von Abgeordneten der Labour Party geteilt wurde (ebd., S. 341 bzw. 364). Insbesondere das Programm Tempora sorgte für Besorgnis, ob die ergriffenen Maßnahmen verhältnismäßig und mit Artikel 8 der Europäischen Menschenrechtskonvention vereinbar seien (ebd., S. 342 ebenso 345). Auch die Beteiligung an Prism und der damit potenziell verbundene Datenaustausch wurden wiederholt problematisiert (ebd., S. 353f.). Generell bemängelten KritikerInnen, dass im Gegensatz zu anderen Staaten und auch den USA in Großbritannien keine wirkliche Debatte über die enthüllten Praktiken stattfinde (ebd., S. 333 ebenso 358f.).

Aber auch auf Seiten des überwachungsskeptischeren kleinen Koalitionspartners wurde auf die historischen Leistungen der »code breakers« sowie auf die Notwendigkeit der Geheimhaltung ihrer Aktivitäten hingewiesen (ebd., S. 361 bzw. 364). Die direkte Verbindung historischer Leistungen und aktueller sicherheitspolitischer Herausforderungen wurde bspw. vom Parteivorsitzenden Nick Clegg betont:

---

6 In seinem 2014 veröffentlichten Bericht kam auch der IOCCO zu der Einschätzung, dass bspw. eine längere Speicherung von erhobenen und nicht für relevant befundenen Daten nicht stattfinde (IOCCO, 2014, S. 15).

> »The security services are similarly awe-inspiring. […] GCHQ has an illustrious history, from the code-breakers who defeated the Enigma machine and shortened the Second World War by at least 2 years, through to the contemporary fight against terrorism.« (UK Government, 2014)

Ein zentraler Bezugspunkt zur Rechtfertigung der expansiven Überwachungsmaßnahmen und zum Nachweis der Benevolenz des GCHQ waren auch beim kritischen Koalitionspartner die historischen Erfahrungen mit dem Nachrichtendienst. Auch KritikerInnen der enthüllten Maßnahmen bezogen ihre Kontestationen damit nicht auf den Nachrichtendienst oder das Potenzial, Daten missbräuchlich zu verwenden, sondern auf das gesetzliche Regelwerk. Auch die Gefahrenlage für das Vereinigte Königreich wurde nicht grundlegend bestritten.

Die Abgeordneten der Tories erwiderten Kritiken mit dem Verweis auf die strenge Kontrolle der britischen Nachrichtendienste (House of Commons, 2013e, S. 367f. ebenso 372). Außerdem betonten sie, dass die Nachrichtendienste große Datenmengen benötigten, um hierin die relevanten Informationen finden zu können – großflächige Überwachungsmaßnahmen waren aus ihrer Sicht also notwendig, um aktuellen Gefahren zu begegnen (ebd., S. 375). VertreterInnen der Tories hielten KritikerInnen zudem entgegen, dass die Gefahrenlage diffuser denn je sei und rekurrierten auf die domestischen Erfahrungen mit Terrorismus, insbesondere die Anschläge in London am 7. Juli 2005 (ebd., S. 345).

Auf die Leistungen des Nachrichtendienstes verwies explizit der damalige Direktor des GCHQ Anfang November 2013. Er stellte in einer Rede ebenfalls eine direkte Verbindung zwischen historischen Erfolgen und aktuellen Praktiken her:

> »I've already spoken about the rich legacy of Bletchley Park for GCHQ: just as the work at Bletchley involved exploiting the adversary's information risk whilst minimising our own, today's internet provides a virtual battlespace for a similar struggle. […] The period we spent in Bletchley Park in World War Two showcases the successes possible when a technological and innovative mindset is allied to an in-depth understanding of the communications environment in which our targets operated.« (GCHQ, 2013)

Wie in diesem Fall und der Äußerung von Nick Clegg wurde in Aussagen immer wieder die direkte Verbindung zwischen historischer Leistung und aktueller Herausforderung hergestellt. Die nachrichtendienstlichen Aktivitäten im Internet wurden so auf eine Stufe mit den Herausforderungen während des Zweiten Weltkrieges gestellt, wobei die Referenz (Schutz vor wem?) der gegenwärtigen Beschützer-Rolle zwischen (internationalem) Terrorismus und feindseligen Staaten schwankt.

Referenzen zu negativen historischen Erfahrungen finden sich zwar im parlamentarischen Kontext, sie sind aber selten und wurden oft nicht aufgegriffen. RegierungsvertreterInnen erwiderten diese Bezugnahmen mitunter gar damit, dass sie aus der Zeit gefallen und nicht mehr mit der nachrichtendienstlichen Tätigkeit im 21. Jahrhundert vergleichbar seien (House of Commons, 2013c, S. 43). Verweise auf das positive historische Selbst des Nachrichtendienstes wurden damit praktisch von allen Parteien geteilt. Eine Position, die die nachrichtendienstliche Beschützer-Rolle gänzlich infrage stellte gab es daher kaum. Stattdessen bezogen sich kritische Stimmen auf die Evaluation des Rechtsrahmens. Beschränkungen der nachrichtendienstlichen Kompetenzen wurden dagegen nur vereinzelt gefordert.

Im Zuge der parlamentarischen Aufarbeitung der Enthüllungen hielt das ISC die erste öffentliche Anhörung seiner Geschichte ab. In diesem Rahmen gaben am 7. November 2013 die Direktoren der drei großen britischen Nachrichtendienste (MI5, MI6 und GCHQ) Auskunft über deren Aktivitäten. In seiner Stellungnahme wies der Direktor des MI6 auf die diffuse Gefahrenlage und die damit verbundenen wichtigen Aufgaben der Nachrichtendienste hin. Zu den Herausforderungen gehörten demnach in erster Linie Terrorismus aber auch Cyberangriffe oder Aktivitäten feindlicher Staaten in Gebieten, die für das Vereinigte Königreich von Relevanz seien. Dabei stellte er auch die enge Kooperation mit den Streitkräften heraus (Intelligence and Security Committee, 2013b, S. 1f.). Das Internet wurde von den Direktoren übereinstimmend als asymmetrische Domäne charakterisiert, die terroristische Bestrebungen tendenziell erleichtere und deren Verfolgung erschwere (ebd., S. 3f.). Aber auch staatliche Akteure versuchten mit dem Internet ihre begrenzten Ressourcen zu kompensieren und Ziele zu beeinträchtigen, die sie sonst nicht erreichen könnten (ebd., S. 12f.). Die Frage, warum die britische Öffentlichkeit erst durch die Snowden-Dokumente von flächendeckenden Maßnahmen erfahren habe, beantwortet der Direktor des GCHQ mit Verweis auf die Notwendigkeit, bestimmte Methoden zur Wahrung ihrer Effektivität geheim zu halten. Ferner gebe es bereits Hinweise darauf, dass TerroristInnen die Informationen aus den veröffentlichten Dokumenten gezielt nutzten um einer Überwachung zu entgehen.

> »What I can tell you is that the leaks from Snowden have been very damaging. They have put our operations at risk. It is clear that our adversaries are rubbing their hands with glee. [...] and our own security has suffered as a consequence.« (Ebd., S. 18)

Der Dienst betreibe weitgehende Überwachung nur zu dem Zweck, einen möglichst großen »Heuhaufen« mit potenziell sicherheitspolitischen Inhalten zu generieren und diesen dann auch nicht komplett, sondern nur partiell und gezielt zu durchsuchen. Ferner versicherte er, dass die Kooperation mit der NSA stets im

Einklang mit britischem Recht gestaltet wurde. Auch die Bedeutung des Dienstes für das ökonomische Wohlergehen des Vereinigten Königreichs wurde in diesem Kontext hervorgehoben (ebd., S. 13-17). Dass die Enthüllungen die Sicherheitslage verschlechtert habe, wurde 2014 auch durch den neuen Direktor des GCHQ, Robert Hannigan, bestätigt. In einem vielbeachteten Beitrag für die Financial Times attestierte er den Betreibern von Sozialen Netzwerken ferner zu »command-and-control networks of choice for terrorists and criminals« geworden zu sein, da sie nach den Enthüllungen starke Verschlüsselung zum Teil ihres Marketings gemacht und damit Ermittlungsbehörden den Zugriff auf Daten erschwert hatten (Financial Times, 2014).

Aus Sicht der Nachrichtendienste war eine umfassende Überwachung daher essenziell, um die Beschützer-Rolle in einer Domäne sicherzustellen, die den GegnerInnen potenziell einen Vorteil biete. Ferner verurteilten sie die Beeinträchtigungen der Rolle durch die Veröffentlichungen. In diesem Kontext wurde auch die wichtige Zusammenarbeit zwischen GCHQ und den britischen Streitkräften herausgestellt. Während die britische Regierung außenpolitisch kritisiert wurde, waren die domestischen Kontestationen zunächst weniger schwerwiegend. Das GCHQ und deren Aktivitäten wurden von VertreterInnen fast aller Parteien positiv bewertet. Dies wurde durch die Bezugnahme zum positiven historischen Selbst sowie die Erfahrungen mit Terrorismus ermöglicht. Kritische Stimmen bezogen sich auf den Rechtsrahmen der Beschützer-Rolle aber nicht auf den Nachrichtendienst. In der Folge geriet die britische Regierung dennoch vermehrt unter Druck, weil innerstaatliche Untersuchungen zu dem Ergebnis kamen, dass die gesetzlichen Regelungen den technischen Realitäten nicht mehr Rechnung trugen.

5.2.2 Die Regierung unter Druck: Selbstbehauptung unter wachsendem domestischen Druck

Die Bemühungen, neue gesetzliche Regelungen zu erlassen wurden zunächst intensiviert, als der Europäische Gerichtshof im April 2014 Regelungen zur Vorratsdatenspeicherung für unrechtmäßig erklärte (Europäischer Gerichtshof, 2014). Damit drohten aus Sicht der Regierung wichtige Informationen verloren zu gehen. Der Data Retention and Investigatory Powers Act 2014 wurde in der Folge zwar verabschiedet. Die Tories konnten ihre Vorstellungen allerdings nicht vollends umsetzen und der kleine Koalitionspartner beschränkte die Regelung, die die Vorratsdatenspeicherung weiterhin erlaubte, auf zwei Jahre (sunset clause). Diese Regelungen hatten zwar kaum direkte Bezüge zur IT-Sicherheit, aber hierdurch ergab sich für das Jahr 2016 zusätzlicher Handlungsdruck für die Regierung (s.u.), da sie weiterhin eine gesetzliche Grundlage für die Vorratsdatenspeicherung aufrecht erhalten wollte und diese im Investigatory Powers Act 2016 mit wei-

teren Kompetenzen der Nachrichtendienste verband (House of Commons, 2015d, S. 1084).

Innerstaatlich wurden die Überwachungsmaßnahmen zunächst aber gestützt. Im Dezember 2014 urteilte das IPT erstmals über die Klagen der Bürgerrechtsorganisation gegen die Überwachungspraktiken des GCHQ. In ihrem Urteil stellten die RichterInnen fest, dass die Nachrichtendienste ihre Kompetenzen nicht über Gebühr ausgedehnt hatten (Investigatory Powers Tribunal, 2014, S. 76). Nachdem weitere Informationen über die konkreten Programme bekannt geworden waren, revidierte das IPT im Januar 2015 aber einen Teil dieses Urteils. In einer Urteilsergänzung teilte das Tribunal mit, dass Teile der Kooperation mit der NSA, die den Umgang mit Daten britischer BürgerInnen betrafen, die von amerikanischer Seite erhoben worden waren, gegen die Artikel 8 bzw. 10 der Europäischen Menschenrechtskonvention verstoßen hatten. Durch das Publikwerden im Rahmen der Aufarbeitung der Enthüllungen seien sie doch seit Bekanntwerden legal (Investigatory Powers Tribunal, 2015c).

Nachdem das IPT 2014 Klagen gegen die umfassende Kommunikationsüberwachung im Internet abgelehnt hatte, reichten Bürgerrechtsorganisationen eine weitere Klage vor dem Europäischen Gerichtshof für Menschenrechte ein (Privacy International, 2018). Im September 2018 urteilte der Gerichtshof, dass Teile von RIPA gegen Artikel 8 und 10 der Europäischen Menschenrechtskonvention verstoßen hatten. Das Gericht beurteilte die Kontrolle der umfassenden Kommunikationsüberwachung für nicht angemessen, befand die Praxis aber nicht für grundsätzlich inkompatibel mit Artikel 8. Zudem bemängelte das Gericht einen fehlenden Schutz für die besonders sensible Kommunikation von JournalistInnen. Da sich das Urteil aber auf die Regelungen nach RIPA bezogen, wurden die neuen Praktiken nach dem IPA, mit dem aus Sicht des Gerichts substanzielle Veränderungen einhergegangen waren, nicht überprüft bzw. infrage gestellt. Die Praktiken des Informationsaustauschs zwischen Geheimdiensten befand das Gericht für vereinbar mit der EMRK (European Court of Human Rights, 2018). Die KlägerInnen sahen in dem Urteil einen Erfolg, interpretierten die Befugnisse im IPA aber als noch weitreichender:

> »This judgment is a vital step towards protecting millions of law-abiding citizens from unjustified intrusion. However, since the new Investigatory Powers Act arguably poses an ever greater threat to civil liberties, our work is far from over.« (English PEN, 2018)

Neben diesem späteren Erfolg vor einem internationalen Gericht, urteilte aber auch das IPT 2015 zugunsten der KlägerInnen. Im Februar bzw. April 2015 entschied das Gericht gegen den Nachrichtendienst. Nach Auffassung der RichterInnen hatte das GCHQ in einem Fall besonders geschützte juristische Kommunikation unrechtmäßig abgehört. Die RichterInnen urteilten, dass die Regelun-

gen zum Umgang mit besonders geschützter Kommunikation nicht mit Artikel 8(2) der Europäischen Menschenrechtskonvention vereinbar waren. Die Regierung musste in diesem Zusammenhang zugeben, dass die Regeln zum Umgang mit diesen Daten nicht transparent gemacht worden waren. In der Folge musste das GCHQ die Daten löschen und die Regierung musste den Umgang mit diesen Daten spezifizieren (Investigatory Powers Tribunal, 2015a). Weiterhin urteilte das IPT im November 2015, dass das GCHQ die Daten zweier Bürgerrechtsorganisationen zwar rechtmäßig abgehört hatte, dass die Daten dann aber zu lange gespeichert worden waren (Investigatory Powers Tribunal, 2015b).

Die Kontestation der Beschützer-Rolle wurde damit durch die Judikative zumindest teilweise unterstützt und die Regierung in der Folge zu einer Spezifizierung der Rolle veranlasst.

Der Druck auf die Regierung erhöhte sich im Laufe der Jahre 2015/16 weiter, da unabhängige Evaluationen durch das ISC und den Independent Reviewer of Terrorism Legislation zu der Auffassung gelangten, dass das gesetzliche Regelwerk reformbedürftig sei. Das ISC hatte unmittelbar nach den Enthüllungen mit der Untersuchung der Überwachungspraktiken begonnen und auch in öffentlicher Anhörung Stellungnahmen dazu eingeholt. Im März 2015 legten die Abgeordneten ihren Bericht »Privacy and Security: A modern and transparent legal framework« vor (Intelligence and Security Committee, 2015). Auch in diesem Bericht bekräftigten die ParlamentarierInnen fraktionsübergreifend zunächst die besondere Bedeutung der Nachrichtendienste für die Sicherheit und das wirtschaftliche Wohlergehen des Vereinigten Königreiches.[7] Weiterhin betonten die Mitglieder des Committees, dass sie der Überzeugung seien, die Nachrichtendienste versuchten nicht die gesetzlichen Regelungen zu umgehen (dies schloss explizit den Human Rights Act 1998 ein). Allerdings kritisierte der Bericht, dass die Überwachungspraktiken und die gesetzlichen Bestimmungen nicht in ausreichendem Maße Transparenz für die Öffentlichkeit generierten. Daher empfahl der Ausschuss, eine neue rechtliche Grundlage für die Arbeit der Nachrichtendienste zu schaffen, die die Kompetenzen der Dienste ebenso transparent mache wie die damit einhergehenden Kontrollmechanismen (ebd., S. 1f.).

Rollentheoretische formuliert, folgten die Abgeordneten damit der Linie der Judikative, die die mangelnde Transparenz kritisierte, die Beschützer-Rolle aber nicht grundsätzlich infrage stellte. Das GCHQ und dessen Aktivitäten standen daher nicht zur Disposition.

Wie im deutschen Fall, war es auch in Großbritannien die großflächige Überwachung der Internetkommunikation, die im Rahmen der Aufarbeitung besonde-

7 Das wirtschaftliche Wohlergehen gehört ebenso zum, mit dem Intelligence Services Act 1994 gesetzlich definierten, Schutzgut wie die nationale Sicherheit und die Prävention schwerer Straftaten (The Stationery Office, 1994, Section 3(2)).

re Aufmerksamkeit erfuhr. Das ISC befasste sich eingehend mit den Kompetenzen zur selektorengestützten Überwachung mit dem Ziel der Verdachtsgenerierung (»bulk interception«). In diesem Kontext konstatierten die Ausschussmitglieder, dass nur ein geringer Teil der erfassten Kommunikation durch menschliche Analysten ausgewertet werde, da zuvor technische Filter große Teile der Daten verwerfen würden. Wie groß die jeweiligen Anteile der überwachten und dann ausgewerteten Daten waren, wurde aber nicht veröffentlicht. Im Gegensatz zum deutschen BND, ist das GCHQ aber nach einer entsprechenden Anordnung (RIPA Section 8(1)) auch dazu berechtigt, gezielt die Kommunikation britischer StaatsbürgerInnen zu überwachen und auszuwerten. Für Datenverkehre mit einem Endpunkt im Vereinigten Königreich und einem außerhalb bestand eine andere Form der Anordnung, die auch die Überwachung großer Datenmengen erlaubt (RIPA Section 8(4)). Beide Anordnungen müssen durch zuständige MinisterInnen ergehen (Intelligence and Security Committee, 2015, S. 2-7). Wenn das GCHQ eine Kommunikation abfängt, die sowohl einen Endpunkt in Großbritannien als auch im Ausland hat, dürfen nur Informationen mit Bezug zum/zur ausländischen KommunikationspartnerIn ausgewertet werden. Sollen zusätzlich Daten über KommunikationsteilnehmerInnen innerhalb des Landes analysiert werden, ist dazu entweder eine Section 8(1) Anordnung nötig oder eine ergänzende Section 16(3) Erweiterung (ebd., S. 41).

Wie in Deutschland sorgte auch im Vereinigten Königreich die verlässliche Distinktion zwischen in- und ausländischer bzw. internationaler Kommunikation für Diskussionen, da eine Unterscheidung bei paketvermittelter Information aufgrund unterschiedlicher Routenwahl und der Architektur des Netzes schwer zu treffen ist. Die Abgeordneten stellten daher fest:

> »[…] in respect of internet communications, the current system of 'internal' and 'external' communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications.« (Ebd., S. 41)

Auch die Erweiterung um Section 16(3) sollte nach Meinung der Ausschussmitglieder entfallen und durch Anordnungen nach Section 8(1) ersetzt werden. Ferner regte das ISC an, dass die unterschiedlichen Schutzniveaus für in- und ausländische Kommunikation nicht nur geografisch gefasst werden sollten, sondern dass zudem britische StaatsbürgerInnen im Ausland den gleichen Schutz genießen sollten wie inländische Kommunikation und ebenfalls nur mit einer Section 8(1) Anordnung überwacht werden dürften (ebd., S. 43f.).

Grundsätzliche Kritik bzw. die Forderung nach einem Verbot großflächiger Überwachungsmaßnahmen, wie sie von den Bürgerrechtsorganisationen Big Brother Watch, JUSTICE, Liberty und Rights Watch vorgebracht wurden, teilten

die Abgeordneten im ISC nicht. Vielmehr kam es aus ihrer Sicht auf eine transparente Regelung sowie eine rechtsstaatliche Kontrolle an, um eine unangemessene Beeinträchtigung von Freiheitsrechten zu verhindern (ebd., S. 35). Forderungen wonach Überwachungsanordnungen durch RichterInnen und nicht MinisterInnen erlassen werden sollten, lehnten die Ausschussmitglieder ebenfalls ab. Sie argumentierten, dass hierdurch eine Prüfung der politischen Opportunität und eventueller internationaler Implikationen ausbleibe, was zu einer erhöhten Zahl von genehmigten Anordnungen führen könne, sowie, dass RichterInnen nicht durch das Parlament politisch verantwortlich gemacht werden könnten (ebd., S. 2-7 bzw. 75f.). Diese Einschätzung wurde von BürgerrechtsaktivistInnen nicht geteilt, sie forderten eine richterliche Prüfung und Anordnung von Überwachungsmaßnahmen (Intelligence and Security Committee, 2014c, S. 13). Das ISC empfahl dagegen, die Kontrolle durch die zuständigen Interception of Communications Commissioner bzw. den Intelligence Services Commissioner zu stärken und ihnen mehr Befugnisse zur Kontrolle der Überwachungsanordnungen bzw. deren Umsetzung einzuräumen (Intelligence and Security Committee, 2015, S. 45 bzw. 78).

Auch die Praxis des gezielten Hackens von Computersystemen im Ausland bemängelten die Abgeordneten. Das GCHQ war gemäß Section 7 Intelligence Services Act dazu berechtigt, IT-Systeme im Ausland zu infiltrieren. Der Ausschuss befand, dass die Zahl der IT-Operationen signifikant zugenommen habe und dass es hierzu außerhalb der »Interference with Property« (Sections 5 und 7 Intelligence Services Act) eine eigenständige gesetzliche Regelung für Eingriffe in IT-Infrastrukturen geben solle (ebd., S. 66f.). In öffentlichen Anhörungen des Ausschusses, wurde die Praxis, in IT-Systeme einzudringen und dabei auf Sicherheitslücken zurückzugreifen von Bürgerrechtsorganisationen grundsätzlich kritisiert, da hierdurch die IT-Sicherheit weltweit unterminiert werde und Risiken für alle NutzerInnen entstünden. Hieraus könnten nicht nur Schäden für die Privatsphäre, sondern auch für das Vertrauen in den Wirtschaftsraum entstehen (Intelligence and Security Committee, 2014d, S. 2). In ihrem Bericht nahmen die Abgeordneten diese Sorgen auf, erkannten aber an, dass das GCHQ für seine Arbeit auf Sicherheitslücken und deren Ausnutzung angewiesen sei. Sie mahnten an, dass die Praxis politisch strenger kontrolliert werden sollte (Intelligence and Security Committee, 2015, S. 69).

Mit Blick auf Eingriffe in die Grundrechte, gaben VertreterInnen des GCHQ dem Ausschuss gegenüber an, dass bei Überwachungsaktivitäten stets die Vorgaben des Human Rights Acts 1998 und damit die Regelungen der Europäischen Konvention für Menschenrechte beachtet würden (ebd., S. 85). Im Gegensatz zu Deutschland, wo dem BND Versagen bei der Einhaltung der Gesetze vorgeworfen wurde, wurde dem GCHQ durch die Abgeordneten attestiert, trotz eines vagen

und reformbedürftigen gesetzlichen Rahmens, vorbildlich und stets nach bestem Wissen gehandelt zu haben (Intelligence and Security Committee, 2015, S. 7).

Der Vorwurf des Ringtausches von Informationen mit der NSA wurde ebenfalls durch den Ausschuss überprüft. Die Abgeordneten konstatierten hierzu, dass das GCHQ prinzipiell durch die gesetzlichen Grundlagen zum Datenaustausch ermächtigt sei, dass die Ausgestaltung jedoch nicht ausreichend spezifiziert sei. Auch in diesem Kontext erkannten die Mitglieder des ISC daher legislativen Handlungsbedarf (ebd., S. 94).

Im Gegensatz zu VertreterInnen der Netzgemeinde forderten Parlament und Judikative die Beschützer-Rolle der Regierung damit nicht substanziell heraus. Auch sie erkannten das Internet nicht als zu schützendes Gut an, sondern beurteilten die Gewährleistung nationaler Sicherheit als wichtiger. Aus rollentheoretischer Perspektive war damit eine Begrenzung der Beschützer-Rolle abgelehnt, mit Blick auf die Rolle als Garant liberaler Grundrechte wurde das GCHQ selbst als unproblematisch und die Überwachungspraktiken grundsätzlich als notwendig beurteilt.

Dieses besondere Vertrauen in den Nachrichtendienst stützte sich auch in der Phase parlamentarischer Aufarbeitung auf dessen historische Erfolge, die immer wieder durch den Direktor des Nachrichtendienstes hervorgehoben (GCHQ, 2014) und ferner von einem wissenschaftlichen Gutachter im Anhörungsprozess angeführt wurden: »I seriously think we have to give our intelligence and security community the tools it says it needs, and rely that they will deal with it lawfully« (Intelligence and Security Committee, 2014b, S. 10).

Nachdem das ISC seinen Untersuchungsbericht im März 2015 vorgelegt und eine Reform der Regelungen empfohlen hatte, folgte im Juni 2015 der Bericht von David Anderson, dem Independent Reviewer of Terrorism Legislation (Anderson, 2015). Im Rahmen seiner Analyse holte er Stellungnahmen verschiedener Interessengruppen ein. VertreterInnen der Nachrichtendienste verwiesen ihm gegenüber wiederholt auf die Notwendigkeit starker Dienste, um den Gefahren durch (domestischen und internationalen) Terrorismus, Cyberangriffe oder militärische Konflikte zu begegnen (ebd., S. 41). Hierzu müsse das GCHQ international als angesehener Kooperationspartner wahrgenommen werden, da nur so gewährleistet werden könne, dass Kooperationen und damit Informationsaustausch stattfänden. Aus diesem Grund äußerten VertreterInnen des GCHQ gegenüber Anderson ferner den Wunsch nach einer klaren gesetzlichen Grundlage für den Datenaustausch mit ausländischen Nachrichtendiensten (ebd., S. 198-201). Technologieführerschaft und Kooperationsfähigkeit war aus Sicht des GCHQ zentral zur effizienten Wahrnehmung der Beschützer-Rolle (ebd., S. 198).

Die Internetunternehmen und Kommunikationsdienstleister betonten in ihren Stellungnahmen gegenüber Anderson, dass sie für ihre Geschäftsmodelle auf vertrauensvolle Kommunikation und Datenintegrität angewiesen seien. Durch die

Snowden-Enthüllungen sei dieses Vertrauen beschädigt worden. Die amerikanischen Internetunternehmen bekräftigten in ihren Ausführungen die Ansicht, dass Unternehmen nicht auf Druck von Regierungen Daten herausgeben sollten, insbesondere dann, wenn es sich um Daten anderer StaatsbügerInnen handelt (ebd., S. 203-206). Dieses Unbehagen formulierte ein/e UnternehmensvertreterIn anonym folgendermaßen: »We can't get into conversations that leave our customers on the outside …our priority is our brand, not UK intelligence« (ebd., S. 206).

Grundsätzliche Kritik an den großflächigen Überwachungsmaßnahmen wurde von Bürgerrechtsorganisationen vorgetragen. Sie sahen in der Kombination neuer technischer Überwachungsmöglichkeiten und der rasant wachsenden digitalen Kommunikation eine Gefahr für die Privatsphäre aller InternetnutzerInnen, die sich ohne demokratische Debatte entfaltet habe:

> »[…] communications methods in general have expanded and the digital world makes surveillance even easier. The expansion of this approach means we have slipped into a mass surveillance model without a democratic debate regarding the consequences.« (Ebd., S. 223)

Insbesondere die Möglichkeit das »digitale Schleppnetz« auszuwerfen und auf diesem Weg, ohne viel Aufwand, große Mengen von Daten zu erheben, sorgte für Kritik, da die gesetzlichen Regularien das Ausmaß dieser Praktiken zum Zeitpunkt ihrer Entstehung noch nicht vorhersehen konnten. Abwägungen der Verhältnismäßigkeit seien bei dem Ausmaß der Internetüberwachung nicht mehr plausibel zu treffen. Auch die Argumentation, dass große Mengen der Daten nicht durch menschliche AnalystInnen ausgewertet würden, überzeugte die KritikerInnen nicht, da aus ihrer Sicht ein Eingriff in die Privatsphäre bereits mit der Erfassung der Daten einherging (ebd., S. 223f.). Gegenüber Anderson formulierten Bürgerrechtsorganisation auch Kritik an der parlamentarischen Aufsicht der Nachrichtendienste. So sei das ISC nur mit Abgeordneten besetzt, die durch die/den PremierministerIn nominiert wurden, Berichte müssten zudem zunächst durch die/den RegierungschefIn freigegeben werden. Ferner dürften MinisterInnen Informationen vor dem Committee zurückhalten (ebd., S. 241).

Wie das ISC gelangte auch Anderson zu der Einschätzung, dass das bestehende gesetzliche Regelwerk nicht mehr angemessen war. Auch er forderte die Regierung auf, eine transparentere Regelung für die Überwachungsmaßnahmen der Geheimdienste zu etablieren. Mit Blick auf die Kapazitäten zur flächendeckenden Überwachung, schloss sich Anderson ebenfalls der Ansicht des ISCs an und empfahl, den Nachrichtendiensten diese Möglichkeit offen zu lassen (ebd., S. 285-288). Die Dienste hätten ihm gegenüber überzeugend dargelegt, dass diese Maßnahmen zur Bekämpfung terroristischer Aktivitäten insbesondere nach den Anschlägen im Juli 2005 notwendig seien (ebd., S. 269). Um die Kontrolle der

Überwachungsmaßnahmen zu vereinfachen, schlug Anderson aber vor, eine Independent Surveillance and Intelligence Commission zu etablieren und dadurch die Interception of Communications und die Intelligence Services Commissioner zu ersetzen (Anderson, 2015, S. 299). Außerdem sollte es auch bei Urteilen des IPT ein Berufungsrecht geben – eine Forderung, die von vielen BürgerrechtlerInnen vorgetragen wurde. Ob die Organisation des ISCs geändert werden sollte, bspw. so, dass die Mitglieder wie in anderen Ausschüssen gewählt werden, überließ Anderson dem Parlament (ebd., S. 305f.). Im Gegensatz zum ISC befürwortete Anderson aber die Anordnung von Überwachungsmaßnahmen durch RichterInnen (ebd., S. 300f.).

Neben dem ISC kam damit eine zweite Untersuchung zu dem Ergebnis, dass es legislativen Handlungsbedarf gebe. Wie das ISC forderte aber auch Anderson im Gegensatz zu AktivistInnen keine substanzielle Beschränkung der Maßnahmen. Aber auch er legte eine juristische Kontrolle der Überwachungsanordnungen nahe und empfahl die Kontrollinstanzen zu stärken. Die Notwendigkeit einer potenten Beschützer-Rolle wurde auch in diesem Kontext mit Verweis auf die Erfahrungen mit Terrorismus begründet. Die Vorschläge zielten folglich darauf, ein ausgewogenes Verhältnis zwischen den Rollen als Garant liberaler Grundrechte und der Beschützer-Rolle herzustellen, nicht auf eine substanzielle Beschränkung.

Im Juni 2015 wurden die Berichte und ihre jeweiligen Empfehlungen im Unterhaus debattiert. In diesem Rahmen betonten RegierungsvertreterInnen, dass die Untersuchungen sowohl die Wichtigkeit der nachrichtendienstlichen Aufklärung unterstrichen und den Verdacht ausgeräumt hätten, die Dienste unterminierten bewusst die gesetzlichen Regelungen (House of Commons, 2015d, S. 1081-1083). Die Innenministerin mahnte weiterhin an, dass bei weiteren Diskussionen stets die Gefahrenlage bedacht werden müsse:

> »[…] these powers are about protecting and saving people's lives. In any debate about the right balance between security and privacy, it is important that we remember the full context of the threats we face. They include the threat from terrorism — both from overseas and home-grown in the UK. […] We also face other threats from organised criminals and the proliferation of cybercrimes such as child sexual exploitation, and threats from hostile foreign states and from military and industrial espionage.« (Ebd., S. 1084f.)

Die Priorität der Regierung lag daher darauf, dem Nachrichtendienst die nötigen Werkzeuge an die Hand zu geben, um die Sicherheit des Vereinigten Königreichs zu gewährleisten und dies im Einklang mit den bürgerlichen Freiheitsrechten umzusetzen (ebd., S. 1085).

Abgeordnete der parlamentarischen Opposition betonten ebenfalls die Bedeutung der Nachrichtendienste und deren »quiet heroism«, sie hoben aber auch die Notwendigkeit hervor, einen neuen gesetzlichen Rahmen für die Tätigkeiten der

Dienste zu schaffen und dabei darauf zu achten, dass die Kontrolle sowie die Befugnisse der Dienste angemessen seien (ebd., S. 1086). Die Labour Party erkannte ferner, wie die Regierung, dass es angesichts der vielfältigen Gefahren nicht zu einem Auslaufen der Befugnisse des DRIPA 2014 kommen dürfe, so dass die zeitliche Dringlichkeit einer Neuregelung überparteilich anerkannt wurde (ebd., S. 1087). Wie David Anderson forderte die Labour Party eine richterliche Anordnung für Überwachungsmaßnahmen. In diesem Kontext wiesen Abgeordnete darauf hin, dass das Vereinigte Königreich mit seiner Regelung auch innerhalb der 5-Eyes exponiert sei. Außerdem versprachen sie sich hiervon eine erhöhte Kooperationsbereitschaft von amerikanischen Internetunternehmen (ebd., S. 1089).

Vor diesem Hintergrund entwarf die Regierung 2016 eine Reform der bestehenden gesetzlichen Regularien mit dem Ziel, die Bedenken auszuräumen, ohne nachrichtendienstliche Befugnisse aufzugeben. Die Neuregelung erfolgte, aufgrund der besonderen Einstellung gegenüber dem Nachrichtendienst und den Erfahrungen mit Terrorismus, vor dem Hintergrund einer domestisch wenig kontestierten Beschützer-Rolle.

5.2.3 Stabilisierung und Ausbau der Beschützer-Rolle: Der Investigatory Powers Act 2016

Der Investigatory Powers Act, der auch aufgrund der erweiterten Befugnisse bei der Strafverfolgung von KritikerInnen den Spitznamen »Snoopers' Charter« bekam, beinhaltete für den Bereich der Nachrichtendienste Kompetenzzuwächse sowie neue Kontrollarrangements. Im November 2015 legte die Regierung einen ersten Gesetzentwurf zum IPA vor. Dieser sorgte sowohl international als auch domestisch für erhebliche Kritik.

Edward Snowden sah in dem Entwurf das umfassendste und am wenigsten kontrollierte Überwachungsgesetz in der westlichen Welt (Snowden, 2015). Der konservative Abgeordnete David Davis bemängelte, dass der Debatte in Großbritannien die angemessene Kritik an den vorgeschlagenen Maßnahmen fehle. Er führte diesen Umstand auf eine fehlende historische Sensibilität zurück:

> »We have a wonderful illusion about our security services, a very comforting illusion. […] Because for the past 200 years we haven't had a Stasi or a Gestapo, we are intellectually lazy about it, so it's an uphill battle.« (The Guardian, 2015a)

Die beständige historische positive Bezugnahme auf das GCHQ wurde aber nur von wenigen PolitikerInnen kritisiert.

Der Gesetzentwurf wurde in der Folge von drei parlamentarischen Ausschüssen evaluiert und mit VertreterInnen der Zivilgesellschaft und Wirtschaft diskutiert. Aus Sicht der Regierung stand am Ende dieses Prozesses ein Entwurf, der

sicherstellte, dass die Sicherheitsbehörden über die notwendigen Kompetenzen verfügten, um die Sicherheit des Vereinigten Königreichs bestmöglich zu gewährleisten, ohne dabei andere Rechte über Gebühr zu beschränken (UK Government, 2016d, S. 2).

Nach diesem Konsultationsprozess wurde der überarbeitete Gesetzentwurf im März 2016 in zweiter Lesung im Unterhaus debattiert. Die Innenministerin betonte in dieser Sitzung, dass der Austausch mit den verschiedenen Interessengruppen zu einem neuen transparenten Gesetz geführt hätte, das sowohl die Sicherheit als auch die bürgerlichen Freiheiten in angemessener Weise miteinander verbinde. Insbesondere verwies Theresa May auf die Neuerungen zum Schutz besonders sensibler Berufsgruppen (bspw. von AnwältInnen und JournalistInnen) sowie auf das explizite Verbot, ausländische Nachrichtendienste um das Abfangen von Daten von Personen innerhalb des Vereinigten Königreichs zu bitten. Ferner wies die Innenministerin auf die neue Institution des Investigatory Powers Commissioners hin, die die Funktionen der Interception of Communications Commissioner, Intelligence Services Commissioner und Chief Surveillance Commissioner bündelte, sowie die neue Praxis zur Anordnung von Überwachungsmaßnahmen, wonach diese nur gemeinsam durch eine/n MinisterIn und eine/n Judicial Commissioner erlassen werden können (sog. double-lock) (House of Commons, 2016a, S. 812f.). Außerdem führte sie aus, dass das Gesetz erstmals die Wilson Doktrin expliziere und damit das Abhören von Mitgliedern des Parlaments nur nach Anordnung durch die/den PremierministerIn möglich sei (ebd., S. 819). Aus Sicht der Regierung bildete der Entwurf damit ein Vorbild für andere Staaten:

> »The Bill will provide world-leading legislation setting out in detail the powers available to the police and the security and intelligence services to gather and access communications and communications data. It will provide unparalleled openness and transparency about our investigatory powers, create the strongest safeguards, and establish a rigorous oversight regime.« (Ebd., S. 813)

Um Kritiken zuvorzukommen, verwies May aber auch darauf, dass aufgrund der Sunset-Clause im DRIPA 2014, schneller legislativer Handlungsbedarf bestünde, um den neuen Gefahren weiterhin begegnen zu können (ebd., S. 813).

Aus Sicht der Regierung erhielt das Gesetz damit das Gleichgewicht zwischen den Rollen Garant liberaler Grundrechte und der Beschützer-Rolle. KritikerInnen sahen in dem Vorhaben einen übermäßigen Ausbau der Beschützer-Rolle.

Besondere Kontestation erfuhren die Pläne zur flächendeckenden Kommunikationsüberwachung (bulk Interception) bzw. zum flächendeckenden Eindringen in zahlreiche Computersysteme (bulk Equipment Interference) (ebd., S. 817). Letztere Maßnahme wurde mit dem IPA erstmals eingeführt und daher besonders kritisch beurteilt. Bulk Equipment Interference ist nicht an ein direktes Ziel gebunden, sondern kann auch mehrere Systeme betreffen. Sie ist aber explizit

darauf beschränkt gegen Ziele im Ausland eingesetzt zu werden, britische BügerInnen dürfen durch diese Maßnahme nicht in erster Linie (primarily) betroffen sein (Home Office, 2018a, S. 67).

Die Regierung hatte zu beiden Praktiken bereits im Entwurfsstadium Erklärungen abgegeben und deren Notwendigkeit betont. Zur bulk interception führte die Regierung aus, sie sei »a vital tool designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK« (UK Government, 2015c, S. 1). Die Regierung wollte damit den Regelungen nach Section 8(4) RIPA eine neue Grundlage geben. Mit Blick auf bulk Equipment Interference argumentierte die Regierung, dass durch die technologische Entwicklung das Abhören von Kommunikation nur noch begrenzt nützlich sei, da die Daten aufgrund von Verschlüsselung nicht mehr auswertbar seien. Aus diesem Grund sei es notwendig den Nachrichtendiensten die Möglichkeit einzuräumen, notfalls auch viele Geräte zu infiltrieren (UK Government, 2015b, S. 1f.). Sie führte ferner aus, dass zwar aufgrund der paketvermittelten Kommunikation in einem globalen Netz, nicht immer genau zwischen in- und ausländischer Kommunikation unterschieden werden könne, dass in beiden Fällen aber inländische Kommunikation nur dann analysiert werden dürfe, wenn eine ergänzende Anordnung durch die/den zuständigen MinisterIn vorläge, die durch eine/n Judicial Commissioner überprüft wurde (UK Government, 2015b,c).

Beide Praktiken wurden bereits in einem offenen Brief vor der parlamentarischen Debatte durch JuristInnen als unverhältnismäßig abgelehnt (The Guardian, 2016). Auch Bürgerrechtsorganisationen kritisierten die Praktiken mit dem Hinweis, dass etwa durch die Zurückhaltung von Sicherheitslücken das Netz insgesamt für alle NutzerInnen unsicherer werde (Big Brother Watch, 2016). Die Regierung argumentierte dagegen, dass diese Maßnahmen unerlässlich seien. Bei fast allen Terrorismusermittlungen sowie bei zahlreichen Einsätzen der Streitkräfte seien derartige Praktiken erfolgreich genutzt worden (House of Commons, 2016a, S. 822f.). Die DUP kritisierte als einzige Oppositionspartei den Regierungsentwurf nicht substanziell. Sie verwies hierzu auf die Erfahrungen mit Terrorismus in Nordirland (ebd., S. 842).

Bei der Abstimmung über das Gesetz enthielten sich die Abgeordneten der Labour Party, da sie einerseits die Notwendigkeit anerkannten, ein neues Gesetz zu erlassen um nicht durch die Sunset-Clause eine Situation zu generieren, in der das Handeln der Sicherheitsbehörden eingeschränkt wäre. Andererseits sahen sie im Vorschlag der Regierung Defizite bei der Wahrung der bürgerlichen Freiheitsrechte. Die neuen Kontrollarrangements waren für viele Abgeordnete nur »kosmetischer« Natur und nicht mit substanziellen Verbesserungen verbunden (ebd., S. 825 bzw. 828f.). Ferner kritisierten sie die zu vage Zielbestimmung des ökonomischen Wohlergehens. Sie vermuteten darin eine verdeckte Überdehnung der Beschützer-Rolle: »This raises the issue of what extra activities the Government

want to cover under this banner that are not covered by national security« (House of Commons, 2016a, S. 831).[8] Aus Sicht der Rollentheorie war dies die Forderung, die Rollenreferenz zu klären. Da in der Vergangenheit Gewerkschaftsmitglieder unter ähnlichen Rechtfertigungen zu Unrecht abgehört worden waren (ebd., S. 831 bzw. 834). Die Abgeordneten sahen zwar ebenfalls die von der Regierung angeführten Gefahren wie Terrorismus und organisierte Kriminalität, dennoch bestanden Zweifel, ob die Fähigkeiten zu bulk interception bzw. bulk Equipment Interference tatsächlich in diesem Maße notwendig waren, da hiermit eine neue Qualität der Überwachung verbunden sei (ebd., S. 833). Ähnlich argumentierten auch Abgeordnete der SNP (ebd., S. 838-844).

International stieß der Plan der Regierung, flächendeckende Überwachung sowie systematisches Hacken auf eine gesetzliche Grundlage zu stellen, ebenfalls auf Widerstand. Der UN-Sonderberichterstatter Joseph Cannataci kritisierte den Gesetzentwurf und forderte die britische Regierung auf:

> »to take this golden opportunity to set a good example and step back from taking disproportionate measures that may have negative ramifications far beyond the shores of the United Kingdom. More specifically, the Special Rapporteur invites the Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other States by continuing to propose measures, especially bulk interception and bulk hacking« (United Nations, 2016b, S. 14)

Diese Kritik wurde von Bürgerrechtsorganisationen geteilt (Liberty, 2016a; Open Rights Group, 2016b) und auch im Parlament erörtert (House of Commons, 2016a, S. 826). Die parlamentarische Opposition warf der Regierung vor, mit dem Gesetz autokratischen Bestrebungen zur Kontrolle des Internets zu folgen und damit einen gefährlichen Präzedenzfall zu etablieren (ebd., S. 844). Ferner argumentierten KritikerInnen, dass die Regierung mit dem Gesetz, im Gegensatz zu den USA, die falschen Schlussfolgerungen aus den Snowden-Enthüllungen zöge und nicht eine Begrenzung der flächendeckenden Überwachung einleite, sondern das Gegenteil hiervon verfolge (ebd., S. 863).

Trotz der Kontestationen aus Zivilgesellschaft und den Reihen der parlamentarischen Opposition wurde der Gesetzesentwurf im März in zweiter Lesung durch das Unterhaus mit der Regierungsmehrheit verabschiedet (ebd., S. 904).

8 Die Regierung hatte schon mit dem DRIPA 2014 versucht, die Verbindung zwischen ökonomischem Wohlstand und nationaler Sicherheit zu definieren. Sie stellte damit klar, dass es um das ökonomische Wohlergehen nur dann gehe, wenn dieses mit der nationalen Sicherheit verbunden sei (The Stationery Office, 2014, Section 3). Diese Festlegung wurde von der Opposition aber als defizitär betrachtet.

Aufgrund der Bedenken zu den besonders sensiblen »Bulk Powers« und auf Drängen der parlamentarischen Opposition, folgte im anschließenden Konsultationsprozess aber eine erneute kritische Auseinandersetzung mit deren Implikationen. Das Joint Committee on Human Rights gelangte bei der Prüfung zu dem Ergebnis, dass deren Einsatz nicht grundsätzlich gegen Artikel 8 der Europäischen Menschenrechtskonvention verstoße, obwohl ein deutliches Spannungsverhältnis konstatiert wurde (House of Lords und House of Commons, 2016, S. 12). Die Ausschussmitglieder forderten daher von der Regierung, den operativen Nutzen der Maßnahmen nachzuweisen und sie daher durch den Independent Reviewer of Terrorism Legislation (David Anderson) eingehend prüfen zu lassen (ebd., S. 13).

Diese Evaluation wurde im Juni 2016 abgeschlossen. In seinem Bericht kam Anderson zu der Einschätzung, dass eine umfassende, strategische Überwachung von Internetkommunikation (bulk Interception) essenziell zur Gewährleistung der Sicherheit im Vereinigten Königreich sei. Die Maßnahmen hätten sich in unterschiedlichen Einsatzszenarien als überaus hilfreich herausgestellt, darunter die Bekämpfung von Terrorismus, die Abwehr von Cyberangriffen oder die Unterstützung der Streitkräfte. Hierbei sei gleichermaßen der Zugriff auf Meta- wie Inhaltsdaten wichtig. Mit anderen, weniger invasiven, Maßnahmen sei ein ähnliches Ergebnis nicht zu erreichen. Daher war die Praxis aus Sicht von Anderson auch nicht ersetzbar. Er gab aber zu bedenken, dass durch die zunehmende Verbreitung von Verschlüsselung diese Maßnahme potenziell an Wirksamkeit verlieren könnte (Anderson, 2016, S. 91).

Die Fähigkeit zum umfassenden Hacken von Systemen (bulk Equipment Interference) wurde daher von Anderson als eine potenzielle Weiterentwicklung der Überwachung am Übertragungsweg gesehen. Auch wenn es zum Zeitpunkt der Prüfung noch keine Anwendungsfälle zur Evaluation der operativen Nützlichkeit gab (ebd., S. 109). Aufgrund des potenziell besonders tiefen Eingriffs in die Privatsphäre mahnte er aber an:

> »[…] that bulk EI will require, to an even greater extent than the other powers subject to review, the most rigorous scrutiny not only by the Secretary of State but by the Judicial Commissioners who must approve its use and by the IPC which will have oversight of its consequences.« (Ebd., S. 110)

Damit stützte Anderson die Einschätzung der Regierung wonach die Fähigkeiten zur Gewährleistung der Sicherheit notwendig seien. VertreterInnen aus Zivilgesellschaft und Wirtschaft hatten diese Position wiederholt kritisiert.

Im parlamentarischen Prozess wurde die Beschützer-Rolle zwar kontestiert, nach einer Prüfung durch Anderson wurden die Maßnahmen, insbesondere die bulk Equipment Interference, aber als notwendig beurteilt. Gegen die Pläne zum staatlichen Hacken gab es allerdings aus der Netzgemeinde bereits seit 2015 Widerstände, sodass es hier zu noch anhaltenden Kontestationsprozessen kam.

2015 wurde von der Regierung erstmals öffentlich eingeräumt, dass die Nachrichtendienste zur Erfüllung ihrer Aufgaben auf das Hacken von IT-Systemen zurückgriffen. Im Februar 2015 veröffentlichte die Regierung unter dem Druck eines laufenden Prozesses vor dem IPT eine offizielle Richtlinie zu dieser Praxis (Home Office, 2015b). Dies führte zu einer Klage verschiedener Bürgerrechtsorganisationen zusammen mit britischen Wirtschaftsunternehmen. Die KlägerInnen sahen die Hacking-Praktiken nicht durch bestehende gesetzliche Regelungen gedeckt und als tiefgreifenden Eingriff in die Privatsphäre, der sensiblere Bereiche betreffe als die Überwachung von Kommunikationsverkehren (Investigatory Powers Tribunal, 2015d, S. 4f.). Ein Vertreter des britischen ISP GreenNet äußerte Bedenken über das Ausmaß der CNE-Aktivitäten des britischen Nachrichtendienstes, die im Zuge des Prozesses aufgedeckt worden waren:

> »We remain extremely concerned that Ed Snowden was right about GCHQ having the most intrusive capabilities of any security agency, and about exactly how widespread their computer network exploitation may be, and the risks to network security and the privacy, freedom and safety of internet users around the world.« (Privacy International, 2015a)

Das IPT wies die Klage im Februar 2016 aber zurück und erkannte in den CNE-Operationen der Nachrichtendienste kein rechtswidriges Verhalten, sondern beurteilte die Praxis als prinzipiell rechtmäßig (Investigatory Powers Tribunal, 2016).

Die KlägerInnen reichten in der Folge Klage vor dem Europäischen Gerichtshof für Menschenrechte und dem Supreme Court ein. Das Verfahren vor dem Europäischen Gerichtshof für Menschenrechte ist noch anhängig. Im September 2019 schlossen sich weitere Bürgerrechtsorganisationen der Klage an (Article 19, 2019). Nachdem Liberty mit Klagen vor dem High Court und dem Court of Appeal gescheitert war, reichte die Bürgerrechtsorganisation zusammen mit sieben ISPs Klage vor dem Supreme Court ein. Ziel dieser Klage war es, dafür zu sorgen, dass Urteile des IPT weiterer juristischer Prüfung offenstehen sollten. Eine richterliche Prüfung war gesetzlich nicht vorgesehen und die vorigen Klagen waren mit Verweis hierauf abgelehnt worden. Der neue IPA sah zwar im Gegensatz zu RIPA prinzipiell eine begrenzte Möglichkeit zur Berufung vor (Section 241). Diese trat am 1. Januar 2019 in Kraft (Home Office, 2018c), wurde aber von KritikerInnen bereits während der Konsultation des Gesetzes als unzureichend bewertet (House of Commons, 2016a, S. 881). Im Mai 2019 urteilte der Supreme Court zugunsten der KlägerInnen und unterwarf damit die Entscheidung des IPT weiterer gerichtlicher Prüfung. Ein Argument, das die RichterInnen zur Begründung der Entscheidung anführten, war, dass sich die Gesetzesinterpretation des IPT losgelöst von Rechtsprechung in anderen Gebieten entwickeln könnte: »Consistent application of the rule of law requires such an issue to be susceptible in appropriate cases to review by ordinary courts« (The Supreme Court, 2019, S. 58).

Privacy International und andere VertreterInnen der Zivilgesellschaft feierten dies als Sieg für den Schutz der Bürgerrechte, da die Entscheidungen des IPT damit nicht mehr unanfechtbar waren und auch die Entscheidung zur CNE wieder vor Gericht überprüft werden kann:

> »Privacy International's tenacity in pursuing this case has provided an important check on the argument that security concerns should be allowed to override the rule of law. Secretive national security tribunals are no exception. The Supreme Court was concerned that no tribunal, however eminent its judges, should be able to develop its own ›local law‹. Today's decision welcomes the IPT back from its legal island into the mainstream of British law.« (Privacy International, 2019)

Andere JuristInnen sahen in dem mit vier zu drei Stimmen gefällten Urteil aber einen Bruch der Parlamentssouveränität, das mit der ursprünglichen Regelung eine weitere richterliche Prüfung ausschließen wollte (ouster clause) (The Guardian, 2019b). Inwiefern eine substanzielle Herausforderung der Bulk Powers erfolgversprechend ist, bleibt zweifelhaft, da der High Court im Juli 2019 urteilte, die Kompetenzen stünden nicht im Widerspruch zum Human Rights Act 1998 und eine Klage von Liberty damit ablehnten (High Court of Justice, 2019). Liberty kündigte aber an, trotz des Urteils weitere Klagen gegen das nachrichtendienstliche Hacking voranzutreiben (Liberty, 2019).

Während dieser laufenden Kontestationsprozesse hatte die Regierung die Praxis der bulk Equipment Interference aber zunehmend ausgebaut. Im November 2018 veröffentlichte das GCHQ zusammen mit dem 2016 gegründeten National Cyber Security Centre (NCSC) den sogenannten Equities Process, mit dem darüber entschieden wird, ob eine Sicherheitslücke für das Hacken von IT-Systemen zurückgehalten oder zum Schließen der Schwachstelle veröffentlicht wird.[9] In der Pressemitteilung wird die grundsätzliche Problematik des Umgangs mit ausnutzbaren Softwareschwachstellen thematisiert: »[…] we do not disclose every vulnerability we find. In some cases, we judge that the UK's national security interests are better served by ›retaining‹ knowledge of a vulnerability« (GCHQ, 2018b).

Bei diesem Prozess stünden stets zwei Ziele im Widerspruch, die sorgsam gegeneinander abgewogen werden müssten. Einerseits könne durch die Veröffentlichung der Information die Schwachstelle für alle NutzerInnen geschlossen und damit die Sicherheit des Netzes insgesamt erhöht werden. Andererseits könne eine Sicherheitslücke aber auch genutzt werden, um nachrichtendienstlich Informationen über Gefahren zu sammeln oder Aktivitäten potenziell feindseliger

9 Das National Cyber Security Centre ist Teil des GCHQ, soll aber öffentlich sichtbarer für die Cybersicherheit im Vereinigten Königreich sorgen.

Akteure (Terrorgruppen, Staaten oder Krimineller) zu vereiteln. Die Standardentscheidung sei dabei stets, Informationen zu veröffentlichen. Die Entscheidung über den Umgang mit einer Lücke treffen VertreterInnen der Nachrichtendienste und des NCSC. In besonders sensiblen Fällen werden die/der DirektorIn des GCHQ und die/der AußenministerIn in die Beurteilung einbezogen. Bei der Entscheidungsfindung wird unter anderem beurteilt, gegen welche Ziele die Schwachstelle eingesetzt werden kann und welche Informationen durch sie erlangt werden können. In die Gleichung fließt aber auch die Risikoeinschätzung ein, welche Ziele im Vereinigten Königreich durch diese Schwachstelle angreifbar wären (bspw. kritische Infrastrukturen) und wie hoch die Wahrscheinlichkeit ist, dass die Lücke durch andere gefunden und ausgenutzt wird (GCHQ, 2018d). Der mit dem IPA etablierte Investigatory Powers Commissioner kontrolliert diese Abwägung. Der neue Prozess sollte diese Entscheidungsfindung transparent und die angelegten Maßstäbe nachvollziehbar machen (GCHQ, 2018b).

Im Dezember 2018 unterrichtete die Regierung das ISC und den Investigatory Powers Commissioner, dass die bulk Equipment Interference deutlich häufiger eingesetzt werden würden als antizipiert. Zunächst war die Regierung davon ausgegangen, dass auf das systematische Hacken nur selten zurückgegriffen werden müsse. Diese Einschätzung hatte sich aber seit der Verabschiedung des IPA verändert. Diese Anpassung wurde mit technischen Veränderungen (Verschlüsselung) begründet, die dazu führten, dass andere Maßnahmen weniger effektiv geworden waren (Home Office, 2018b).

Die Beschützer-Rolle ist mit Blick auf die bulk Equipment Interference domestisch nach wie vor kontestiert und steht auch international in der Kritik. Insbesondere mit der bulk Equipment Interference konnte die britische Regierung die Beschützer-Rolle im Bereich der Nachrichtendienste ausbauen. Diese Erweiterung hat einen anhaltenden Kontestationsprozess ausgelöst, es ist aber unwahrscheinlich, dass diese Kontestationen domestisch folgenreich sein werden. Dies liegt daran, dass die Maßnahme nach der Prüfung durch David Anderson auch von großen Teilen des Parlaments akzeptiert wird und dass die britischen Gerichte bereits die Einschätzung vertreten haben, die Praxis sei grundsätzlich zulässig.

5.3 Zwischenfazit

Im Lichte der durch die Snowden-Enthüllungen entstandenen Öffentlichkeit, mussten die Regierungen beider Untersuchungsstaaten ihre Beschützer-Rollen evaluieren. Die Veröffentlichungen wurden in beiden Staaten allerdings unterschiedlich aufgenommen. Während die britische Regierung die Publikation der Dokumente verurteilte und offensiv gegen den Guardian vorging, um weitere