The UK intelligence community before and after Snowden

Professor Richard J. Aldrich

Department of Politics and International Studies (PaIS)

University of Warwick

Report requested by the German Bundestag

Printed paper 18/843

18th electoral term 18.03.2014

Committee of Inquiry on Intelligence

Die britischen Nachrichtendienste vor und nach Snowden

Professor Richard J. Aldrich

Akronyme

CIA	Central Intelligence Agency
Comsec	Communications security
DSMA	Defence and Security Media Advisory Notice System (DA-Notice)
Elint	Electronic intelligence
GCHQ	Government Communications Headquarters
IMP	Intercept Modernisation Programme
IPT	Investigatory Power Tribunal
IRTL	Independent Reviewer of Terrorism Legislation
ISC	Intelligence and Security Committee, UK Parliament
JIC	Joint Intelligence Committee
MI5	Security Service
MI6	Secret Intelligence Service (auch SIS)
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NSA	National Security Agency
NSC	UK National Security Council
OSA	Official Secrets Act
PSIS	Permanent Secretaries Committee on the Intelligence Services
RCUK	Research Councils UK
RIPA	Regulation of Investigatory Powers Act 2000
SAS	Special Air Service
Sigint	Signals intelligence
SIS	Secret Intelligence Service (also MI6)
TCG	Tasking and Co-ordinating Group
TPIMs	Terrorist Prevention and Investigation Measures
WIF	Warwick Intelligence Futures project
WMD	Weapons of Mass Destruction

Die britischen Nachrichtendienste vor und nach Snowden

1. Zusammenfassung

Wenige Felder der Staatstätigkeit besitzen größere Bedeutung als die elektronische Aufklärung und Internetsicherheit. Durch die Enthüllungen Edward Snowdens wurde diesem Thema große öffentliche Aufmerksamkeit zuteil. Die National Security Agency (NSA) und ihre Partner, mit denen sie vor dem Hintergrund von Globalisierung und Terrorismus Daten austauscht, sind rasch gewachsen. In unsicheren Zeiten scheint größeres Wissen oft ein Wundermittel für Sicherheitsfragen zu sein. Ob sich globale Herausforderungen als internationaler Terrorismus, organisierte Kriminalität, Krankheiten oder demographische und sozioökonomische Veränderungen darstellen – es ist allgemein üblich, sich bei gesellschaftlichen Risiken an wissensintensive Organisationen zu wenden. Im Zentrum dieser Aktivitäten stehen heute die z. B. durch soziale Medien, Netzkarten oder Kundenkarten gewonnenen Daten.

Der Staat verfügt längst nicht mehr über den Großteil dieser Daten. Die gravierendste Veränderung des letzten Jahrzehnts besteht darin, dass „Überwachung“ mit „Einkaufen“ verschmilzt und keine Domäne spezialisierter staatlicher Einrichtungen mehr ist; sie hat die Gesellschaft erreicht. Heute sind die großen Sammler nachrichtendienstlich verwertbarer Informationen die Banken, Fluggesellschaften, Supermärkte, Internetanbieter und Telekommunikationsunternehmen. Jede Organisation – ob im öffentlichen oder privaten Sektor – sammelt, speichert und übermittelt heute Daten in noch nie dagewesenem Ausmaß, häufig über Ländergrenzen hinweg. Typisches Beispiel für diese Entwicklung sind Fluggesellschaften; sie sind eifrige Erfasser und ebenso Abnehmer aufbereiteter Daten für kommerzielle und Sicherheitszwecke. Sind solche Organisationen die Sicherheitsbehörden der Zukunft?

Welche Folgen hat das? In Großbritannien werden die Konsequenzen häufig finster dystopisch dargestellt. Doch die Menschen sind heute durch moderne Kommunikationsmittel immer enger miteinander verbunden. Potenziell ermöglicht das neue Zeitalter „wissensintensiver Sicherheit“ engere Partnerschaften und offenere Formen der Politikgestaltung, wodurch Geheimhaltung und Vertraulichkeit in Staat und Wirtschaft ebenso schwinden wie die Privatsphäre. Aber dies setzt größeres Vertrauen darin voraus, wie Unternehmen und Regierungen mit personenbezogenen Daten umgehen, zusammen mit „pauschalen“ Datenschutzrechten. Wir brauchen ferner grundlegend neue Ansätze und neue Konzepte, sollen die Aufsicht verbessert und das Vertrauen der Öffentlichkeit erhalten bleiben. Die Politik braucht dringend eine Lösung, denn: Informations- und Kommunikationstechnologien entwickeln sich rasant weiter, während sie für Minister und Unternehmensvorstände häufig noch ein Rätsel bleiben.

Parlamente, Justiz, Menschenrechtsorganisationen und Medien mühen sich, ihre Potenziale und Gefahren zu erfassen. Kurz: Die Folgen elektronischer Aufklärung und Internetsicherheit sind zwar wichtig, aber bislang noch zu wenig verstanden und reguliert. Wie Geheimdienstarbeit selbst sind ihre Kontrolle und der Schutz von Rechten zunehmend verteilte Aktivitäten. Bestimmend sind hier nicht mehr reguläre Ausschüsse, sondern die globale Zivilgesellschaft mit breiten Bündnissen von Whistleblowern, Journalisten, Wissenschaftlern, Aktionsgruppen,

Anwälten und NGO. Diese flexiblen „Spionageabwehr"-Bündnisse arbeiten uneinheitlich, haben jedoch den Vorteil, dass sie die multinationalen Allianzen der Nachrichtendienste widerspiegeln. Den nationalen Regierungen bereitet die „Regulierung durch Enthüllung" Sorge; sie arbeiten mit Nachdruck daran, Whistleblower zu zügeln. Will die britische Regierung jedoch den Stillstand auf diesem schwierigen Terrain überwinden, wird sie wohl dem Rat von David Anderson, des vom Antiterrorgesetz autorisierten *Independent Reviewer of Terrorism Legislation*, folgen müssen und sich für eine gerichtliche Prüfung von Anordnungen zur Überwachung entscheiden. Sie wird ferner effizientere Mechanismen für eine Überprüfung der internationalen nachrichtendienstlichen Zusammenarbeit brauchen.

2. Aufgabe

Die Aufgabe besteht darin zu untersuchen, wie in Großbritannien das Parlament, die Massenmedien und die Wissenschaft die folgenden Themen diskutieren:

1. Arbeit (Leistung, Abläufe) der britischen Nachrichtendienste.

2. Parlamentarische Kontrolle der Nachrichtendienste.

3. Schutz der Privatsphäre und der Freiheitsrechte in Großbritannien.

4. Dies ist im Rahmen eines anderen Fragenkomplexes der Untersuchung zu betrachten. Auch darauf werde ich versuchen einzugehen, bin mir aber bewusst, dass diese allgemeineren Fragen nicht unmittelbar zu meinem Auftrag gehören.

5. Das Fazit extrahiert daraus den breiteren und technologischen Kontext, in dem sich das britische Geheimdienstwesen wandelt, und unterbreitet einige wenige Vorschläge.

3. Ansatz, Quellen und Methoden

Über die britischen Nachrichtendienste und Sicherheitsbehörden ebenso wie über ihre Kontrolle und Regulierung gibt es zahlreiche Darstellungen und Übersichten. Dagegen ist die Aufgabe hier eine beratende und kommentierende; ich stütze mich dabei auf eine umfassende Diskussion dieser Angelegenheiten, die seit den 1980er Jahren in der Wissenschaft geführt wird.

Seit mehr als drei Jahrzehnten werden in Großbritannien die Nachrichtendienste und Sicherheitsbehörden wissenschaftlich untersucht (Andrew und Dilks 1984). Dementsprechend berücksichtigen meine Ausführungen über lange Zeiträume gesammelte Daten. Sie stützen sich ferner auf das Projekt *Warwick Intelligent Futures* (WIF) und ein in Kürze erscheinendes Buch über die britische Kernexekutive und die Nachrichtendienste (2016). Von 2008 bis 2012 führte Warwick gemeinsam mit der Universität Nottingham zwei Projekte der

Wissenschaftsförderorganisation *Arts and Humanities Research Council* (AHRC) durch, deren Ergebnisse in dieses Gutachten einfließen. Ferner wurden im Sommer 2015 weitere Recherchen zum Untersuchungsgegenstand durchgeführt. Es handelt sich hier um eine wissenschaftliche Analyse, die bestrebt ist, die britischen Entwicklungen in einen größeren Zusammenhang zu stellen; sie umfasst ferner einige Anmerkungen zur Entwicklung in den nächsten zehn Jahren. Es ist wohl angebracht darauf hinzuweisen, dass ich keiner Sicherheitsüberprüfung unterzogen wurde und daher keinen bevorrechtigten Zugang zu Verschlusssachen habe.

4. Erklärung zur Ethik

Bei den Recherchen zu dieser Untersuchung und zu anderen verwandten Projekten war ich stets um die Einhaltung wissenschaftsethischer Standards bemüht. Ich halte mich an die Richtlinien des Warwick University Research Ethics Committee und die *Policy and Guidelines on Governance of Good Research Conduct* der britischen Wissenschaftsförderorganisationen (RCUK 2015).

5. Das Ende der Nachrichtendienste?

Das 21. Jahrhundert wird durch *Big Data*, größere Mobilität und höheren individuellen Vernetzungsgrad gekennzeichnet sein. Geschwindigkeit und Ausmaß der Veränderungen sind beachtlich. IBM schätzt, dass 90 Prozent der Daten weltweit in den letzten zwei Jahren entstanden sind. Weltweit wurden 2012 mehr als acht Billionen Kurznachrichten (SMS) verschickt. In fünf Jahren wird alles, was wir im Laden für mehr als zehn Euro kaufen, eine IP-Adresse haben und Informationen über seine Umgebung sammeln. Viele Nutztiere in der Landwirtschaft tragen SIM-Karten, die ihren Gesundheitszustand übermitteln, und in zehn Jahren wird es überall ein entsprechendes Body-Monitoring für Menschen geben. In zwanzig Jahren wird zum Verschicken von E-Mails ein Blinzeln genügen. In Städten wie Berlin, London, New York und Toronto wird der Großteil menschlicher Interaktion aufgezeichnet werden. Diese Daten werden nicht nur einen unvorstellbaren Umfang haben, sondern auch über Mobilgeräte, die immer enger in den Körper (und letztendlich den Geist) integriert werden, immer leichter zugänglich werden. Wer sorgt für die Sicherheit dieser unserer digitalen Schatten? Und werden sie uns einschränken – oder uns zu mehr Fähigkeiten und Freiheiten verhelfen?

In unsicheren Zeiten wird größeres Wissen häufig als Wundermittel für Sicherheitsfragen dargestellt. Ganz gleich, ob Sicherheitsprobleme im Kontext herkömmlicher Gefechte (die keineswegs der Vergangenheit angehören), von Aufständen und internationalem Terrorismus, organisierter Kriminalität, Friedenssicherung oder humanitären Hilfsmaßnahmen betrachtet werden – es ist üblich, darauf mit wissensintensiven Organisationen zu reagieren, die sich auf Big Data zur Risikobewältigung stützen. Ferner: Da die Mehrzahl der Operationen sich nach General Rupert Smith hinab verlagert in Richtung auf einen „war amongst the people“ (Krieg unter Menschen), rückt der Mensch mehr und mehr in den Mittelpunkt nachrichtendienstlicher Arbeit (Smith 2007). Heute senden die Menschen einen stetigen Strom „elektronischer Abgase“ aus (so eine CIA-Formulierung), wobei die Daten aus so alltäglichen Quellen wie Tweets, Kundenkarten oder Spiele-Chatrooms stammen und das Geheimdienstwesen verändern werden, sodass wir uns auf etwas hinbewegen, was sich vielleicht als „wissensintensive Sicherheit“ bezeichnen lässt.

Ein interessanter Aspekt dieser Entwicklung sind die sich verändernden Datenschutzrechte. Früher befanden sich Daten von Interesse für die Nachrichtendienste hauptsächlich im Bereich der Regierung; dies verlagert sich allmählich insofern, als der Sicherheitsschwerpunkt mehr und mehr auf innerstaatlichen Konfrontationen, Aufständen und der Masse liegt. Die wichtigste Veränderung des letzten Jahrzehnt liegt darin, dass „Überwachung" mit Reisen und Einkaufen zusammenfließt. Sie ist keine Domäne spezialisierter staatlicher Behörden mehr; sie hat das Internet und sogar die Gesellschaft allgemein erreicht. Zu den großen Datensammlern, die für die Sicherheitsbehörden von Interesse sind, gehören Banken, Fluggesellschaften, Supermärkte, Internetanbieter und Telekommunikationsunternehmen. Zahlreiche Organisationen – ob im öffentlichen oder privaten Sektor – sammeln, speichern und übermitteln heute Daten in noch nie dagewesenem Ausmaß, häufig über Ländergrenzen hinweg. Fluggesellschaften und Flughäfen sind deshalb gute Beispiele für *Dual-Use*-Geheimdienstpartner, weil sie sowohl selbst in großem Umfang Daten sammeln als auch „Kunden" aufbereiteter Daten für kommerzielle, Sicherheits- und militärische Zwecke sind.

Was folgt aus dem Vormarsch von Big Data? Die Konsequenzen sind beunruhigend und unterlaufen herkömmliche vertraute Kategorien. Die Grenzen zwischen nachrichtendienstlichen Informationen und anderen Daten, zwischen Offenheit und Geheimhaltung, auch zwischen „privat" und „öffentlich" scheinen rasch zu verschwimmen. Aber es eröffnet auch faszinierende Möglichkeiten für neue Public-Private-Partnerships und verstärkte Berichtspflichten. Bestes Beispiel ist die Internetsicherheit. Hier kooperieren einst nur im Verborgenen wirkende Regierungsbehörden, deren Namen noch vor zehn Jahren der Öffentlichkeit unbekannt waren, offen und erfolgreich mit allen gesellschaftlichen Bereichen, um unsere elektronische Infrastruktur zu schützen. Von Nachrichtendiensten und Sicherheitsbehörden erwartet man möglicherweise, ihr Tun viel offener zu erklären. Wir bewegen uns vielleicht in Richtung auf eine „transparente Gesellschaft" (David Brin), in der sich Geheimhaltung und Privatsphäre radikal verändern, was für Staat, Wirtschaft und Bürger erheblichen potenziellen Nutzen birgt. Privatsphäre, Geschäftsgeheimnisse und amtliche Verschlusssachen werden erodiert; viel wird davon abhängen, wie entsprechende Datenschutzrechte geklärt werden (Brin 1999).

Idealerweise profitieren die Nachrichtendienste als positive Kraft und auch die übergeordneten Behörden mit ihren Aufsichts- und Kontrollfunktionen von der Tatsache, dass die Menschen heute vernetzter oder gar der Vernetzung „verfallen" sind (Agar 2003). Potenziell ermöglicht das neue Zeitalter „wissensintensiver Sicherheit" engere Partnerschaften und offenere Formen der Politikgestaltung. Dies erfordert jedoch ein hohes Maß an Vertrauen darin, wie alle möglichen Arten von Unternehmen und die Sicherheitsapparate mit personenbezogenen Daten umgehen. Wir brauchen ferner innovative Ansätze und neue Konzepte, soll das Vertrauen der Öffentlichkeit erhalten bleiben. Die Aufgabe muss dringend gelöst werden, denn: Informations- und Kommunikationstechnologien entwickeln sich rasant weiter, während das Thema für Minister und Unternehmensvorstände häufig noch ein Rätsel bleibt. Parlamente, Justiz, Menschenrechtsorganisationen und Medien mühen sich, ihre Gefahren zu erfassen. Kurz: Big Data mag wirtschaftliche, gesellschaftliche und politische Vorteile haben, von der Mehrheit der an Sicherheitspolitik Beteiligten wird der Komplex jedoch kaum ganz verstanden.

Wissensintensive Sicherheit beinhaltet auch für die Geheimdienst- und Sicherheitsapparate komplexe Fragen, weil sie das Geheimdienstwesen mit anderen wissensintensiven Aktivitäten verbindet – von Energie über Verkehr bis zum Gesundheits- und Sozialwesen. Wir müssen sehr viel vorurteilslosere Fragen zu den gesellschaftlichen Konsequenzen wissensintensiver Sicherheit

stellen. Kann wissensintensive Sicherheit ein offeneres und flexibleres Konzept für Operationen der staatlichen Sicherheitskräfte fördern? Welche Rolle werden Unternehmen spielen, was bedeutet es für die Rüstungswirtschaft? Wie wird die Sicherheit wissensintensiver Systeme national und international geregelt? Wie wird das Vertrauen der Öffentlichkeit in wissensintensive Systeme erhalten, wenn der Staat sie einsetzt? Schließlich, und nach der „Snowden-Krise" wohl am wichtigsten: Was bedeutet wissensintensive Sicherheit für Bürgerrechte und unsere die nationale Sicherheit regelnden Gesetze?

Das Geheimdienstwesen muss die transformierenden Technologien zu den gesellschaftlichen Aspekten von Information in Beziehung setzen, um zu einer „neue Vision" seiner Rolle beizutragen, die mehr auf Konsens und Partnerschaft gründet. Diese erfordert modernste Forschung und ein ganzes Spektrum sozial- und naturwissenschaftlicher Methoden. Das birgt ein beträchtliches Potenzial. Wissensintensive Sicherheit wird nicht nur die Zukunft des Militärwesens, der Weltwirtschaft und der modernen Gesellschaft bestimmten, sondern auch dafür sorgen, dass sie vernetzter sind, und das oft in überraschender Weise. In den kommenden zehn Jahren wird Big Data alle Lebensbereiche durchdringen. Zu verstehen, wie digitale Güter vor Missbrauch geschützt und positiv zur Effizienzsteigerung genutzt werden können, wird unsere Möglichkeiten für Wohlstand und Nachhaltigkeit unserer Gesellschaften erweitern. Aber die Herausforderungen für das Geheimdienstwesen sind enorm, weil die technologische Entwicklung rasant fortschreitet und unsere Gesellschaften zunehmend von Daten abhängen werden.

Wie dem auch sei, in Kooperation verfügen Universitäten, die großen Internetanbieter und die Sicherheitsbehörden auf diesem Gebiet über vorzügliche Stärken und das Potenzial, zum Thema der wissensintensiven Sicherheit kreative Ansätze beizusteuern. Um Risiken erfolgreich zu bewältigen, Konsens herzustellen und zu glaubwürdiger Kontrolle zu gelangen, brauchen wir eine stärkere Verflechtung von Menschen, Organisationen und Nationalstaaten. Fortschritte in diesem Bereich erfordern nicht nur, naheliegende Bedrohungen antizipieren zu können, sondern auch langfristige Veränderungen auf dem weiteren Feld der Politikgestaltung und der Gesellschaft zu verstehen, ebenso wie diese mit technologischer Entwicklung zusammenspielen.

Nachrichtendienste und Sicherheitsbehörden leben heute, wie Rovner (2013) es formuliert, im „Twitter-Zeitalter". Wir erleben nicht nur radikale Veränderungen im Geheimdienstwesen, vielleicht sogar sein Ende als im Verborgenen operierende und in Spezialgebiete unterteilte Disziplin im herkömmlichen Sinne, sondern auch das Schwinden der Geheimhaltung, nicht zuletzt weil neue Geheimdienstpraktiken eine zusätzliche Kontrolle durch die Massenmedien hervorbringen. Zwar gewinnt durch die neue Sozialökologie des Sicherheitswesens das Vertrauen der Öffentlichkeit immer mehr an Bedeutung, doch vollzieht sich dieser Wandel paradoxerweise vor dem Hintergrund einer Reihe von Ereignissen, die eben dieses Vertrauen untergraben.

Dazu gehören beispielsweise das Fiasko um die angeblichen irakischen Massenvernichtungswaffen oder Praktiken in den Grenzen der Europäischen Union, die von der CIA selbst als Folter bezeichnet werden (Allen & Foster 2015).

Teils infolge dieser Entwicklungen konkurrieren Whistleblower, Menschenrechtler, NGOs und Journalisten mit politischen Gremien um die Vorrangstellung als Kontrollinstanz und begegnen Big Data zunehmend mit Argwohn, wenn nicht sogar Technikfeindlichkeit. In diesem Bereich gibt es große Herausforderungen für die Forschung; noch können wir Einstellungen zum

Geheimdienstwesen in Wirtschaft, Gesellschaft und selbst in weiten Teilen der Regierungen Europas kaum quantifizieren. Mit unseren Überlegungen zum Geheimdienstwesen müssen wir sicherlich über den vertrauten Rahmen der Regierungseinrichtungen hinausgehen.

6. Ende der Geheimhaltung

Im Sommer 2013 deckte Edward Snowden frappierende Einzelheiten aus mehreren streng vertraulichen US-amerikanischen und britischen Überwachungsprogrammen auf; um sie zu veröffentlichen, kooperierte er mit Washington Post und Guardian, womit er für internationales Aufsehen sorgte. Snowden erntete gleichermaßen Beifall und Schmähung. Für London und Washington sind diese jüngsten Enthüllungen die schwersten Verstöße gegen Sicherheits- und Geheimhaltungsvorschriften seit Jahrzehnten. Die Medien haben diese Vorgänge vor allem auf die Themen Überwachung und Freiheitsrechte bezogen und „das Ende der Privatsphäre“ in den Mittelpunkt gerückt. Dies hat natürlich zu einer gewissen moralischen Panik geführt, gerichtet gegen Regierungen, die angeblich in der Lage sind, jeden Aspekt unseres digitalen Lebens zu überwachen. Die unsere Privatsphäre betreffenden Veränderungen sind aber nur ein Teil des Bildes, denn die beschriebenen Entwicklungen bestehen auch in einer „Krise der Geheimhaltung“ für den Staat. Am meisten beunruhigt viele Amtsträger in London aber nicht, dass die Regierung uns im Blick hat – sondern dass wir die Regierung im Blick haben.

Snowden ist symptomatisch für etwas viel Umfassenderes. Alle Regierungen sind zunehmend besorgt über die unbefugte und umfangreiche Veröffentlichung vertraulicher Dokumente durch unzufriedene Mitarbeiter, oft als „Whistleblower“ bezeichnet. Die Apparate investieren beträchtliche Summen in den Schutz von Geheimsachen; in den USA belaufen sich die jährlichen Kosten dafür auf schätzungsweise 11 Milliarden Dollar (Shane 2011). Das ist eine undurchsichtige Welt; zwar wird ein beträchtlicher technologischer Aufwand getrieben, um geheime Informanten und die mit ihnen kooperierenden Journalisten aufzuspüren, doch ist bislang nur relativ wenig über Verfahrensgeheimnisse und ihre Gegner bekannt. Es handelt sich um einen technischen Krieg, der lange vor Snowden begann und seit dem 11. September mit zunehmender Härte geführt wird.

Im Zentrum stehen neue Technologien. In den letzten zehn Jahren sind zehn Whistleblower bekannt geworden, als erste Katherine Gun 2003, eine Mitarbeiterin des GCHQ (Government Communications Headquarter). Allerdings verwenden in jüngerer Zeit Websites wie WikiLeaks bestimmte Anonymisierungssoftwares, um Beamten oder Mitarbeitern zu ermöglichen, in Kooperation mit etablierten Zeitungen große Konvolute zu veröffentlichen. Im November 2010 stellte WikiLeaks 250.000 Seiten aus US-amerikanischer Depeschen ins Netz, wodurch freimütige Äußerungen von Amtsträgern zu einem breiten Spektrum aktueller internationaler Angelegenheiten öffentlich wurden. „Es kommt“, wie Heather Brooke, die Journalistin, die den Spesenskandal britischer Abgeordneter ans Licht brachte, im Gefolge dieser Ereignisse feststellte, „ die Datenflut“ (Brooke 2010).

Die Folgen sind umwälzend. Regierungen sehen sich nun mit einem Paradigmenwechsel im Zusammenhang mit neuen Formen von Kontrolle und Berichtspflicht konfrontiert. Internetaktivisten und digitale Whistleblower behaupten, sie strebten eine neue Form horizontaler Regulierung an, die durch informatorische Demokratisierung gesichert würde. Im

„Twitter-Zeitalter“ können Journalisten durch Blogs und soziale Netzwerke umfangreiche Recherchen in Gang setzen, die mit der Arbeit von Untersuchungsausschüssen, eingesetzt von gewählten Organen, konkurrieren. Die Führung bei eingehenden Untersuchungen der Aktivitäten von Sicherheitsbehörden könnte von den formal eingesetzten Gremien und Ausschüssen übergehen auf die globale Zivilgesellschaft mit NGOs, Bürgerrechtsanwälten, Journalisten und regionalen Organen wie dem Europarat.

Das ist nicht unbedingt neu. Harry Howe Ransom beschrieb Journalisten als die „shock troops of accountability“ (Stoßtruppen der Rechenschaftspflicht) und drückte damit aus, wie Presserecherchen zur CIA Anfang der 1970er Jahre einem wahren Untersuchungsmarathon den Weg zum Capitol Hill ebneten (Johnson 1986). Aber zweierlei hat sich seitdem wohl verändert. In den 1970er Jahren brauchte Daniel Ellsberg einen vierundzwanzigstündigen Zugang zu Fotokopierern, um die Pentagon-Papiere ans Licht der Öffentlichkeit zu bringen – heute können verdrossene Amtsträger und Mitarbeiter ganze Archive von Geheimmaterial auf einem USB-Stick fortschaffen. Der direkte Zugang zu umfangreichen streng vertraulichen Daten ermöglicht geheimen Informanten, Whistleblowern und Journalisten, formale Kontrollorgane zu übertrumpfen. Wer liest noch die redigierten und zensierten Berichte des britischen Geheimdienstausschusses, wenn er Luke Hardings Analyse im *Guardian* mit Links zu den originalen Powerpointpräsentation des GCHQ lesen kann?

Für Parlamente und Volksvertretungen sind die regulatorischen Fragen um Whistleblowing und Geheimhaltung in vielerlei Hinsicht genauso wichtig wie die Regulierung und Kontrolle der Nachrichten- und Sicherheitsdienste – und beides ist auf das Engste miteinander verknüpft. In den Vereinigten Staaten und der Europäischen Union wird über den Schutz von Whistleblowern neu nachgedacht; damit verbunden sind bedeutende normative Fragen, etwa wo man die Grenze ziehen soll zwischen dem Recht der Öffentlichkeit auf Information und dem Recht von Staatsbediensteten, ihren Ministern vertrauliche Hinweise zu geben. Snowden hat Whitehall und Washington überrascht, und nun sind neue Regelungen für das zu treffen, was von der Geheimhaltung übrig bleibt.

Seit mehr als zehn Jahren führen Amerika und Europa Gespräche zu diesen Angelegenheiten. Auslöser waren die Sonderüberstellungen und die Geheimgefängnisse in Europa. Im November 2005 enthüllten aufsehenerregende Berichte von Dana Priest in der *Washington Post* die Existenz von CIA-„Geheimgefängnissen“ in „mehreren demokratischen Staaten Osteuropas“, in denen wichtige Häftlinge einsaßen. Die verstörende Vorstellung von Geheimgefängnissen auf europäischem Gebiet war der Ausgangspunkt, doch interessierten sich EU-Einrichtungen bald für weitere Fragen wie die „Geisterflüge“ durch europäischen Luftraum, die Häftlinge zu entlegenen Zielen brachten. Sie prüften ferner die Möglichkeit von Sonderüberstellungen aus europäischen Länder wie Schweden, Deutschland und Italien in Länder mit bedenklichen Menschenrechtsbilanzen außerhalb der EU (Priest 2005).

Der Ausschuss für Recht und Menschenrechte des Europarates der Parlamentarischen Versammlung übernahm die Federführung. Der Berichterstatter, der Schweizer Politiker Dick Marty, verfügte für seine Untersuchung nur über begrenzte Mittel. Unterstützt wurde er jedoch vom Generalsekretär des Europarates, der seine Befugnis nach Artikel 52 der Europäischen Menschenrechtskonvention nutzte, um die Mitgliedstaaten um Angaben darüber zu ersuchen, wie ihre Gesetze gegen geheime Inhaftierung schützen (auch durch andere Staaten), und bat um genaue Einzelheiten zu aktuellen Fällen. Im März 2006 kam die Venedig-Kommission in ihrem

Rechtsgutachten zu dem Schluss, dass geheime Inhaftierungen nicht mit der Europäischen Menschenrechtskonvention vereinbar sind. Bemerkenswerterweise machte die Venedig-Kommission geltend, dass die Unterzeichnerstaaten nicht nur selbst derartige Praktiken zu unterlassen haben, sondern auch verpflichtet sind, solche Aktivitäten von Partner-Nachrichtendiensten in den Grenzen Europas zu kontrollieren, eine Forderung von großer Tragweite. Das Europäische Parlament führte eigene Untersuchungen der Überstellungen durch und berichtete darüber im November 2006; die Europäische Kommission untersuchte daraufhin selbst den Sachverhalt und legte im November 2007 ihren Bericht vor (Hakimi 2007).

Diese Untersuchungen waren in dreierlei Hinsicht von Bedeutung. Erstens betonen sie, dass zahlreiche angesehene Anwälte heute der Auffassung sind, dass *nationale* Kontrollmechanismen nicht ausreichen, um zunehmend multinational angelegte Geheimdienstoperationen zu untersuchen. Zweitens wird das Ausmaß deutlich, in dem verdeckte Operationen dennoch Untersuchungen zugänglich werden, bedingt durch eine Vielfalt offener Quellen wie den Aufzeichnungen von Plane-Spotters (Flugzeugbeobachtern). Nach diesen Ereignissen stellte ein CIA-Mitarbeiter fest: „Es gibt keine Geheimhaltung mehr, nur noch verzögerte Aufdeckung“ (CI). Am wichtigsten ist drittens: Eine Reihe von Regierungsvertretern und Behörden in Europa fühlten sich veranlasst, bei den Amerikanern darauf zu drängen, in Sachen Geheimhaltung und insbesondere Journalisten restriktiver vorzugehen. Die Antwort der Amerikaner: Die Verfassung verbietet Regelungen wie den britischen *Official Secrets Act* (zum Schutz von Staatsgeheimnissen und amtlichen Informationen). Allerdings verstärkten sie den Druck auf Journalisten durchaus, indem sie gegen ihre Informanten ermitteln uns sie mit Nachdruck strafrechtlich verfolgen. Dieses geheime Abkommen wurde 2006 und 2007 im Rahmen der transatlantischen Neuverhandlung der Strategie des Westens zur Terrorismusbekämpfung geschlossen (CI).

Die Obama-Administration setzt mehr als alle anderen Vorgängerregierungen zusammen auf die strafrechtliche Verfolgung geheimer Informanten. Dabei ist Obama sogar noch konsequenter als George W. Bush – er will die Gerichte nutzen, um Whistleblower im Regierungsapparat zu bestrafen und die mit ihnen kooperierenden Journalisten unter Druck zu setzen. Einer der wichtigsten Aspekte von Obamas nationaler Sicherheitsstrategie ist die feste Entschlossenheit, Geheimprogramme noch geheimer zu machen und weitere undichte Stellen zu vermeiden. Dies zeigen die fünfunddreißigjährige Haftstrafe für Chelsea Manning, der Quelle der Wikileaks zugespielten Depeschen des Außenministeriums, und die Entscheidung, Snowden wegen Spionage anzuklagen (Harris 2012).

Zum Teil ist das „Ende der Geheimhaltung“ durch die Regierung beschleunigt worden. Die Nachrichtendienste und sogar die Sicherheitsbehörden allgemein haben eine wichtige Grundlage der Geheimhaltung ausgehöhlt. Die Anschläge vom 11. September führten bei den westlichen Nachrichtendiensten zu einem Paradigmenwechsel, den das GCHQ so beschrieb: „vom Informationsbedarf zum Austauschbedarf“. Der weltweite Terrorismus und die globale organisierte Kriminalität nisteten sich in den nationalen Zuständigkeiten ein und erforderten somit eine stärkere überstaatliche Vernetzung – das Motto lautete „gut miteinander auskommen“. Nach Auffassung mancher gingen dieser Austausch und die Geheimdienstkooperationen zu weit, was dazu führte, dass mit Sicherheitsüberprüfungen zu sorglos umgegangen wurde. Sowohl Manning, ein einfacher Gefreiter und gerade Anfang Zwanzig, als auch Snowden, ein vertraglich befristeter Mitarbeiter und ebenfalls in den Zwanzigern, hatten Zugang zu Hunderttausenden von Dokumenten auf geheimen Servern. Wir

erleben, wie die inneren Grenzen im Regierungsapparat ebenso wie die Grenzen zwischen den Sicherheitsbehörden und dem wachsenden Heer vertraglich befristeter Logistiker und Techniker aus der Wirtschaft gewollt durchlässiger gemacht werden (Priest und Arkin 2012).

Die Nachrichtendienste wehren sich. Sie fahren nun eher eine Vorwärtsstrategie der Informationskontrolle, um ihren Ruf zu schützen (Aldrich 2009). Aus der Öffentlichkeitsarbeit hören wir von „Nation-Branding". Ist es da zu verwegen, künftig von „Intelligence-Branding" zu sprechen? Bereits 1996 forderte eine Reihe von Experten und Anwälten eine neue Informationsmanagement-Strategie, die Informationskontrolle als größere Offenheit darstellt und schädliche undichte Stellen durch verstärkte Anstrengungen in der PR-Arbeit ausgleicht (Gill 1996, Moran 2013). Für manche wird diese Strategie veranschaulicht durch die aktuellen autorisierten Darstellungen der Geschichte des britischen Security Service und des Secret Intelligence Service sowie die filmische Verarbeitung von CIA-Aktionen in *Zero Dark Thirty* (Andrew 2009, Jeffery 2011). Im April 2014 kündigte die britische Regierung an, Robert Hannigan zum neuen Direktor des GCHQ zu bestellen; Hannigan hat Erfahrungen in der Öffentlichkeitsarbeit. All dies gehört zur neuen Infosphäre der „wissensintensiven Sicherheit"; wir werden neue Konzepte für eine entsprechende Regierungsarbeit für den Umgang mit den Erwartungen der Öffentlichkeit an Freigaben und Offenheit erarbeiten müssen.

7. Arbeit (Leistung, Abläufe) der britischen Nachrichtendienste

7.1 Allgemeine Entwicklung

Wie erfüllen die britischen Nachrichtendienste und Sicherheitsbehörden ihre Aufgaben? Wie erzielen sie Effizienz und Effektivität? Wie haben sie sich vor dem Hintergrund der Angriffe auf Amerika und Europa von 2001 bis 2005 verändert? Dieser Abschnitt befasst sich mit Entwicklungen im britischen Sicherheitsapparat; er untersucht die Nachrichtendienste und Sicherheitsbehörden zusammen mit dem Whitehall-Apparat, der diese Behörden mit der Kernexekutive verbindet.

Ferner widmet er sich den damit zusammenhängenden Aspekten des *High Policing* (der nachrichtendienstlichen Polizeiarbeit). Er will die wichtigsten Entwicklungen seit Ende des Kalten Krieges vor dem Hintergrund der Europäisierung, der Globalisierung und des so genannten „globalen Krieges gegen den Terror" untersuchen. Dabei geht er auf einige bedeutendere Gesetzesänderungen ein, die Kontrollmechanismen und bemerkenswerte neue Regulierungskriterien nach sich zogen. Allgemein aber ist es wichtig zu betonen, dass der britische Sicherheitsapparat sich in den beiden letzten Jahrzehnten in dreierlei Hinsicht stärker verändert hat:

a.) Bislang geheime Bereiche des Staates sind in beispiellosem Maße exponiert. In den 1980er Jahren wurde die bloße Existenz von Einrichtungen wie Secret Intelligence Service (MI6) häufig noch von einer durch obsessive Geheimhaltung charakterisierte Regierung geleugnet. Die stärkste Triebkraft der Veränderung war hier Europa. Vor dem Europäischen Gerichtshof

angestrengte Prozesse brachten viele Länder, auch Großbritannien, dazu, sich zu ihren Behörden zu bekennen, sie auf feste rechtliche Grundlagen zu stellen und Kontrollmechanismen einzuführen. Whitehall hatte dann 1994 begonnen, aus der Not eine Tugend zu machen: Man sprach von Open Government und richtete Internetseiten zur Personalbeschaffung für das GCHQ ein. Die Wende hin zu größerer Transparenz verstärkte sich mit der Diskussion um die Nachrichtendienste vor dem Irak-Krieg. Untersuchungen zu Geheimdiensten und Massenvernichtungswaffen hatten 2005 das bis dahin noch sanfte Rampenlicht in grelles Scheinwerferlicht verwandelt. Als John Scarlett seinen Posten als neuer Leiter des MI6 in Vauxhall Cross antrat, war sein Gesicht bereits bekannt, über seine beruflichen Erfolge wurde in der Tagespresse ausführlich berichtet.

b.) Die britischen Nachrichten- und Sicherheitsdienste sind längst keine passiven Beobachter mehr – heute sind sie Problemlöser, Durchsetzungsinstanz und Gestalter von Ereignissen. Ursächlich wirkt hier die Globalisierung. Der Kalte Krieg verlangte von den Geheimdiensten vor allem, sich auf die passive Beobachtung eines relativ statischen Feindes zu konzentrieren (mit Ausnahme von Nordirland). Mitte der 1990er Jahre hatte die Liberalisierung der Volkswirtschaften in Verbindung mit der bevorstehenden EU-Erweiterung zu größerer Besorgnis über die internationale Kriminalität geführt. Statistisch war die organisierte Kriminalität lebensbedrohlicher als Krieg und Terrorismus und wurde als eigenständiges Sicherheitsproblem zunehmend anerkannt. Dies führte im April 2006 zur Schaffung einer neuen Behörde, des National Criminal Intelligence Service (später Serious Organised Crime Agency). Es war ferner Grund für eine Wende hin zur nachrichtendienstlichen Polizeiarbeit und bewirkte, dass Sicherheitsbehörden nicht mehr nur beobachteten, sondern auch aktiv gegen schädliche Aktivitäten vorgingen. Diese Entwicklung setzte bereits 1999 ein, doch vollendete der plötzliche Anstieg terroristischer Aktivitäten die Transformation der Sicherheitsbehörden. Der MI6 rühmt sich zunehmend seiner verdeckten „weichen“ Operationen, die er als „Event-Shaping“ (Gestaltung von Ereignissen) bezeichnet.

c.) Staatliche Nachrichtendienste werden erweitert, ihre Größe kann heute nicht sicher angegeben werden. So hat sich die Mitarbeiterzahl des britischen Inlandsgeheimdienstes (MI5) 2008 ungefähr auf 4000 verdoppelt. Der frühere Special Branch wurde weitgehend durch Anti-Terror-Einheiten und Spezialeinsatzkräfte ersetzt, die in regionalen Zentren mit ebenfalls nachrichtendienstlicher/militärischer Präsenz stationiert sind. Auch MI6 und GCHQ wachsen – die letztere Behörde ist inzwischen schon zu groß für das neue Gebäude. Viele Ministerien wie auch Kommunen beteiligen sich an Maßnahmen gegen Radikalisierungstendenzen und sammeln nachrichtendienstliche Informationen über möglichen Extremismus. Ferner gibt es bedeutende Public-Private-Partnerships mit dem GCHQ; der MI6 lagert Teile seiner Tätigkeiten an zuverlässige Unternehmen aus, die häufig von früheren Regierungsmitarbeitern geleitet werden. Zudem sind heute alle staatlichen Einrichtungen befugt, „verdeckte Operationen“ durchzuführen.

Zunehmende Größe wirkt sich auf Aussehen und Charakter aus. Als eine der historischen Vorzüge des britischen Sicherheitsapparates werden häufig die geringe Größe und echte Gemeinschaft genannt. Die leitenden Kräfte sind in der Regel erfahrene Fachleute, weniger von

der Politik ernannte Personen (anders als in den Vereinigten Staaten); man kennt sich untereinander. Jedoch: Der inzwischen erweiterte britische Sicherheitsapparat birgt neue Herausforderungen, was Koordinierung und Management angeht. Dem versucht man durch eine wachsende Zahl behördenübergreifender Arbeitsgruppen und Teams beizukommen, auch mit themenbezogenen Untersuchungsgremien, die sich mit Fragen wie Terrorismus und Bedrohungen der Computer- und Netzsicherheit befassen.

7.2 Der Kalte Krieg

Der britische Sicherheitsapparat blickt auf eine lange Geschichte zurück. Der ehrwürdigste Teil ist der polizeiliche *Counter-Terrorist Branch* (SO16), dessen Ursprünge auf die 1880er Jahre zurückgehen. Die führende Sicherheitsbehörde ist der britische Inlandsgeheimdienst (MI5); er wurde 1909 als Antwort auf weitgehend fiktive Ängste vor deutscher Spionage geschaffen. Die Hauptgegner zur Zeit des Kalten Krieges waren die Spitzeldienste des Ostblocks, deren Agenten bei der Beschaffung nachrichtendienstlicher Informationen beachtliche Erfolge erzielten, wenngleich ihre Leitungen sie nicht wirksam zu nutzen vermochten (Andrew & Mitrokhin 1999). Der Kalte Krieg und die aufkommenden ideologischen Auseinandersetzungen weckten Ängste vor „Subversion“, was wiederum zur Ausweitung politischer Polizeiarbeit führte.

Zu den MI5-Aktivitäten gehörten auch Hintergrundermittlungen zu britischen Bürgern, die in sicherheitsrelevanten Regierungsbereichen arbeiteten, „Zuverlässigkeitsüberprüfung“ genannt. Die Anzahl der so überprüften Personen war hoch; dazu gehörten Politiker in Whitehall ebenso wie Wissenschaftler in Aldermaston und sogar Angestellte in der Rüstungsindustrie. Zuverlässigkeitsüberprüfungen wurden unter großem Druck der Amerikaner nach der Enttarnung sowjetischer Maulwürfe eingeführt, unter ihnen der Atomspion Klaus Fuchs. Dies war eine der letzten Initiativen der Regierung Attlee. In den 1960er und 1970er Jahren war die Furcht vor sowjetischer Infiltration in Washington wie in Whitehall groß und führte zum „Verwanzen“ von Downing Street. Zu den Sicherheitsmaßnahmen gehörten Zuverlässigkeitsüberprüfungen von BBC-Mitarbeitern; es kam vor, dass sie wegen ihrer Aktivitäten an den politischen Rändern nicht befördert wurden. Strittig ist, ob auch potenzielle Minister auf die schwarze Liste gesetzt wurden. Es gab im MI5 jedenfalls eine Akte über Jack Straw, dem wohl erfahrendsten Kabinettsmitglied des letzten Jahrzehnts, und auch über Peter Mandelson wegen politischer Aktivitäten in seiner Jugend (Sunday Times 1996; Barnett 2002, 376-7).

Das Ende des Kalten Krieges kam für die britischen Sicherheitsbehörden überraschend. Es war weder von der wichtigsten britischen Einrichtung für nachrichtendienstliche Informationsauswertung, dem Joint Intelligence Committee (JIC), noch von den Nachrichtendiensten der Verbündeten vorhergesagt worden. Dies führte für die britischen Sicherheitsbehörden zwar zu Etatkürzungen von rund 25 Prozent, doch hatte es nicht solche psychischen Krisen zur Folge, in die es ihre amerikanischen Kollegen stürzte. Nach 1989 war die IRA immer noch aktiv, und so wurden knappe Mittel nach Nordirland umgeleitet. Der MI5 erhielt 1992 die Zuständigkeit für nachrichtendienstliche Informationen über die IRA weltweit. Außerdem war es nach wie vor erforderlich, einige extremistische Gruppen zu überwachen und Datenbanken zu pflegen, um Zuverlässigkeitsüberprüfungen zu unterstützen. In den 1990er Jahren verlagerte sich der Schwerpunkt auf themenbezogene Gruppen und militante Islamisten

(Lustgarten und Leigh 1991, 613-642).

7.3 Nordirland

Der britische Sicherheitsapparat genießt Ansehen für seine Vernetzung und seine Einbeziehung in die Kernexekutive. Dies gilt jedoch nicht für Nordirland, wo in den ersten zehn Jahren der Problemphase sechs verschiedene Nachrichtendienste und Sicherheitsbehörden sich auf den Füßen standen.

Denn in den 1970er gab es fast jedes Jahr 250 Tote, erst in den 1980er Jahren ging die Zahl deutlich zurück. Durch schrittweise Infiltration der paramilitärischen Einheiten in Verbindung mit dem Einsatz eines breiten Spektrums von Überwachungstechnologie konnte ein wachsender Anteil geplanter Anschläge vereitelt werden. Teils erforderte dies den Aufbau großer Geheimdienstkorps, die fähig waren, verdeckte Operationen durchzuführen, ein Prozess, der normalerweise zehn Jahre braucht (Gearty, 1991, 123). Eine ordentliche Nachrichtendienststruktur gab es in der Provinz erst Mitte der 1980er Jahre mit der Schaffung sechs regionaler *Tasking and Co-ordinating Groups* (TCG), die uneingeschränkte Kontrolle über sämtliche verdeckten Operationen in einem bestimmten Gebiet hatten. Das aktuelle nachrichtendienstliche Informationsmodell (National Intelligence Model) der britischen Polizei nutzt die TCG und andere Erfahrungen aus dem Irland-Konflikt, und man könnte denken, dass sich dieses Konzept bei den heutigen regionalen Antiterror-Einheiten wiederfindet.

Anders als Margaret Thatchers Versicherung „keine Gespräche mit Terroristen“ war Großbritannien durch MI6-Agenten in Dublin ständig in Kontakt mit der IRA. Letzthin hat dies in den 1990er Jahren den Weg zu einer politischen Lösung in Nordirland geebnet. Die abnehmenden IRA-Aktivitäten waren für MI5 am deutlichsten spürbar. Nach dem Ende des Kalten Krieges noch im Kampf gegen den irischen Terrorismus führend, verlor der Dienst nun einen weiteren zentralen Operationsbereich. Um ihn am Leben zu halten, tat die Regierung – nach einer minimalen öffentlichen Anhörung – den ungewöhnlichen Schritt, ihm die Zuständigkeit für die nachrichtendienstliche Unterstützung im Kampf gegen organisierte Kriminalität zu übertragen.

Viele heutige Sicherheitsfragen stellten sich in den 1990er Jahren ähnlich. Nach den IRA-Anschlägen in der Londoner City 1993 und auf Canary Wharf 1996 kamen neue Besorgnisse über strategischen Terrorismus auf, der die nationalen Infrastrukturen und das wirtschaftliche Wohl gefährdete und beunruhigende Fragen zur Belastbarkeit aufwarf. Die Antwort wies auch den Weg zu Public-private-Partnerships in Sicherheitsbelangen. Um die Londoner City wurde ein *Ring of Steel* gezogen, Ausdruck eines Geflechts von Vereinbarungen zwischen Behörden, privaten Sicherheitsfirmen und den Finanzinstitutionen. Die Operation „Griffin“ (Greif) unterstützt nicht nur die Ausbildung der von den Banken angestellten privaten Sicherheitskräfte, sondern ermöglicht auch den Austausch von Informationen zwischen den Partnern des öffentlichen und privaten Sektors. Ein Teil der Kommunikationsinfrastruktur für Griffin wird von den Banken, weniger durch Regierungsnetze bereitgestellt. Dieser Prozess der „Griffinisierung“ – des Aufbaus öffentlich-privater Sicherheitspartnerschaften – hat sich beschleunigt (London Assembly 2005).

Landläufig geht man davon aus, dass Nordirland für die Behörden kein Sicherheitsproblem mehr darstellt. Tatsächlich aber gibt es dort immer noch eine beträchtliche terroristische Bedrohung durch Abspaltungen von den Paramilitärs, und 2010 waren deutliche Spitzen der terroristischen Aktivitäten zu verzeichnen. Nordirland hat den Operationen der beiden Sicherheitsbehörden wie denen der Armee seinen Stempel aufgedrückt. Seit 2001 jedoch halten sich die Minister im Londoner Kabinett mit Genehmigungen für langfristig angelegte Infiltrationen zurück, wie sie noch für die 1990er Jahre typisch waren. Die Gefahr von Terroranschlägen mit hohen Opferzahlen hat zu einem risikoscheuen Ansatz und der Neigung geführt, eher „hinzusehen und zuzuschlagen“ als „zu beobachten und abzuwarten“.

7.4 Globalisierung

Allgemein herrscht der Eindruck vor, die derzeitigen Aktivitäten und Operationen der britischen Nachrichten- und Sicherheitsdienste seien durch die Terrorismusbekämpfung geprägt. Tatsächlich aber bringen die wichtigsten Veränderungen seit dem Ende des Kalten Krieges allgemeinere globalisierungsbedingte Entwicklungen des internationalen Systems zum Ausdruck. Globalisierung wird meist mit Deterritorialisierung und einem angeblichen Schwinden des souveränen Staates verbunden, wobei auch Aspekten der Kommunikationsrevolution als beschleunigenden Faktoren eine Bedeutung beigemessen wird. In Großbritannien zeitigt die Globalisierung die deutlichsten Folgen wohl für die Wirtschaft. Hier wurde rascher als in anderen europäischen Ländern dereguliert, auch hat Großbritannien erkennbar von der Ausdehnung des Welthandels und des Finanzsektors profitiert. Das Wachstum Londons als bedeutendem Finanzzentrum und die neue Stellung seines Flughafens als weltgrößter Drehscheibe ist ein Sinnbild dafür. Anfang der 1990er Jahr haben wohl alle in der Regierung die Globalisierung als uneingeschränkt gut betrachtet.

Mit der Globalisierung gedieh auch Al-Qaida – just zu einer Zeit, da die Ressourcen der Nachrichtendienste nach dem Ende des Kalten Krieges drastisch gekürzt wurden. Zudem entwickelten sich in den 1990er Jahren zwar gesonderte, aber miteinander verbundene Herausforderungen, deren viele sich als komplexe illegale Netzwerke beschreiben lassen. Dazu gehörten Rauschgifthandel, Geldwäsche, Menschenhandel, Verbreitung von Kernwaffen und illegaler Kleinwaffenhandel. Diese Probleme wurden durch die Globalisierung verschärft und überschnitten sich mit „neuen Kriegen“, wofür das frühere Jugoslawien das bekannteste Beispiel ist. In Russland, auf dem Balkan und in Zentralasien spielte eine Reihe von undurchsichtigen Figuren aus den Sicherheitsbehörden auch im kriminellen Milieu eine wichtige Rolle. Infolge dessen war MI6 nicht mehr auf festen Basen in den jeweiligen Ländern stationiert, sondern operierte zunehmend mit mobilen Kommandos in kurzfristig angelegten Einsätzen (Kaldor 2013).

Was diesen neuen Bedrohungen gemeinsam war, waren die zumeist verdeckten Operationen. Ende der 1990er Jahre revidierte die britische Regierung ihre Etatkürzungen bei den Sicherheitsbehörden (Rice und Thomas 1997, 14-15). Diese Wende wurde Ende 1999 bei einem Gipfel in Downing Street 10 mit MI5, MI6 und GCHQ bestätigt, auf dem eine beträchtliche Umverteilung der Mittel zur Bekämpfung der organisierten Kriminalität beschlossen wurde. Im Juni 2000 machte die schockierende Entdeckung von 85 illegal eingeschleusten Chinesen, die in einem Container in Dover zugrunde gegangen waren, den Ernst dieser Entwicklung deutlich.

Kriminalität wurde zunehmend neu interpretiert als Sicherheitsproblem, mit dem sich die Nachrichtendienste befassen mussten. Teils spiegelte dies die geplante Erweiterung der NATO und der Europäischen Union wider, wodurch Großbritannien eine offene Grenze bekam, die bis zum Ural reichte (National Criminal Intelligence Service 2000; Barnett 2002, 366-7).

Globalisierung ist eng mit dem Rückzug des Staates verbunden. In Großbritannien manifestiert sich dies in Deregulierung und Privatisierung. Dass das Land zunehmend vom Finanz- und Dienstleistungssektor abhängig wurde, erforderte ebenfalls, die gemeinsame Aufmerksamkeit auf wichtige nationale Infrastrukturen zu richten. In den 1990er Jahren bestand die neue Priorität darin, die Sicherheit des E-Commerce zu gewährleisten. Das bedeutete für den britischen Sicherheitsapparat einen Paradigmenwechsel. Bislang ging es bei der Sicherheit der Kommunikationsinfrastruktur weitgehend um die Regierungsbehörden. Für die Sicherung der elektronischen Kommunikation und Computersysteme in der täglichen Regierungsarbeit sorgte die Communications Electronic Security Group (CESG), eine Unterorganisation des GCHQ in Cheltenham. Ende der 1990er Jahre wurde man sich jedoch mehr und mehr bewusst, dass die Regierung für Banken und Wirtschaft, die sich zunehmend auf das Internet stützten, dasselbe Schutzniveau installieren musste. Zudem waren viele zuvor öffentliche Versorgungseinrichtungen, auch die britische Telekommunikationsinfrastruktur, privatisiert worden. So wandelte sich die CESG 1997 von einer im Verborgenen operierenden Abteilung in einen öffentlich wahrnehmbaren technischen Beratungsdienst, der Standards für die Informationssicherheit setzte und Support für Unternehmen auf Kostendeckungsbasis bot.

Ihre Aktivitäten bleiben jedoch umstritten, weil viele ihr Interesse an einer Förderung wirklich sicherer Systeme in Zweifel ziehen. Sowohl innerhalb der NSA als auch im GCHQ gibt es seit Langem Spannungen zwischen den Befürwortern eines defensiven Sicherheitskonzepts und jenen, die eine Schwächung der Systeme anstreben, um offensive Infiltrierungen zu erleichtern. Diese Debatte ist inzwischen schärfer geworfen, unter anderem weil die britische Verkehrs- und Energie-Infrastruktur immer mehr vom Internet abhängt und die Gefahr von Cyberkriegen größer wird. Vielen Verantwortlichen im GCHQ bereitet auch der Eindruck Unbehagen, dass die Amerikaner als fünfte Dimension der Kriegführung die Militarisierung des Cyberspace herausstellen. Aufgeregte Debatten werden nun um die Verwundbarkeit der britischen nationalen Infrastruktur geführt, und die Einschätzung des Schutzbedarfs ist wohl eine neue nachrichtendienstliche Disziplin (CI).

Im GCHQ werden MI5 und MI6 zuweilen als „Knirpse“ oder „kleine Fische“ bezeichnet. Das GCHQ ist als größter und teuerster Teil des britischen Sicherheitsapparates immer der Geheimdienstriese gewesen. Größe und Ausdehnung sind schwer zu quantifizieren, den Etat einzuschätzen ist besonders schwierig. In der Regel nutzt das GCHQ in großem Umfang Teile der britischen Verteidigungsinfrastruktur, Satelliten und Unterseeboote eingeschlossen. Sollen diese Kosten eingerechnet werden? Dann belaufen sich die realen Kosten für das GCHQ mit Stand von 2015 vielleicht auf rund 3 Milliarden Pfund jährlich. Vermehrt ist festzustellen, dass der Staat versucht, die Kosten durch gesetzliche Bestimmungen „wegzurechnen“, indem er den Internetanbietern und Telekommunikationsunternehmen bei Speichern und Zugängen bestimmte Lasten aufbürdet.

Für das GCHQ gab es die größte Krise Mitte der 1990er Jahre. Das exponentielle Wachstum des globalen Telekommunikationsaufkommens in Verbindung mit neuen Kommunikationsmöglichkeiten schuf ernste Probleme. Zwischenzeitlich war der Etat nach einer

von Roger Hurn 1995 im Auftrag des Finanzministeriums durchgeführten Überprüfung um 25 Prozent gekürzt worden, als „Dividende“ der veränderten Situation nach dem Kalten Krieg. Im Jahr darauf wurde unter der Leitung von David Omand die alte fordistische Organisationsstruktur größtenteils abgeschafft. Nach dem Vorbild führender Unternehmen wurde eine Management-Revolution in Gang gesetzt, die zu flacheren Hierarchien, flexiblen Teams und intensiverem Informationsaustausch führte. Die Ingenieursabteilung wurde vollständig privatisiert. Anschließend wurde entschieden, im Rahmen eines neuen Programms („Signals Intelligence New Systems“, SINEWS) in modernste Signalaufklärungstechnologien zu investieren. Symbolisch für diesen Wandel war der Umzug in das riesige neue GCHQ-Hauptquartier, auf Privatkapitalbasis finanziert und 2003 fertiggestellt. Damals war das GCHW davon ausgegangen, nur zwei Drittel des Gebäudes zu belegen und den Rest zu verpachten – heute ist es für den GCHQ-Betrieb zu klein. Nach dem 11. September wurde ein Großteil der für die Terrorismusbekämpfung verfügbaren neuen Mittel in die Internetsicherheit investiert.

7.5 Der „neue Terrorismus“ und der 11. September

Ende der 1990er Jahre richtete sich die Aufmerksamkeit des britischen Sicherheitsapparates mehr und mehr auf eine Entwicklung, die von manchen der „neue Terrorismus“ genannt wird. Er ist charakterisiert durch religiösen Fundamentalismus und brutale Anschläge, verbunden mit neuen Organisationsstrukturen und Operationen, die Nutzen aus der Globalisierung ziehen. Dies manifestierte sich im Exodus ausgebildeter ausländischer Kämpfer aus Afghanistan nach dem Ende des vom Westen unterstützten Kampf gegen die sowjetischen Besatzer. Zudem wuchs die Besorgnis über die Wechselwirkungen zwischen Terrorismus, Waffenverbreitung, gescheiterten Staaten und organisierter Kriminalität. Das britische Antiterrorgesetz von 2000 war eine Reaktion darauf; es enthielt eine breitere Definition von Terrorismus, die nun auch politische, religiöse und ideologische Ursachen sowie Aktivitäten außerhalb Großbritanniens berücksichtigte. Dies erweiterte die polizeiliche Gewalt um die Befugnisse Beenden, Durchsuchen und Verhaften und ermöglichte gründlichere Finanzermittlungen. Nach dem nordirischen Friedensabkommen fanden es manche Beobachter merkwürdig, dass Sonderbestimmungen eher ausgeweitet als aufgehoben wurden. Diese Veränderungen nahmen jedoch künftige Probleme vorweg (Moran 2006, 343). Nach den Anschlägen vom 11. September entschied sich die britische Regierung für eine neue Antiterrorstrategie, genannt CONTEST. CONTEST hat vier wichtige Dimensionen:

- Verhütung: Bekämpfung der Ursachen des Terrorismus im In- und Ausland, beispielsweise durch Unterstützung des gemäßigten Islam.

- Verfolgung: Effizienter Einsatz der Nachrichtendienste, um Terroristen zu stören und zu ergreifen, mit verbesserter Zusammenarbeit und internationalem Informationsaustausch, verschärfter Grenzsicherung und neuen Maßnahmen gegen Identitätsdiebstahl und Terrorfinanzierung.

- Schutz: Sicherheitsmaßnahmen zur Minderung von Risiken für Briten im In- und Ausland.

- Abwehrbereitschaft und Folgenbewältigung: Verbesserung der Kapazitäten für den

Terror-Ernstfall oder andere Katastrophen.

Man kann nun behaupten, dass noch die Dimension „Präemption“ (Präventivschläge) hinzukäme, die die Besorgnis der Regierung über groß angelegte Anschläge und den möglichen Einsatz unkonventioneller Waffen zum Ausdruck bringt. Der britische Sicherheitsapparat ist allgemein viel weniger bereit hinzunehmen, dass potenzielle Terroristen frei bleiben. Im Laufe der Jahre und als Erkenntnis aus den nordirischen Erfahrungen hatte Großbritannien eine Geheimdienststrategie gegen Terrorismus entwickelt, die man als „abwarten und beobachten“ beschreiben konnte und die Hoffnung ausdrückte, dass Terroristen in Freiheit weiterhin wertvolle Informationen liefern würden. Seit dem 11. September hat sich die britische Strategie mehr zum „hinsehen und zuschlagen“ verlagert. Dies beeinträchtigt den Nachrichtenfluss, denn sind Verdächtige erst einmal hinter Schloss und Riegel, sind die Informationen, die sie im Verhör anbieten können, rasch überholt (Omand 2005, 107-116).

Nach dem 11. September hat sich auch die britische Kernexekutive verändert. Im Juni 2002 wurde der Posten des *Intelligence Coordinator* (Geheimdienstkoordinator) im Cabinet Office zum *Second Cabinet Secretary* mit erweiterter Zuständigkeit für *Intelligence, Security and Resilience* aufgewertet. Dass *Resilience* („Katastrophenfestigkeit“) hinzukam, drückte die erweiterte Funktion Sir David Omands und seinen Wunsch aus, das vernetzte Regieren mit zahlreichen Ministerien zu fördern, die zuvor kaum über diese Aspekte nachgedacht hatten (Omand 2004, 26-33). Die herkömmliche Auffassung, Sicherheit falle in die Zuständigkeit spezialisierter Abteilungen, wurde damit aufgegeben. Dies spiegelte sich in einem neuen Mechanismus für die Verarbeitung operativer Erkenntnisse über den Terrorismus wider, dem *Joint Terrorism Analysis Centre*, das dem britischen Inlandsgeheimdienst (MI5) unterstellt und im MI5-Gebäude im Thames House angesiedelt ist; ihm werden Mitarbeiter aus allen öffentlichen Einrichtungen sekundiert, hinzu kommen externe Experten und Wissenschaftler. Diese Einbeziehung aller Beteiligten wird allseits gelobt und in ganz Europa zum Vorbild genommen. MI5 selbst hat eine erweiterte koordinierende Funktion für eine Reihe nationaler Sicherheitsaktivitäten, die weit über die traditionelle Rolle hinausgehen und auch die Infrastruktur umfasst – sogar die Lagerung von Landwirtschaftsdünger (Bamford 2004, 744-5).

Auch neue Befugnisse gab es. Am meisten umstritten war das neue *Anti-Terrorism Crime and Security Act* (Antiterror- und Sicherheitsgesetz) von 2001, das die polizeilichen Befugnisse gegen Verdächtige ausdehnte (Fenwick 2002). Die 2000 und 2001 neu übertragenen Befugnisse machten sich die Behörden prompt zunutze und inhaftierten Demonstranten, die offenkundig keine Beziehungen zum Terrorismus hatten – meist Friedensdemonstranten, die gegen eine Rüstungsmesse in London protestierten. In einem Fall führte die Polizei einen Befehl zur Durchsuchung und Beschlagnahme nach Artikel 44 des Terrorismusgesetzes gegen ein elfjähriges Mädchen aus. Ähnlich räumt das US-Justizministerium ein, dass der *Patriot Act* kaum gegen Terrorismus angewendet wird, sich aber gegen Drogenhandel und organisierte Kriminalität als nützlicher erwiesen hat. Dies drückt eine gezielte Aushöhlung der Grenze zwischen nachrichtendienstlichen und strafrechtlichen Ermittlungen aus. Das augenfälligste Beispiel dafür ist die Verwendung von Geheimdienstinformationen für Geheimprozesse, die Einwanderung, Haft oder Hausarrest betrafen. Dieses Material ist von unterschiedlicher Zuverlässigkeit, aber dennoch schwer anzufechten (Moran 2006, 342, 345; Wada 2002, 51-9).

Das Antiterror- und Sicherheitsgesetz von 2001 (Anti-Terrorism Crime and Security Act) ermöglichte, eine beträchtliche Anzahl Personen ohne Anklage auf unbestimmte Zeit festzuhalten, was gegen die Europäische Menschenrechtskonvention verstößt. Viele erinnerte dies an die fragwürdigen Internierungen in Ulster nach dem *Special Powers Act* (Gesetz über Sondervollmachten) von 1972. Bis Februar 2004 wurden vierzehn Personen nach diesen Bestimmungen im Londoner Belmarsh Prison festgehalten. Es handelte sich um Nicht-EU-Bürger, die auf der Grundlage von Geheimdossiers inhaftiert wurden – meist enthielten diese nur Listen ihrer Verbindungen und weniger ihrer Aktivitäten. Die Rückführung ins Herkunftsland war die einzige Alternative zu ihrer dauerhaften Inhaftierung. Im folgenden Dezember befand ein neunköpfiges Gremien des britischen Oberhauses dies für eine Verletzung ihrer Menschenrechte. Dieses System wurde ersetzt durch Kontaktverbote, deren Folgen ähnlich dem Hausarrest sind, und in jüngerer Zeit durch Maßnahmen nach dem *Terrorism Prevention and Investigation Measures Act* von 2011. Nach weiteren 2002 verabschiedeten Rechtsvorschriften erhielt der Innenminister die Befugnis, die Staatsbürgerschaft abzuerkennen (Bamford 2005, 748-9; Chirinos 2005, 265-76; Walker 2005, 400-1).

Es ist interessant, was die Briten annehmbar fanden bzw. ablehnten. Haft ohne ordentliches Verfahren und Notstandspläne in Verbindung mit der Untersuchungshaftdauer führten hier zu politischen Protesten. Das Thema wurde unter Gordon Brown 2010 erneut aufgegriffen; sein Versuch, die Haftdauer zu verlängern, wurde im Oberhaus vom kürzlich pensionierten MI5-Generaldirektor vereitelt, der diese Vorschläge für Unsinn erklärte. Auch Personalausweise geben immer wieder Anlass zu Diskussionen. Doch gleichermaßen wichtige Änderungen, die im Ausland eintraten und Briten betrafen, erregten kaum Aufsehen. Nach schwierigen Verhandlungen schlossen die EU und die Vereinigten Staaten ein Abkommen über den Austausch von Fluggastdaten. Ein ähnliches Abkommen ermöglicht US-amerikanischen Antiterror-Ermittlern den Zugriff auf Daten von Überweisungen in Europa, die durch das überall verbreitete Swift-System getätigt werden. Auch gab es Initiativen, europäischen Telekommunikationsanbietern vorzuschreiben, Verbindungsdaten zu speichern, um Ermittlungen zu unterstützen. Diese führten zur Einrichtung riesiger Datenspeicher mit Informationen über britische Bürger, die sich aggregieren und mit privaten Organisationen austauschen lassen, aber keiner nationalen Kontrolle unterliegen. Über all dies war in der Fachpresse zu lesen, aber weder den Bürgern noch ihren politischen Vertretern waren die Schöpfungen diese transatlantischen Sicherheitsapparates klar ersichtlich – bis zu den Snowden-„Enthüllungen“ im Juli 2013 (Mathieson 2005, 1-2; Rees 2006, 231).

7.6 Irakische Massenvernichtungswaffen, Downing Street und der Nationale Sicherheitsrat der Vereinigten Staaten

Die Nichteinhaltung der UN-Resolutionen gegen Massenvernichtungswaffen löste 2003 eine umstrittene Invasion und die Besetzung des Irak aus. Zuvor hatte die britische Regierung beschlossen, zwei Irak-Dossiers zu veröffentlichen, die sich ihr zufolge auf Geheimdienstmaterial stützten. Sie waren für die Öffentlichkeit aufbereitet, es waren keine freigegebenen Geheimdienstberichte. Kritische Journalisten konnten nicht glauben, dass das Regierungspresseamt der Versuchung widerstanden haben konnte, die Dossiers aufzubauschen.

Darauf wurden erbitterte Auseinandersetzungen unter den Augen der Öffentlichkeit geführt, die den Sicherheitsapparat mehr als je zuvor ins Rampenlicht rückten. Vor allem die Rolle des Joint Intelligence Committee (JIC), ein bis dahin kaum bekanntes Gremium für nachrichtendienstliche Informationsauswertung, wurde zum Gegenstand der nationalen Debatte. Zwar entsprachen die Dossiers einem langfristigen Trend zu mehr öffentlicher Darstellung der Nachrichtendienste, doch riskierten sie auch den Vorwurf, genutzt zu werden, um politische Unterstützung zu mobilisieren, statt politische Fragen zu klären. Die Qualitätskontrolle der Dossiers, insbesondere des zweiten, war eher rudimentär.

Nach der Invasion wurden keine Massenvernichtungswaffen gefunden. Die Kontroverse verschärfte sich, und es folgte ein beispielloser Untersuchungsmarathon in Whitehall und Washington; in Großbritannien allein waren es zwischen Juli 2003 und Juli 2004 vier Ermittlungen. Geheimdienstinformationen über irakische Massenvernichtungswaffen waren Thema der ersten Untersuchung durch das *Parliamentary Select Committee on Foreign Affairs* und der zweiten durch das *Intelligence and Security Committee* (ISC). Der dritte Ausschuss unter Vorsitz von Lord Hutton untersuchte die Umstände des Todes von Dr. David Kelly, eines Mikrobiologen, der bei der ersten Untersuchung hart ins Kreuzverhör genommen worden war. Schließlich wurde Lord Butler, ein früherer Kabinettssekretär, mit einer breiter angelegten Untersuchung der britischen Geheimdienstinformationen über Massenvernichtungswaffen beauftragt. Die Hutton-Untersuchung vor allem veranlasste Wissenschaftler und Journalisten zu einer bemerkenswert detaillierten Darstellung des britischen Sicherheitsapparates (Davies 2004, 495-520). Lord Butlers Untersuchung widersprach den Erkenntnissen des ISC zur Gesamtqualität der britischen Geheimdienstinformationen über den Irak und offenbarte den ISC – das ständige parlamentarische Kontrollgremium – als schwach.

War dies nun ein Fall von Geheimdienstversagen oder von Täuschung durch Politiker? Die Antwort muss zwangsläufig lauten: beides. Nachdem die Bestände an irakischen Massenvernichtungswaffen 1991 deutlich unterschätzt worden waren, wollten die Mitarbeiter der Nachrichtendienste nicht erneut überrascht werden und entschieden sich deshalb für eine „Worst-Case-Analyse“. Außerdem hatten die Verbündeten bei der Einschätzung der Massenvernichtungswaffen so eng kooperiert, dass sie, weit davon entfernt, die Ergebnisse der jeweils anderen in Zweifel zu ziehen, einer Art „Gruppendenken“ erlagen. Nur die Niederländer und die Kanadier äußerten starke Zweifel. Aber es gab auch Unehrlichkeit auf der Regierungsseite. Zwar gab es einige glaubhafte Geheimdienstinformationen, die vermuten ließen, die Iraker könnten Teile ihre alten Bestände von 1991 versteckt halten, ferner gab es einige Hinweise darauf, dass der Irak nach wie vor Komponenten von Massenvernichtungswaffen auf dem Weltmarkt beschaffen wollte und weitergehende Ambitionen hatte. Allerdings gab es keinen stichhaltigen Beweise für die zentrale Behauptung, der Irak betreibe eine „fortgesetzte“ Produktion von Massenvernichtungswaffen. Diese letztere Auffassung wurde vom Premier in seinem persönlichen Vorwort zum Dossier über irakische Massenvernichtungswaffen nachdrücklich vertreten (Aldrich 2005, 73-5, 81). Butler stellte fest, dass die Geheimdienstberichte dazu im Zeitraum 2002 bis 2003 keine Veränderungen auswiesen, einem Zeitraum, als Großbritannien seine Politik der Eindämmung des Irak radikal auf Konfrontation umstellte (Runciman 2004, 76-7).

Daraus sind interessante und verblüffende Lehren für eine verbesserte Berichtspflicht zu ziehen. Die vier Untersuchungen des Sicherheitsapparates verlagerten die Berichtspflicht immer weiter nach unten. Ihre Aufträge erlaubten keine Untersuchung der Beziehungen zwischen

Nachrichtendiensten und Politikgestaltung, sodass Transparenz zur Jagd auf kleine Fische wurde, während man die Großen laufen ließ. Wichtiger noch: Viele schlussfolgerten, dass es eine Gesamtleitung für den wachsenden britischen Sicherheitsapparat gab, wobei Blairs legerer Führungsstil noch hinzukam. Auf Kabinettsebene gab es vermutlich einen Ministerausschuss für die Nachrichten- und Sicherheitsdienste. Doch obwohl wiederholt angemahnt, kam dieses Gremium in der gesamten Amtszeit Blairs nicht einmal zusammen (Davies 2013, 272-91).

Brown wie Cameron kamen zu der Auffassung, dass die Kabinettsmaschinerie verbessert und gestärkt werden musste. Also entwickelten sie die *National Security Strategy* und schließlich den *National Security Council*. In diesem Rahmen trifft sich der Premierminister wöchentlich persönlich mit den Leitern aller drei Nachrichten- und Sicherheitsdienste. Die Geheimdienstchefs werden vom JIC in dieses neue Gremium entsandt. Der JIC prüft nach wie vor die Dienste, während der NSC mögliche Lösungen zur Prüfung durch das Gremium vorlegt (Davies 2013, 293-9). Der NSC gilt weithin als Erfolg, nicht zuletzt, weil er ein breites Spektrum von Whitehall-Akteuren einbezieht, auch jene, in deren Zuständigkeit die organisierte Kriminalität und die Entwicklungen im Ausland fallen. Allerdings neigte Cameron eher dazu, den NSC operativ statt strategisch zu nutzen. Dass darin die Nachrichtendienste und Sicherheitsbehörden mitwirken, fördert eher einen interventions- und maßnahmenorientierten Ansatz (CI).

7.7. Terrorismus nach 2005

Die Anschläge in Madrid 2004 und in London 2005, ebenso der geplante Anschlag auf Verkehrsflugzeuge ab Heathrow 2006 offenbarten ein massives innenpolitisches Problem. MI5 hatte sich zwar in den 1990er Jahren für radikale islamische Gruppen in Großbritannien interessiert, war über ihre Präsenz jedoch nicht sonderlich beunruhigt. Exilianten drückten ihre Opposition gegen ihre Regierungen in Saudi-Arabien, Pakistan und Algerien aus, galten aus Londoner Sicht aber als unproblematisch. Allerdings war Al-Qaida bestrebt, diese Gruppen im weltweiten Krieg gegen die Vereinigten Staaten und ihre Verbündeten zu mobilisieren (Gerges 2005; Bamford 2004, 739-40). Forciert durch die Kontroverse um den Irak-Krieg und die engeren Beziehungen zwischen Großbritannien und den Vereinigten Staaten und Israel, wurden die radikalisierten islamischen Gruppen mit einem Mal zum Problem. Die Londoner Anschläge vom 7. Juli 2005 machten zudem das Ausmaß einer neuen Bedrohung im Innern deutlich (Gregory & Wilkinson 2005). Die Politik des Westens hatte viele Menschen aufgebracht, die zehn Jahre zuvor an einen Anschlag auf britische Einrichtungen nicht einmal gedacht hätten. Infolge dessen war und ist die Anzahl Aktiver so groß, dass sie die Überwachungskapazitäten selbst eines erweiterten Sicherheitsapparates übersteigt (Herrington 2015, Pythian 2006).

Elizabeth Manningham-Buller, MI5-Generaldirektorin, stellte 2006 fest, dass es in Großbritannien 1600 auffällige Personen gab (Manningham-Buller 2007). Die Überwachung eines einzigen Verdächtigen erfordert den Einsatz von zwanzig Sicherheitskräften. Auch mit dem Ausbau von MI5, größeren spezialisierten Polizeieinheiten und der fallweisen Hinzuziehung von spezialisierten Militäreinheiten ist es nicht möglich, mehr als zweihundert Personen gleichzeitig zu beobachten. Scotland-Yard-Chef Sir Ian Blair offenbarte im Sommer 2005, dass er über den

Etat für terrorbezogene Sicherheitsmaßnahmen hinaus täglich 500.000 Pfund aufwenden musste. Die Kapazitäten des Sicherheitsapparates sind völlig ausgeschöpft, was wiederum die Kapazitäten zur Bekämpfung von organisierter Kriminalität und Spionage erschöpft (Harfield 2006, 743-61). Dies bereitete den Weg für eine intensivere technische Überwachung.

Inzwischen sorgt das harte amerikanische Vorgehen für veränderte Einstellungen in der britischen Justiz. Im Kalten Krieg wurde britischen Richtern gerne Feigheit unterstellt, wenn ihnen das Gespenst nationaler Sicherheitsstrategien begegnete (Lustgarten und Leigh 1994, 321). Nach den Enthüllungen über Guantanamo, Abu Graib und die „Sonderüberstellungen" wehte jedoch ein anderer Wind. Mit dem *Human Rights Act* 1998 fühlten sich hohe Richter ausreichend gestärkt, den Sicherheitsapparat in die Schranken zu weisen. Das augenfälligste Beispiel ist die Folter. Am 8. Dezember 2005 befand das Oberhaus, dass in Drittländern unter Folter erzwungene Aussagen vor britischen Gerichten unzulässig sind. Das Thema Folter stieß auf Resonanz, und die Richter kamen mehr und mehr zu dem Schluss, dass das britische Kontrollorgan für die Geheimdienste, der ISC, mehr Wert auf Effizienz und Effektivität als auf Ethik und Recht legte. Von mancher Seite wird behauptet, die geplanten Anschläge auf Verkehrsmaschinen in Großbritannien im August 2006 seien vereitelt worden durch Geheimdienstinformationen, die die pakistanischen Sicherheitsbehörden durch energische Verhöre von Rashid Rauf, einem britischen Staatsbürger, erlangt hatten. Aber das Ausmaß, in dem unter Folter gewonnene Erkenntnisse dazu beigetragen haben, Anschläge in Großbritannien zu vereiteln, ist und bleibt wohl auch unklar (Danchev 2006, 587-95; Campbell und Ramesh 2006).

Die Regierung sucht nach Wegen, Radikalisierung zu verhindern, verhält sich hier aber unsicher. Bemühungen des Außenministeriums, sich direkt mit Radikalen in Verbindung zu setzen, wurden von den einen als zu zaghaft, von andern als Beschwichtigungspolitik kritisiert. Auf institutioneller Ebene kam das Verlangen nach einem differenzierteren Vorgehen durch die Einrichtung eines neuen *Office on Counterterrorism and Security* im Innenministerium 2007 zum Ausdruck, geleitet von Charles Farr.[1] Gleichzeitig wurde der Posten des Geheimdienstkoordinators im *Cabinet Office* abgewertet. Zu Farrs neuer Abteilung gehört ein *Research Information and Communications Unit* unter Leitung von Jonathan Allen, ebenfalls ein Diplomat mit Erfahrung in der Öffentlichkeitsarbeit. Dies bildet einen offenen Schwenk hin zum Konzept „Überzeugen und Loyalität gewinnen" und läuft parallel zur lange praktizierten verdeckten Informationsbeschaffung. Die Schaffung dieser von Diplomaten geleiteten Abteilung signalisiert ferner Deterritorialisierung und das Ende eines Sicherheitsapparates mit überwiegend innenpolitischem Schwerpunkt.

7.8 Das Intercept Modernisation Programme

Die Identifizierung einer erheblichen Bedrohung im Innern, verbunden mit externen forcierenden Elementen, führte in Großbritannien dazu, die Einstellungen zu Überwachungspraktiken grundlegend zu überdenken. Die personellen Überwachungskräfte waren überfordert; es gab Vorschläge, die Möglichkeiten der Nachrichtendienste auszubauen, um die eigene Bevölkerung beobachten zu können, was die gewohnten Grenzen zwischen

[1] A.d.Ü.: Die offizielle Bezeichnung lautet richtig „Office for Security and Counter-Terrorism" (OSCT).

Auslands- und Inlandsaufklärung stark verwischt. Herkömmlicherweise wurden der Auslandsaufklärung relativ wenige Grenzen auferlegt. Nachrichtendienste wie das GCHQ sind befugt, die Kommunikation ausländischer Regierungen und von im Ausland lebenden Personen mehr oder weniger ungehindert zu überwachen, erleichtert durch weitgefasste Genehmigungen, die so genannten „Artikel 8(4)-Anordnungen“. Über die Überwachung im Innern lässt sich das Gegenteil feststellen. Früher war die Inlandsaufklärung durch Regelungen begrenzt, die zielgerichtete Aktivitäten förderten, um eine breitere Überwachung der Bevölkerung zu verhindern. Vor allem waren die Innenminister bei Anordnungen gegen Ziele im Innern zurückhaltender und wiesen entsprechende Anträge zurück.

Allerdings wurden durch die neuen Kommunikationstechnologien in Verbindung mit der wachsenden terroristischen Gefahr die Rufe nach einer „Modernisierung“ lauter. Besonders beunruhigend waren die mit Internet-Telefonie verbundenen Probleme, da man davon ausging, dass die meisten Gespräche in den nächsten zehn Jahren über das Internet geführt würden. Viele vertreten die Auffassung, dass ein eher technisches Konzept die Nachrichtendienste in die Lage versetzen würde, größere Anzahlen von Menschen passiv zu überwachen und die knappen personellen Überwachungsressourcen effizienter gegen die gefährlichsten Ziele einzusetzen. Schließlich wurde die Regierung infolge brutaler Terroranschläge wie jener vom 7. Juli mit ihrem Überwachungskonzept risikoscheuer.

Im letzten Jahrzehnt hat die britische Regierung eine Reihe bedeutender Vorstöße gemacht, die eine klare Wende hin zu stärkerer Überwachung der eigenen Bevölkerung zeigt. Britische Minister drängten in Europa auf Gesetze, die Telefongesellschaften und Internetanbietern vorschreiben, große Datenmengen über persönliche E-Mails, Webseitenaufrufe und Telefongespräche zehn Jahre lang zu speichern. Diese „Verbindungsdaten“ müssten Polizei und Nachrichtendiensten auf Antrag zugänglich gemacht werden. Diese Vorschläge wurden von Datenschützern als umfassendste Ausweitung staatlicher Sicherheitsüberwachung von Personen angeprangert, die je in Betracht gezogen wurde. Hauptgegner war sogar die Internetbranche selbst, die den Plänen vehement widersprach und erneut Fragen der Privatsphäre und des Geschäftsgeheimnisses in den Vordergrund rückte. Es geht hier jedoch nicht um den Inhalt von Gesprächen oder Nachrichten, sondern um Namen und Adressen von Teilnehmern, um Ursprung und Ziel von E-Mails und aufgerufener Webseiten. Diese Maßnahme wurde 2006 in europäisches Recht aufgenommen (Mathieson 2005).

Diese Art Vorratsdatenspeicherung durch Internetanbieter ging den Briten nicht weit genug. So stellte die britische Regierung 2008 ein neues Überwachungsprogramm beispielloser Reichweite vor. Innenministerin Jacqui Smith gab das ungewöhnliche *Intercept Modernisation Programme* (Programm für Kommunikationsüberwachung, IMP) der britischen Regierung bekannt. Mit geschätzten Kosten von 12 Milliarden Pfund kam das Vorhaben einem gewaltigen Überwachungsprogramm gleich, das weit über alles hinausging, was es in Großbritannien jemals gegeben hatte. Obwohl Europa letztendlich übereingekommen war, Internetanbietern die Speicherung früherer Verbindungsdaten vorzuschreiben, setzte Großbritannien dennoch auf die Schaffung eines riesigen regierungseigenen Speichers mit eben derselben Funktion. Einfach ausgedrückt: Die Regierung wollte alle Daten selbst speichern. Das hätte die Erfassung und Speicherung von Einzelheiten aller Telefonate und E-Mails, von Texten und Webzugriffen aller Briten bedeutet, weshalb Lord Carlisle of Berriew, Kronanwalt und Großbritanniens *Independent Reviewer of Terrorism Legislation* (vom Antiterrorgesetz autorisierter unabhängiger Kontrolleur, IRTL), sogleich seine Besorgnis über die neue regierungseigene Datenbank ausdrückte: „Die

bloße Vorstellung ist entsetzlich." Und er fügte hinzu: Es würde darauf hinauslaufen, dass die Behörden wahllos und ohne Kontrolle recherchierten (Verkaik und Morris 2008).

Ende 2008 veranlasste die wachsende öffentliche Ablehnung die Regierung, den Gesetzentwurf im letzten Moment zurückzuziehen. Stattdessen beschloss sie, den Plan durch List zu realisieren. Bemerkenswerterweise ohne jegliche Gesetzgebung wurde ein Pilotvorhaben mit geschätzten Kosten von zwei Milliarden Pfund auf den Weg gebracht. Es wurden sogar „Stichproben" bei einem großen Festnetz- und einem großen Mobilfunkanbieter gemacht. Die britische Regierung hatte stets darauf beharrt, bei IMP ginge es nur darum, bestehende Möglichkeiten der Kommunikationsüberwachung in einer Welt raschen technologischen Wandels zu erhalten. Die Wirklichkeit sah aber ganz anders aus. Im April 2009 sucht das GCHQ per Anzeige einen neuen Leiter für ein ehrgeiziges Programm, dass es *Mastering the Internet* (Das Internet beherrschen) nannte. Der finstere Projektname erregte Aufsehen, und das GCHQ sah sich bald zu einer öffentlichen Erklärung gezwungen, in der es die Entwicklung einer Technologie dementierte, die eine Überwachung aller Internetnutzung, Telefongespräche und Bürger in Großbritannien ermögliche.

Im August 2009 jedoch wurden die Regierungsdementis von Plänen erweiterter Überwachung offen angefochten. Die britischen Telekommunikationsunternehmen und Internetanbieter selbst, darunter British Telecom und Virgin, verurteilten diese Pläne als unberechtigten Eingriff in die Privatsphäre. Genau die Unternehmen, auf die die britische Regierung zur Realisierung ihres Vorhabens angewiesen war, gaben deutlich zu verstehen, dass die Regierung in Bezug auf die geplante umfassende Überwachung gegenüber der Öffentlichkeit nicht ehrlich war. Sie erklärten der Regierung: „Wir halten die Beschreibung des Regierungsvorhabens als „Aufrechterhaltung" bestehender Möglichkeiten für unaufrichtig: Das Datenvolumen, dass die Regierung nun [von uns] zu erfassen und zu speichern erwartet, ist beispiellos, ebenso wie das Ausmaß, in dem so in die Privatsphäre der Bürger eingegriffen wird … Es ist eine rein diplomatische Umschreibung, die nur dem Zweck dient, Zustimmung zu gewinnen, indem das Ausmaß der geplanten staatlichen Machterweiterung verschwiegen wird." Die britischen Internetanbieter scheuten auch das gewaltige Volumen persönlicher Telefon- und Internetdaten, die zu speichern von ihnen erwartet wurde. Sie beschwerten sich sogar, dass ihnen „keine Anlagen bekannt" seien, die sie überhaupt in die Lage versetzen könnten, „ein solch großes Datenvolumen zu erfassen und zu speichern" (Leppard 2009).

Was wollte die Regierung mit all diesen Daten? Und warum sollten sie zentral gespeichert werden? Die Antwort lautet einfach „Data-Mining" (intelligente Datenanalyse), eine Praxis, die heute die heimtückischste Bedrohung persönlicher Freiheit darstellt. Was Überwachung im Zeitalter allgegenwärtiger Computer und Mobilgeräte zu etwas Besonderem macht, ist: Unsere Daten werden nie gelöscht. Millionen von Einzelheiten über unser tägliches Leben werden routinemäßig gespeichert; irgendwann in der Zukunft kann all dies zusammengeführt und durchsucht werden, um bestimmte Muster zu erkennen. Was zunächst eingeführt wurde, um das Leben leichter zu machen, etwa Mobiltelefone, vermittelt auch ein genaues elektronisches Abbild unseres Lebens. In Großbritannien wurden 2006 rund 60 Milliarden SMS verschickt, zusammengenommen ein Bild unserer digitalen Lebens aus winzigsten Mosaiksteinchen. Noch vor zehn Jahren wurden diese Daten von den meisten Unternehmen verworfen; heute aber, da sich die Speicherkosten alle zwei Jahre halbieren, behalten sie viele Firmen. Was viele Regierungen heute gerne hätten ist, diese Daten zu übernehmen und für eine völlig neue Art von Geheimdienstarbeit zu nutzen, mit neuen, vor fünf Jahren noch unvorstellbaren mächtigen

Analysewerkzeugen (Sommer und Hosein 2009).

Beim Data-Mining durchsuchen Computer unvorstellbare Datenmengen nach Informationen, die Muster und statistische Beziehungen ergeben. Das ermöglicht Regierungen, nach Personen oder Gruppen mit einem bestimmten Verhalten zu suchen und Profile von Verdachtspersonen zu erstellen. Intelligente Datenanalyse ist so mächtig wie gefährlich. Mächtig ist sie, weil man mit ihr riesige Mengen persönlicher Daten sichten kann, gefährlich, weil sie häufig „Falschmeldungen" ergibt. Mit anderen Worten: Mancher wirkt verdächtig, weil sich eine Reihe zufälliger Aktivitäten zu einem Muster verbinden, das der Computer für problematisch hält. Ferner ermöglicht sie *Social Profiling*, also die Erstellung eines Profils gesellschaftlichen Verhaltens. Derzeit ist Data-Mining begrenzt, weil nur die Regierung auf so große Datenmengen zugreifen kann. Allerdings gibt es durchaus Begehrlichkeiten. Nach dem *Regulation of Investigatory Powers Act* 2000 (RIPA, Gesetz zur Regelung der Telekommunikationsüberwachung) können die Behörden Internetanbieter oder Mobilfunkfirmen auffordern, ihnen Einzelheiten zu Telefonaten, E-Mails und Internetnutzung bestimmter Kunden zu überlassen, ohne dafür eine Anordnung haben zu müssen. Im Jahr 2008 richteten die Behörden an Telekomunternehmen die atemberaubende Zahl von 504.073 solcher Aufforderungen. Allein dies ist zwar schon zuviel, doch immer noch „Kleinkram", weil es nur um die Überwachung von Einzelpersonen geht. Der nächste Schritt zur Überwachung in großem Maßstab ist eben Data-Mining. Für viele Staaten sind große Vorräte persönlicher Daten wie bei Facebook und Google der große Preis; Snowden behauptet, sowohl NSA als auch GCHQ hätten danach gegriffen (Harding 2013).

7.9. Snowden

Ende der 1990er Jahre befand sich die NSA in der Krise. Das Internet wuchs exponentiell, und das Mobilfunkaufkommen stieg ins Unermessliche. Die Informations- und Kommunikationsrevolution war in vollem Gange, und dennoch waren die Etats der NSA und ihres britischen Partners gekürzt worden. Der damalige NSA-Direktor Michael Hayden strebte engere Beziehungen zu Microsoft und Google an, um bei der Entwicklung vorn bleiben zu können. Ferner privatisierte er einige Back office-Bereiche der NSA, um Kosten zu senken und die Dynamik der IT-Branche zu nutzen. Durch diese Hintertür kam Edward Snowden. Snowden hatte 2012 eine neue NSA-Stelle angetreten, dieses Mal in Hawaii, einem Knotenpunkt im Späh- und Lauschsystem von NSA, GCHQ und ihren Verbündeten. Dadurch hatte er Zugriff auf Hunderttausende Dokumente, aus denen hervorging, wie der Westen im Twitter-Zeitalter streng geheime Signalaufklärung betrieb (Harding 2013, 37-9).

Am 6. Juni 2013 enthüllte Glenn Greenwald vom *Guardian*, dass die NSA routinemäßig die Aufzeichnungen der Telefondaten von Millionen Verizon-Kunden abgriff. Amerikanische Spitzenanwälte von Harvard und Yale beurteilten diese Aktivitäten als illegal und verfassungswidrig. Es folgten Einzelheiten zum ebenfalls streng geheimen Überwachungsprogramm PRISM; es wird von der NSA geführt und ermöglicht ihr Zugriff auf die Systeme von Internetriesen wie Facebook, Yahoo, Microsoft und Skype. Präsident Obama suchte zu beschwichtigen. Es zeigte sich jedoch bald, dass Snowden sehr viel mehr als die Dokumente gestohlen hatte, bei denen es um ein oder zwei Massenüberwachungsprogramme ging, und vieles davon betraf die britischen Aktivitäten. In der Öffentlichkeit verteidigte die amerikanische

Regierung ihre Programme standhaft; intern war sie über die Enthüllung der Aktivitäten ihres britischen Partners GCHQ bestürzt.

Bald nämlich deckten die Zeitungen auf, wie Gordon Brown das GCHQ autorisiert hatte, ausländische Staatschefs bei zwei G20-Gipfeln in London 2009 auszuspähen. Die Zeitungsartikel kamen zur unrechten Zeit, denn Cameron bereitete einen G8-Gipfel in Nordirland vor. Zugegen waren auch Wladimir Putin, Barak Obama und Angela Merkel. Snowdens Enthüllungen warfen die naheliegende Frage auf: Zu genau welchen Maßnahmen gegen seine erklärten Freunde, mit denen er nun das Podium teilte, hatte der Premierminister das GCHQ befugt? Die Medien mochten die persönliche Animosität, und alle Zeitungen brachten ein Foto der beunruhigten Bundeskanzlerin, wie sie in ihr stets mitgeführtes Handy sprach.

Die Regierung reagierte rasch. Im Juli 2013 erschienen zwei GCHQ-Agenten beim *Guardian* – von den Journalisten der Zeitung mit dem Spitznamen „Hobbits“ belegt –, um die Herausgabe bzw. Zerstörung der Festplatten mit Informationen zu fordern. Am 20. Juli kehrten sie mit einem Entmagnetisierer zurück, einem Gerät, mit dem sich magnetische Datenträger zuverlässig löschen lassen, und drangen zu einem fensterlosen Keller tief unter den Räumen des *Guardian* vor. Mitarbeiter der Zeitungen beobachteten, wie die Hobbits zu Bohrmaschinen und Winkelschleifern griffen. Funken flogen. Was Cameron gern überspielt hätte war, dass ihm die Strafverfolgung nach dem *Official Secrets Act* gedroht hatte; er ließ die Möglichkeit fallen, den Herausgeber einer führenden Zeitung ins Gefängnis zu bringen. Herausgeber und Chefredakteur Alan Rusbridger hatte Camerons Vorhaben vorausgesehen und erkannt, dass er praktisch unverwundbar war.

Drei weitergehende Sicherheitsfragen stellten sich. Erstens: Wie wirkten sich Snowdens Enthüllungen auf die Kommunikationspraxis von Terroristen und international operierenden Kriminellen aus? Kurzfristig hielten die sich von ihrer Elektronik fern, langfristig strebten sie eine bessere Verschlüsselung an. Zweitens: So unterschiedlichen Ländern wie Kirgisien und Brasilien wurden nun die neuen Möglichkeiten elektronischer Überwachung zum Ausspähen ihrer Bürger bewusst; sie standen nun beim Kauf von Überwachungssoftware Schlange. Drittens: Die von NSA und GCHQ angewandten Methoden zur passiven Spionage öffneten anderen Staaten und nichtstaatlichen Akteuren die Augen; sie erkannten die Potenziale und konnten sie nun für Verbrechen oder Sabotage nutzen. All dies hatte ursprünglich wohl nicht in Snowdens Absicht gelegen.

Das britische Kabinett hatte die Komplexität des Problems nicht erkannt. Da NSA und GCHQ ihr Augenmerk weniger auf Staaten als auf verdächtige Personen richteten und Supermarkt-Kundenkarten für Spähoperationen nun genauso wichtig waren wie Nachrichtendienste, konnten ernsthafte öffentliche Debatten über Freiheitsrechte nicht mehr geführt werden, ohne einige Informationen über Quellen und Methoden preiszugeben, die für Terroristen von Nutzen sein konnten. Snowden war daher beides in einer Person – Held und Schurke. Hinzu kam, dass Cameron und sein Außenminister mit ihren Beteuerungen, das GCHQ habe nicht ungesetzlich gehandelt, unrecht hatten. Nach komplizierten, über ein Jahr dauernden Ermittlungen, erklärte das *Investigatory Powers Tribunal* (IPT, „Gericht für die Geheimdienstaufsicht“) das von GCHQ und Amerikanern gemeinsam durchgeführte Programm zur massenhaften Überwachung für gesetzwidrig (Bowcott 2015).

Frühere GCHQ-Mitarbeiter beharren darauf, dass die Übertretung nicht vorsätzlich war, und

verweisen auf die Zahl der Anwälte im GCHQ – einige der wichtigsten Personen in dem riesigen Rundgebäude. Ferner betonen sie, dass der massenhafte Zugriff auf personenbezogene Daten nicht dasselbe sei wie Massenüberwachung. Jedenfalls sei das Interesse der Sicherheitsbehörden zum großen Teil auf Geodaten oder Verbindungsmuster und soziale Netzwerke gerichtet – nicht auf Verbindungsinhalte. Ein Großteil dieser Arbeit hätten Computer anonym erledigt – es gab keine Spione, die Bürger observierten. Dagegen war für Snowden, den *Guardian* und die Bürgerrechtler der Aspekt der künstlichen Intelligenz – mit dem Beigeschmack von „Terminator" – der beunruhigendste. Was eigentlich die Privatsphäre verletzende Überwachung ausmacht, stand nun zur Diskussion – und lag weitgehend im Auge des Betrachters (CI).

Einer der größten Fehler des GCHQ war die Weigerung, sich zu erklären. Während MI5 und MI6 kürzlich ihre Archive für unabhängige Historiker öffneten, wollte das GCHQ diesen Weg nicht beschreiten. Selbst sein amerikanischer Partner, die NSA, hatte eine zuvor als streng geheim eingestufte und codewortgeschützte vierbändige bis 1989 reichende Geschichte der Behörde freigegeben. Das GCHQ-Presseamt war ein Durcheinander; ein Pressesprecher, Alfred Bacchus, wollte es sogar wegen Rassendiskriminierung verklagen. Frühere GCHQ-Direktoren wie David Omand beteiligten sich im Sommer 2013 an der Debatte und leisteten wichtige Beiträge, das GCHQ selbst aber glänzte durch Abwesenheit. Cameron schritt mit einer dramatischen Geste ein. Er ernannte mit Robert Hannigan jemanden zum neuen Direktor, der nie zuvor in einem Nachrichtendienst gearbeitet hatte. Hannigans berufliche Laufbahn begann in einem PR-Unternehmen, bevor er ins Pressereferat des *Northern Ireland Office* kam. Nach dem Weggang seines Chefs rasch befördert, wechselte er in Alastair Campbells Bereich Kommunikation und Strategie der britischen Regierung von Tony Blair. Cameron schuf ferner eine neue Presseabteilung im zentralen Geheimdienstapparat in Downing Street, um eine Gruppe von seines Erachtens geheimdienstfeindlichen Journalisten, NGOs und Anwälten zurückzudrängen.

8. Kontrolle der Nachrichtendienste und Sicherheitsbehörden

8.1 Parlamentarische Kontrolle und Europäischer Gerichtshof

In den 1990er Jahren war der britische Sicherheitsapparat mit einem Umbruch der Regulierung konfrontiert. Den Anstoß gaben vor allem zwei Fälle vor dem Europäischen Gerichtshof für Menschenrechte (EGMR). Die erste Klage wurde 1984 von [der Labour-Politikerin] Harriet Harman eingebracht, als durch einen MI5-Mitarbeiter bekannt wurde, dass über sie und einen Mitarbeiter Akten geführt wurden. Der Kernpunkt ihrer Beweisführung war, dass MI5 keine Klagebefugnis besitze und geeigneter Mechanismen für Aufsicht und Berichtspflicht entbehre. Im Fall Leander von 1987 urteilte der Europäische Gerichtshof gegen den schwedischen Nachrichtendienst aus ähnlichen Gründen. Wie die meisten europäischen Staaten taten auch Großbritannien und Schweden so, als existierten ihre Sicherheitsdienste gar nicht, in der Hoffnung, dass Sicherheitskräfte nie gefasst würden. In ganz Europa hatte man es nun sehr eilig, die Behörden in die Gesetzbücher einzutragen. Trotz anfänglicher Befürchtungen bedeuten eine sichere Rechtsstellung und klare Richtlinien für die Überwachung, dass die Behörden mehr Operationen durchführen können. Die Rechtsvorschriften sind großzügig, da das Kriterium nun

lautet: „Ist es legal?“ und nicht: „Werden wir erwischt?“ Dieses Ergebnis hatten Bürgerrechtler, die seit langem für eine stärkere Regulierung eintraten, nicht erwartet, und sie begrüßten es auch nicht.

Mit dem *Security Service Act* von 1989 und dem *Intelligence Services Act* von 1994 hatten die drei wichtigsten britischen Nachrichtendienste ihren Platz im Gesetzbuch und damit formal und offiziell ein Aufgabengebiet. Darüber hinaus fielen die Funktionen des *National Criminal Intelligence Service* (heute *National Crime Agency)* unter das Polizeigesetz von 1997. MI5 behielt ein begrenztes Mandat, gegen Subversion – auch durch Rechtsextreme – vorzugehen, wenngleich der problematische Begriff „Subversion“ im Gesetzestext nicht mehr verwendet wurde. Es wurde eine Reihe von Gerichten und Kommissionen (meist frühere Richter) eingesetzt, die sich mit Beschwerden gegen Operationen befassen sollten. Die Sicherheitsbehörden zogen Personalberater hinzu, um auf Mitarbeiter einzugehen, die Bedenken wegen ihrer Arbeit hegten. Vielleicht am wichtigsten: Sie zauberten etwas hervor, was zum wahrnehmbarsten Mechanismus der Berichtspflicht wurde, das *Intelligence and Security Committee* (ISC).

Der ISC ähnelt auf den ersten Blick einem parlamentarischen Sonderausschuss. Er ist jedoch ein gesetzlich vorgeschriebener Ausschuss und genießt weder die Vollmachten eines Sonderausschusses, noch gehört er zum Parlament. Bis vor kurzem wählte der Premierminister seine Mitglieder, die ihm unterstellt sind, unter den Abgeordneten aus. ISC-Berichte werden zusammen mit den Antworten der Regierung veröffentlicht, jedoch in bereinigter Form, und sie können vom Premier redigiert werden. Kurz: Der Ausschuss besteht aus Abgeordneten, ist aber kein Parlamentsausschuss. Trotz aktueller Reformen fehlt dem ISC eine ausreichend große und seriöse Forschungsabteilung, was ihn neben seinen ausländischen Pendants kraftlos wirken lässt. Inzwischen wenden Mitglieder regelrechter parlamentarischer Sonderausschüsse, in der Regel des Innenausschusses, ein, die Schaffung des ISC beschnitte sie in ihrem Recht, die Sicherheitsbehörden zu überprüfen. Manche beklagen, seine Berichte seien bloße „Audits“ und enthielten kaum Überlegungen oder Analysen, wenngleich mit den Behörden funktionierende Arbeitsbeziehungen unterhalten werden. In der Wissenschaft oder in den Medien gibt es keinen Konsens über die Effizienz des ISC.

Theoretisch setzt der ISC seine Themen selbst, obwohl er in der Praxis dazu neigt, auf Berichte in den Medien und von Aktionsgruppen zu reagieren. Er veröffentlicht Jahresberichte in redigierter Fassung sowie eine Reihe von Sonderberichten zu Themen, die er für wichtig hält. Das ISC-Mandat beschränkt sich auf die Untersuchung von Fragen wie Verwaltung, Verfahrensweisen und Ausgaben; dennoch hat er im Laufe der Jahre an Selbstvertrauen gewonnen. Er prüft zunehmend operative Belange, sodass manche meinen, er sei zu einem ernsten Kritiker der Dienste geworden, wofür die Untersuchung der Behandlung von Gefangenen in Afghanistan und Irak typisch sei (Gill und Phythian 2006; Phythian 2007).

Im Juli 2007 widmete sich Gordon Browns Grünbuch *The Governance of Britain* der Frage, wie der ISC „so weit wie möglich“ nach den anderen Sonderausschüssen auszurichten sei, wozu auch die Wiedereinsetzung eines *Investigator* gehöre, dessen Amt 2004 unvermittelt aufgelöst wurde. Ähnliche Gedanken wurden 2008 im Rahmen der britischen *National Security Strategy* diskutiert. Der ISC wurde 2013 mit dem *Justice and Security Act* reformiert: Er wurde damit zu einem Ausschuss des Parlaments und erhielt umfassendere Vollmachten sowie ein größeres Ausgabengebiet, zu dem auch die operativen Aktivitäten und die Nachrichten- und

Sicherheitsaktivitäten der Regierung gehörten. Heute untersucht der ISC neben den drei Nachrichtendiensten und Sicherheitsbehörden die nachrichtendienstliche Tätigkeit des *Cabinet Office*, darunter JIC, *Assessments Staff* und *National Security Secretariat*. Ferner kontrolliert er den Militärnachrichtendienst des Verteidigungsministeriums und die Abteilung für Sicherheit und Terrorismusbekämpfung im Innenministerium. Mit dem *Security and Justice Act* 2013 sollte auch die Position des ISC als Zentrum formaler Kontrolle gestärkt und die Bemühungen seitens der Justiz abgewehrt werden, in diese Funktion einzugreifen. Zwar kann das Parlament durch die Reformen nach diesem Gesetz die Ausschussmitglieder absegnen, diese müssen aber nach wie vor vom Premierminister nach Abstimmung mit den Oppositionsführern ernannt werden.

Es ist immer wieder versichert worden, der Geheimdienst- und Sicherheitsausschuss ISC unterscheide sich von anderen parlamentarischen Ausschüssen insofern, als er sicherer sei und nichts nach außen dringe. Angesiedelt innerhalb des „ring of secrecy“ (Kreis der Geheimhaltung) hat er in beträchtlichem Maße Zugang zu vertraulichen Dokumenten und Geheimdienstmitarbeitern. Die Dienste legen Wert auf die Geheimhaltungsregelungen, und der Umgang des Ausschusses mit sensiblen Informationen ist wesentlich für den Aufbau vertrauensvoller Beziehungen. Viele Ausschussmitglieder sind frühere Minister und werden häufig wegen ihres sachlichen Auftretens ausgewählt. Allerdings hielt kürzlich der Vorsitzende des ISC seinen Rücktritt für unvermeidlich: Es ging um Fragen parlamentarischer Ethik und das Durchsickern eines ISC-Berichts an die *Sunday Times*.

Auch die Experten sind hinsichtlich des modernisierten britischen Sicherheitsapparates und der Kontrollmechanismen gespalten. Die einen halten die Reformen für einen echten Paradigmenwechsel; andere meinen, die Einführung von Tribunalen, Ausschüssen und Beratern sei ein Versuch, unzufriedene Geheimdienstmitarbeiter aus dem unberechenbaren Einflussbereich der Justiz und normaler Arbeitsgerichte herauszuhalten. Seit Einrichtung der Gerichte Mitte der 1980er Jahre wurden nur sehr wenige Klagen gegen Nachrichtendienste und Sicherheitsbehörden aufrechterhalten. Je nach Perspektive wird dies als beruhigend oder eben als besorgniserregend empfunden (Brown HC 314 2007, sec.38).

Das Argument, Reform und Modernisierung hätten in Wirklichkeit zu größerer Undurchsichtigkeit geführt, überzeugt besonders in Bezug auf die Novelle des *Official Secrets Act*. Im novellierten Gesetz fehlt der unbestimmt-allgemeine Artikel 2, der durch Vergehen gegen bestimmte Gruppen von Personen und Informationen ersetzt wurde. Mit dem Gesetz hat man sich allerdings auch sehr bemüht, die Möglichkeit auszuschließen, dass sich jemand auf das „öffentliche Interesse“ beruft, um zu verhindern, dass Whistleblower die Gerichte nutzen, um ihre Ansichten über Missbräuche in den Behörden zu verbreiten. Darauf haben Whistleblower wie David Shayler, der dissidente MI5-Mitarbeiter, versucht, sich auf Artikel 10 (Schutz der Meinungsfreiheit) der Europäischen Menschenrechtskonvention zu stützen. Dessen ungeachtet können Whistleblower nach wie vor die Anwälte der Regierung ausstechen, wie die Fälle Catherine Gun 2005 und Derek Pasquill 2007 zeigen (Gill 1996, 313-320; Morrison 2006, 51-2).

Im britischen Parlament hat es der ISC mit ernsteren Rivalen zu tun. Verschiedene Sonderausschüsse haben Aufgabengebiete, die sich überschneiden, etwa Verteidigung, Außenpolitik, Inneres, Nordirland und Terrorismus. Manche neigen zu eigenen Untersuchungen in Bereichen, die auch vom ISC geprüft werden, beispielsweise der Außenausschuss, der die Begründung der Regierung für den Krieg gegen den Irak untersuchte (FAC 2004). Der Gemeinsame Menschenrechtsausschuss untersuchte Vorwürfe, Mitarbeiter britischer

Nachrichtendienste seien mitschuldig an Folter (JCHR 2009). Die Einsetzung eines unabhängigen Ausschusses unter Vorsitz von Lord Butler, der Geheimdienstinformationen über irakische Massenvernichtungswaffen untersuchte, wurde weithin als Eingeständnis gewertet, dass die Befugnisse des ISC nicht ausreichen, sich mit ernsten Problemen zu befassen.

Die meisten Experten sind heute äußerst skeptisch hinsichtlich der eiligen Versicherungen des ISC im Juli 2013 nach den Snowden-Enthüllungen. Insbesondere scheint die Entgegennahme von NSA-Material ohne entsprechende Anordnung den Beteuerungen des ISC zu widersprechen, dass eine von einem Minister unterzeichnete Überwachungsanordnung immer dann vorlag, wenn das GCHQ die Amerikaner um nachrichtendienstliche Informationen ersuchte. Inwieweit das gesamte Material, das dem GCHQ von seinem transatlantischen Partner überlassen wurde, durch solche Anordnungen gedeckt war, ist nach wie vor unklar. Nach den Aussagen des GCHQ vor dem IPT („Gericht für die Geheimdienstaufsicht“) erhält Cheltenham außer den Ergebnissen von Überwachungen nach einer Anordnung gemäß dem Gesetz über die Telekommunikationsüberwachung (RIPA) auch nicht ausgewertetes Material ohne die erforderliche Anordnung, wenn „es technisch nicht machbar ist, die Ergebnisse durch eine RIPA-Anordnung zu bekommen“ (Ogilvie & Sankey, 2014).

Die Nachrichtendienste und Sicherheitsbehörden beantragen nach dem RIPA von 2000 normalerweise zweierlei Arten von Anordnungen. Der Innenminister kann eine Anordnung nach Artikel 8(1) ausstellen, die sich auf die Kommunikationsüberwachung bestimmter Personen oder Örtlichkeiten bezieht. Der Außenminister kann eine Anordnung nach Artikel 8(4) ausstellen, die sich auf die Kommunikation von außen oder im Ausland bezieht und häufig allgemeiner ist. Beide Formen der Anordnung können sich auf Material von Diensten anderer Staaten beziehen. Die Diskussion dreht sich um weiteres nicht ausgewertetes Material, das ohne die erforderliche Anordnung des Außenministers entgegengenommen wird. Der ISC hatte das GCHQ rasch von den PRISM-Vorwürfen entlastet, teils weil das GCHQ beteuerte, nicht rechtswidrig gehandelt zu haben. (Bislang hat noch niemand etwas über weiteres Material wissen wollen, das von anderen Five Eyes-Verbündeten, von Mitgliedern im Verbund „Nine Eyes“ in Europa, wie Frankreich, oder von anderen bilateralen Partnern wie Schweden übernommen wurde.) Dem ISC wurde nachgewiesen, in der Sache Snowden im Unrecht gewesen zu sein und ebenso sich bezüglich der Qualität der Irak-Erkenntnisse 2004 geirrt zu haben, sodass heute seine Ermittlungsbefugnisse in Zweifel gezogen werden.

8.2 Die Rolle der Medien

Die Fehler des Parlaments und der Kabinettsmitglieder zeigen die wachsende Bedeutung der Medien als weiterem Kontrollorgan. Wie der Innen-Sonderausschuss des Unterhauses bestätigt, war die Pressefreiheit für die Berichte über die Snowden-Affäre zentral. In Großbritannien wird die Pressefreiheit durch die Bestimmungen der Europäischen Menschenrechtskonvention zur Meinungsfreiheit garantiert, nicht durch einen Grundrechtekatalog ähnlich dem 1. Zusatzartikel der US-Verfassung. Laut Ewan MacAskill, einem der wichtigsten britischen Journalisten, die über die Snowden-Affäre berichteten, konnten zwar die US-Medien die Snowden-Dokumente veröffentlichen, der *Guardian* wurde jedoch von der britischen Regierung wiederholt unter Druck gesetzt. Dieser Vergleich ist nicht ganz aussagekräftig. In den Vereinigten Staaten herrscht ein eher regelloses System mit direkten Telefonverhandlungen zwischen Regierung und Herausgebern, das einer weniger formalen und weniger effektiven Version des britischen Systems gleichkommt. Es ist auch falsch zu behaupten, in den Vereinigten Staaten gäbe es keine

Entsprechung zum *Official Secrets Act*. Es gibt dort sogar Gesetze, die sowohl die Identität von Agenten als auch bestimmte Erkenntnisse der Signalaufklärung (SIGINT) schützen, wenngleich Letztere eher selten gegen die Presse gerichtet werden (MacAskill in Moore 2014).

Wie die US-Regierung ergreift auch die britische Regierung selten rechtliche Schritte gegen die Medien, wenn sie vertrauliche Informationen an die Öffentlichkeit bringen. Dies liegt teils daran, dass häufig Minister oder frühere Minister und ihre Berater für die Informationsweitergabe verantwortlich sind; wenn sie zudem frühere vertrauliche Dinge in ihren Memoiren ansprechen, genießen sie offenbar Immunität. Staatsanwälte sind sich ebenfalls bewusst, dass es auch die durchaus reale Gefahr gibt, dass die Richter einen Angeklagten aus grundsätzlichen Erwägung für unschuldig erklären. Dennoch hat die Regierung in der Snowden-Affäre mit einstweiligen Verfügungen gedroht. Geradezu abenteuerlich war die vom GCHQ geleitete Zerstörung der Festplatten im Guardian-Keller, wo die Snowden-Dokumente gespeichert gewesen sein sollen (siehe oben S. xx). Ergebnis: Der *Guardian* speichert seine Kopien nicht mehr in London, sondern ist auf die *New York Times* angewiesen, um in dem Material zu recherchieren. Journalisten des Guardian, die am Snowden-Fall arbeiten, suchen jetzt die Büros der *New York Times* auf. Manche meinen, der Fall Snowden zeige, dass eine ordnungsgemäße Geheimdienstkontrolle nur funktioniert, wenn Großbritannien ähnliche Verfassungsartikel wie der 1. Zusatzartikel zur amerikanischen Verfassung hätte. Allerdings wird dabei wohl ignoriert, dass die Berichte von Dana Priest von 2005 über Geheimgefängnisse in Europa auf Antrag der US-Regierung zensiert und die Namen der Länder mit diesen Gefängnissen gestrichen wurden. Kurz: Die amerikanischen und britischen Systeme ähneln sich mehr, als es auf den ersten Blick scheint.

Der Kern des britisches Systems zum Ausgleich zwischen den kollidierenden Ansprüchen nationaler Sicherheit und Berichterstattung im öffentlichen Interesse gehört damit grundsätzlich zur allgemeinen Ökologie der Geheimdienstkontrolle. Das *Defence and Security Media Advisory* (DSMA) System (zuvor *Defence Advisory Notice System)* ermöglicht die freiwillige Redaktion sensiblen Geheimdienstmaterials. Dadurch können Herausgeber und Behörden sich informell ins Benehmen setzen und einen Mittelweg anstreben, bevor ein Artikel veröffentlicht wird, sodass über vieles, wenn auch nicht über alle Einzelheiten berichtet werden kann. Die ursprüngliche Entscheidung des *Guardian*, sich darauf bei Berichten über das Snowden-Material nicht einzulassen, verschärfte eine Debatte darüber, wie das DSMA-System „im Zeitalter von Internet und sozialen Medien“ effizient funktionieren kann.

Die britische Regierung begründet die Notwendigkeit, die Medien einzuschränken, vor allem mit ihrer internationalen Verantwortung und der nach wie vor bedeutenden Rolle Großbritanniens in der Weltpolitik. Bei Militär- und Geheimdienstoperationen, die diese Position unterstützen, bedeuten Presseberichte ein Risiko für britisches Kräfte im In- und Ausland und könnten Leben kosten bzw. Militäreinsätze gefährden. Nachrichten sind zwar international, doch stammen die meisten Artikel über die britische Sicherheit aus dem Inland, sodass das DSMA-System nach wie vor bei der Mehrzahl von Berichten greift, die der nationalen Sicherheit schaden könnten. Die Beteiligung am DSMA-System ist völlig freiwillig, was seinen Einfluss auf die Medien wiederum begrenzt. Allerdings eröffnen Pressekonsultationen und die unumgänglichen Gespräche mit den Diensten die Möglichkeit einer gerichtlichen Anordnung gemäß OSA; ebenso könnten auf dieser Grundlage bei längeren Gesprächen, unterstützt durch andere Kanäle, nachrichtendienstliche Erkenntnisse gegen undichte Stellen gesammelt werden (Vallance in Moore 2015).

Inwieweit ist die Steuerungsfunktion durch das DSMA-System für den Umfang verantwortlich, in

dem über Snowden in den britischen Medien berichtet wurde? Es gibt gewiss ständige DSMA-Anforderungen, die sich auf Dinge wie Signalaufklärung beziehen und von einer Berichterstattung abhalten. Funk und Fernsehen reagierten unterschiedlich, während andere Medien meist dazu neigten, die Snowden-Enthüllungen nach dem Sommer 2013 nicht weiter zu beachten. Die BBC berichtet hin und wieder darüber, Zeitungen wie *Times, Telegraph, Mail* und andere dagegen nur in begrenztem Umfang. Einigen Journalisten zufolge liegt dies weniger an der Steuerungsfunktion durch das DSMA-System als daran, dass der Murdoch-Konzern keine Sendezeit für *Guardian*-Berichte bereitstellen wollte, die einigen wie ein Kreuzzug vorkamen. In manchen Fällen wurde der Inhalt, selbst bei den seriösen Zeitungen, einfach für zu technisch gehalten (CI). Ein Faktor ist auch die nationale Kultur. In den Vereinigten Staaten betrachtet man die Bundesregierung ohnehin mit Argwohn. In Deutschland riefen die Snowden-Enthüllungen sogar Erinnerungen an den DDR-Sicherheitsapparat wach. In Großbritannien aber wird elektronische Überwachung eher wohlwollend mit Bletchley Park oder gar James Bond in Verbindung gebracht (MacAskill in Moore 2014).

Zwischen Geheimhaltung und parlamentarischer Kontrolle herrscht ein Spannungsverhältnis. Bei der Arbeit von Nachrichtendiensten geht es heute weniger um russische U-Boote oder chinesische Raketen, sondern mehr um Menschen. Daher ist es schwieriger geworden, über Bürgerrechte und Grundfreiheiten eingehender ohne eine die nationale Sicherheit gefährdende Preisgabe von Informationen zu diskutieren. In Großbritannien sind Verfahren gemäß OSA Angelegenheit der Kronanwälte; dabei wird über zwei Stufen entschieden, ob es sich lohnt, eine Strafverfolgung einzuleiten. Diese beiden Stufen betreffen die Beweislage und das öffentliche Interesse. Im Fall Snowden gab es klare Beweise für eine vorsätzliche Verletzung des OSA, also hätte man ein Strafverfahren einleiten können. Wäre dieses aber im öffentlichen Interesse gewesen? (McDonald in Moore 2014) Die Regierung bekräftigt zwar, dass eine Strafverfolgung gemäß OSA Angelegenheit der Staatsanwälte ist, doch zeigt die Erfahrung, dass entsprechende Entscheidungen teils politisch motiviert sind, insbesondere die Entscheidung, eine aussichtslose oder verfängliche Klage fallenzulassen. (Aldrich 2010, 360)

8.3 Kontrolle und internationale nachrichtendienstliche Zusammenarbeit

In Großbritannien hat die Snowden-Affäre ein Schlaglicht auf das Problem der Geheimdienstkontrolle und der internationalen nachrichtendienstlichen Zusammenarbeit geworfen. Eine solche Kooperation – oder „Verbindung“ – gilt seit Langem als Bereich, der für Kontroll- und Aufsichtsorgane undurchsichtig ist, auch für Experten, Journalisten und Wissenschaftler ist es ein schwieriges Gelände. Dies liegt teils an der extremen Geheimhaltung, die Nachrichtendienste für die Kooperation vorsehen. Sie wollen nicht nur eine Beeinträchtigung dieser Beziehungen vermeiden, es liegt ihnen auch nicht viel daran, die eigenen übergeordneten Behörden über das Ausmaß ihrer Abhängigkeit von Partnern in bestimmten nachrichtendienstlichen Bereichen zu informieren. Zudem ist nachrichtendienstliche Zusammenarbeit eine diffuse Angelegenheit und somit an sich schwer zu kontrollieren. Einige größere Nachrichtendienste rühmen sich zwar einer für das Kooperationsmanagement zuständigen Abteilung, in Wirklichkeit aber erstreckt sich Geheimdienstkooperation über alle Aspekte nachrichtendienstlicher Prozesse (Alexander 1998).

Über mehr als ein Jahrzehnt hat sich das „schwarze Loch“ internationaler

nachrichtendienstlicher Zusammenarbeit rasant ausgedehnt. Stephen Lander, der Generaldirektor des MI5, hält ihr exponentielles Wachstum in den letzten zehn Jahren für die bedeutendste Veränderung in der Welt der Nachrichtendienste (Lander 2004). Am deutlichsten äußerte sich dies nach 2001 in Zusammenhang mit dem weltweiten „Krieg gegen den Terror", der das Wachstum dieses Bereichs stark beschleunigte. Er führte ferner zu aggressiveren Operationen durch im Verborgenen operierende Kräfte – dazu gehören auch Überstellungen –, auf deren Untersuchung einige Parlamente großen Wert legen. Dies spiegelt eine grundlegendere Änderung in der Art der Geheimdienstaktivitäten wider, die sich seit Mitte der 1990er Jahre entwickelte, nämlich Globalisierung (siehe oben, Abschnitt 7.5). Die meisten Ziele der Nachrichtendienste seit Ende des Kalten Krieges haben eine zunehmend globalisierte Dimension, sodass die Nachrichtendienste und Sicherheitsbehörden wiederum gezwungen sind, ihre Aktivitäten zu globalisieren. Die Behörden sowie ihre Operationen und Ziele bewegen sich in transnationaler Richtung. Die sich daraus ergebenden Veränderungen bringen die Entwicklung eines globalen Systems nachrichtendienstlicher Kooperationen und die beschleunigte Privatisierung einiger zentraler Funktionen mit sich. Dann überrascht es kaum, dass Kontrolle und Aufsicht schwieriger werden.

Der Begriff „Globalisierung" wird zwar in der Öffentlichkeit wie in der akademischen Welt *ad nauseam* gebraucht, jedoch kaum eindeutig definiert. Jan Arte Scholte betont in seinen häufiger zitierten Schriften eher die räumlichen (oder räumlich-zeitlichen) Aspekte dieses Phänomens. Unter dieser Perspektive geht es hauptsächlich um Sozial- und politische Geographie, gekennzeichnet durch die Entwicklung „supraterritorialer Räume", die parallel zu herkömmlicher souveräner Territorialität existieren (Scholte 2000). Diese spezielle Auffassung von Globalisierung lässt sich unmittelbar auf die heutigen nachrichtendienstlichen Ziele, Behörden und Operationen beziehen. Seit dem Ende des Kalten Krieges sehen sich Staaten zunehmend mit Sicherheitsproblemen konfrontiert, die von nichtstaatlichen Akteuren ausgehen. Die Staaten verschärfen die Situation noch, indem sie dem freien Verkehr von Geld, Fachwissen, Nachrichten und Ideen die Grenzen öffnen, um vom exponentiellen Wachstum des Handelsvolumens zu profitieren. Terroristen, Kriegsherren und Kriminelle machen sich diese Freiheit ebenfalls zunutze. Viele feindliche Kräfte reiten auf der Welle der Globalisierung und nutzen verteilte Netzwerke, um ihre Aktivitäten zu verbergen, und sind dadurch schwer greifbar (Naim 2005).

Wir erleben nicht nur eine quantitative Zunahme der Kooperationen von Nachrichtendiensten unterschiedlicher Staaten, sondern auch qualitative Veränderungen. Wir erleben zuvor nicht für möglich gehaltene Partnerschaften, weniger die aus dem Kalten Krieg vertrauten Geheimdienstkombinationen. Während sich der Großteil sinnvollen Austauschs auf bilateraler Ebene vollzieht, nimmt auch die Kooperation in Bereichen wie Ausbildung und Feldeinsätzen zu. Und wir erleben einen auffallende Zunahme der Operationen. Über den Umfang, in dem diese bilateralen Beziehungen und Austausche durch rechtskräftige Vereinbarungen ordentlich geregelt werden, kann gestritten werden (CI).

Globalisierung wird eng verbunden mit der kosmopolitischen Vorstellung vom Weltbürger, die gemeinsame liberale und humane Werte und – natürlich – Menschenrechte impliziert. Also interessieren sich die Institutionen der Europäischen Union heute stärker für die Geheimdienstkontrolle. Sie haben wohl keine andere Wahl, angesichts des wachsenden Einflusses der Nachrichtendienste als Form der Polizeiarbeit für die Schattenseiten der Globalisierung. Vor allem die europäischen Ermittlungen zu den Überstellungen waren

erfolgreich und trugen dazu bei, wichtige Untersuchungen zu diesem Thema seitens des Genfer Zentrums für die demokratische Kontrolle der Streitkräfte (DCAF) in Zusammenarbeit mit dem norwegischen Parlament anzustoßen (Born & Leigh 2010).

Die wichtigste Veränderung in Bezug auf die Geheimdienstkontrolle ist der Aufstieg der globalen Zivilgesellschaft. Hier manifestiert sich Globalisierung in den Verbindungen zwischen den Polizeien und den Sicherheitsdiensten, sodass die Unterscheidung der Dimensionen „innen“ und „außen“ unscharf wird. Und schließlich: Private Sicherheitsfirmen und privatwirtschaftliche Anbieter nationaler Infrastrukturen – zuweilen selbst multinationale Unternehmen – spielen in Geheimdienstfragen eine größere Rolle in Form von Bürgerinitiativen und transnationalen Gremien, die themenbezogene Kampagnen wie Menschenrechte und Umwelt führen.[2] Die Zahl transnationaler NGOs verdoppelte sich in den 1990er Jahren. Freilich umfasst die transnationale Zivilgesellschaft sowohl zivile wie nichtzivile Elemente. Die förderlichen Aspekte der Globalisierung – nicht zuletzt das Internet –, die neue Formen oppositioneller Politik ermöglichen, sind häufig dieselben Aspekte, die neue Formen der Unsicherheit durch transnationale Bedrohungen erzeugen. Es gibt die Auffassung, dass diese informellen Netzwerke der *countersurveillance* oder Gegenüberwachung durch Aktivisten und Interessengruppen, obwohl sie Nachrichtendienste nicht direkt zur Rechenschaft ziehen können, sich offenbar dennoch weniger um staatliche Grenzen scheren als nationale Komitees und Untersuchungsausschüsse (Kalathil und Taylor C. Boas 2003).

Gehen wir davon aus, dass sich nachrichtendienstliche Tätigkeiten heute globalisieren, dann gibt es eine erkennbare Diskrepanz zwischen den aufkommenden neuen Formen operativer Aktivitäten und den herkömmlichen Mustern der Rechenschaftslegung, die zunehmend beschränkt erscheinen. Nachrichtendienstliche Zusammenarbeit bildet für Kontroll- und Aufsichtsgremien immer eine Herausforderung. Wie der Fall Snowden zeigt, haben Umfang und Ausmaß der Kooperation zu einem qualitativen Wandel geführt, durch den sich herkömmliche Formen der Rechenschaftslegung – im souveränen Nationalstaat begründet – zunehmend als veraltet und unvollständig erweisen.

Die stärkste Triebkraft informeller Zivilgesellschaft sind die Medien in Verbindung mit Aktionsgruppen. Was aber können die Nationalstaaten selbst tun, um die Rechenschaftslegung so zu erweitern, dass sie auch nachrichtendienstliche Zusammenarbeit einbezieht? Dass mit Politikern besetzte Ausschüsse Einblick in diesen sensiblen Bereich erhalten, ist nach wie vor relativ unwahrscheinlich. Allerdings könnte eine bislang wenig geprüfte Alternative im Amt eines Generalinspekteurs bestehen, der erweiterte Vollmachten erhält, um in mehr als einem Land tätig zu werden. Wenn nachrichtendienstlich kooperierende Staaten komplexe Protokolle für die Weitergabe sensiblen Materials vereinbaren können, können sie sich auch über gemeinsame Richtlinien für inspizierende Beamte einigen. Das Amt des Generalinspekteurs hat wohl seine Defizite insofern, als seine Untersuchungen intern sind, also eher wie bei polizeilichen Einheiten für innere Angelegenheiten. Aber im hochgeheimen Bereich nachrichtendienstlicher Zusammenarbeit ist diese Option wohl das, was gebraucht wird. Ein hoher Geheimdienstbeamter, vielleicht ein angesehener früherer Leiter eines nationalen Dienstes, könnte als „fliegender“ Generalinspekteur für eine Reihe kooperierender Länder dienen und vielleicht einem Organ wie der NATO untergeordnet sein. Dies würde bei vielen Beamten zweifellos Entsetzen hervorrufen, doch wird dies von Regierungsjuristen als denkbar diskutiert,

[2] Anm. d. Ü.: Möglicherweise hat sich hier die Diktiersoftware sogar sinnentstellend ausgewirkt.

zumindest im Rahmen der prominenteren europäischen, US- und Commonwealth-Dienste.

9. Schutz der Privatsphäre und der Freiheitsrechte in Großbritannien

9.1 Die begrenzten Funktionen des ISC

Viele britische Abgeordnete sind über Geheimdienstfragen und insbesondere technische Überwachungsfragen oft schlecht informiert. Das ist beunruhigend, weil das GCHQ Vorwürfe eigener Mitarbeiter hinsichtlich eines bestimmten Programms häufig einfach damit abtut, man habe nicht gesetzwidrig gehandelt. Das mag zunächst beruhigend scheinen, doch ist klar, dass den Abgeordneten selbst Art und Umfang der Befugnisse, die sie dem GCHQ und anderen gemäß RIPA übertragen hatten, kaum bewusst waren. In Westminster glauben viele, die Hauptaufgabe parlamentarischer Kontrolle sei die Prüfung von Menschenrechtsfragen. Dies gilt besondere für die Mitglieder des Oberhauses. Einige betonen die Bedeutung des Parlaments für Garantien, dass die Nachrichtendienste nicht gegen internationale Verpflichtungen insbesondere nach der Europäischen Menschenrechtskonvention verstoßen.

Dies gibt seit 2005 und der Kontroverse um die Sonderüberstellungen sowie die Aufdeckung der Geheimgefängnisse in Europa durch Dana Priest immer wieder Anlass zu Besorgnis (Bochel et al. 2014, 163). Frühere Minister haben sich öffentlich besorgt gezeigt über das Ungleichgewicht des Geheimdienstaustausches zwischen Großbritannien und den USA und sich laut über „unsere Aufträge“ gewundert, die wir zum Ausgleich erledigen (Patten 2005, 97).

Wie gesehen liegt der Schwerpunkt im ISC-Aufgabengebiet nicht auf der Verteidigung der Freiheitsrechte sondern eher auf Effizienz und Effektivität. Das wichtigste Element im Abwehrschirm für Freiheitsrechte sind zunächst die Anwälte in den Behörden selbst, denen es darum geht, dass ihre Mitarbeiter nicht irgendwann vor Gericht stehen. Das zweite Element bilden Richter, entweder in britischen Gerichten, am Europäischen Gerichtshof oder im Gericht für die Geheimdienstaufsicht (siehe unten). Richter urteilen in Geheimdienstangelegenheiten zunehmend rigoros, weil sie bestürzt feststellen müssen, dass dem ISC an Rechten und Freiheiten nicht viel gelegen ist. Dementsprechend hat das britische Parlament 2013 ein neues Gesetz verabschiedet, das die Position des ISC stärkt und gleichzeitig die Ermessensfreiheit der Gerichte in Geheimdienstangelegenheiten einschränkt – dies war eine Antwort auf die Urteile britischer Gerichte in den Jahren 2008 bis 2010, dass amerikanische Geheimdokumente zur Auseinandersetzung um die Folter veröffentlicht werden durften.

Der ISC hat dennoch die Auffassung vertreten, dass das Gesetz zur Regelung der Überwachung verschärft werden muss. Im März 2015 äußerte der ISC, ein einheitliches vom Parlament verabschiedetes Gesetz solle die komplexen und veralteten Vorschriften zur Regelung der Eingriffsmöglichkeiten britischer Nachrichtendienste und Sicherheitsbehörden ablösen. Bis dahin hatte der ISC einige der massenhaften Überwachungen durch die britischen Behörden nicht einmal zur Kenntnis genommen. Das IPT wiederholend, betrachtet er den Rechtsrahmen

nun als undurchsichtig und veraltet. Die Labour-Abgeordnete und ISC-Mitglied Hazel Blears erläuterte die Einschätzung des Ausschusses und betonte die gestiegenen Erwartungen der Öffentlichkeit an Offenheit und Transparenz hinsichtlich der allgemeinen Befugnisse von Nachrichtendiensten. Ferner wurde die Notwendigkeit betont, das Verständnis in der Öffentlichkeit zu verbessern und ihr Vertrauen zu stärken.

Im jüngsten Bericht widmet sich der ISC insbesondere massenhaften personenbezogenen Daten. Im Zentrum stehen beim ISC nach wie vor Effizienz und Effektivität, weil dem Ausschuss zufolge das GCHQ Zugriff auf den Internetverkehr durch massenhafte Überwachung haben müsse; der ISC versichert, das GCHQ führe keine „pauschale Überwachung" durch, noch entsprächen seine Aktivitäten einer unterschiedslosen oder wahllosen Überwachung. Im Hinblick auf neue Rechtsvorschriften empfahl der ISC, dass Anträge auf Anordnungen standardisiert werden sollten. Das bedeutet, dass GCHQ und SIS in ihren Anträgen nach Artikel 8(4) an den Außenminister auf Anordnungen zur Auslandsüberwachung genauere Einzelheiten nennen müssen (was dem derzeit vom MI5 angewandten Verfahren entspricht). Ähnliches würde für Überwachungsersuchen der Dienste in Whitehall gelten. Dem ISC war sehr daran gelegen, weniger „themenbezogene Anordnungen" zu sehen, die sich auf eine umfassendere definierte Gruppe beziehen und das Risiko einer allgemeinen Erfassung in großem Maßstab bergen. Damit verbunden war die Hoffnung, dass neue Vorschriften kürzere Fristen erlauben. Dies sind allerdings marginale Änderungen, die die an diesem Bereich interessierte Öffentlichkeit nicht überzeugen konnten (CI).

Organisationen wie *The Open Rights Group* fordern, die parlamentarischen Kontrollmechanismen selbst zu reformieren, um Freiheitsrechten höheren Stellenwert zu geben. Ihnen zufolge muss der ISC völlig unabhängig, dem Parlament voll rechenschaftspflichtig und in der Lage sein, die nötige technische, rechtliche und ethische Expertise zur richtigen Beurteilung der Überwachung zu bieten. Dies bedeutet jedoch ein Missverständnis des grundlegenden Problems, dass der ISC immer noch von Interessenkonflikten betroffen wäre. Es wäre wohl besser anzuerkennen, dass der ISC in erster Linie die Effektivität prüft und Fragen von Rechten und Freiheiten anderen Organen überlässt.

Dagegen kann David Anderson, *Independent Reviewer of Terrorism Legislation*, nur wenig Zeit für den ISC aufwenden und betont statt dessen die Bedeutung der Ablösung ministerieller Anordnungen durch ein für Überwachungen zuständiges Gericht nach amerikanischem Vorbild, das unabhängige Urteile zu Überwachungsersuchen sprechen würde. Dem schlossen sich die überlegteren Aktionsgruppen an, ließen politische Kontrolle beiseite und konzentrierten sich auf die rechtliche Anfechtung. Sie haben sich in der Diskussion um Freiheiten weg vom Schutz der Privatsphäre hin zum Schutz der Meinungsfreiheit orientiert – was nach der europäischen Charta der Grundrechte eine solidere Verteidigung ermöglichen würde. Dies wird in den nächsten zehn Jahren wohl ein großes Reizthema sein.

9.2 Independent Reviewer of Terrorism Legislation (IRTL)

Seltsamerweise besitzt eine der effizientesten Institutionen im Bereich Bürgerrechte, Nachrichtendienste und Überwachung keine Klagebefugnis gegen Geheimdienste. Der IRTL muss dem Parlament jährlich Rechenschaft über die Wirkung des Antiterrorgesetzes von 2000

ablegen und kann ferner Stellung zu entsprechenden nachfolgenden Rechtsvorschriften nehmen. Weitere Untersuchungen können auf Antrag der Regierung oder auf eigene Initiative des *Independent Reviewer* eingeleitet werden. „A Question of Trust", ein wichtiger Bericht zur Zukunft der Ermittlungsbefugnisse, wurde im Juli 2014 vom Parlament in Auftrag gegeben und im Juni 2015 veröffentlicht. Im Wesentlichen besteht diese Funktion im uneingeschränkten Zugang in Verbindung mit Unabhängigkeit und Erfahrung als Richter. Seit 2001 hatte die Funktion Lord Carlile of Berriew C.B.E. Q.C. inne, danach, seit Februar 2011, David Anderson Q.C. (Anderson 2014).

Vergleicht man die Tätigkeit von IRTL und ISC, zeigt sich erneut die Unzulänglichkeit letzterer Institution. Andersons Bericht war genauer und aufschlussreicher, und seine Änderungsvorschläge waren gehaltvoller. Zu den Kernthemen des RIPA stellte Anderson fest:

> Das RIPA, von Anfang an unklar formuliert, ist so oft ausgeflickt worden, dass es für jeden, eine kleine Gruppe Eingeweihter ausgenommen, völlig unverständlich ist. Ein Vielzahl alternativer Vollmachten, einige ohne rechtliche Absicherung, machen das Bild noch verworrener. Dieser Zustand ist undemokratisch, unnötig und – auf lange Sicht – unerträglich. (IRTL 2015)

In der Form, doch nicht in Struktur oder Amtsbefugnis, ähnelt der IRTL am ehesten dem Amt eines Generalinspekteurs. Der britische IRTL und der US-amerikanische und australische Generalinspekteur haben außergewöhnlich detaillierte, unvoreingenommene und ausgewogene Stellungnahmen zu einem Themenfeld vorgelegt, das sehr umstritten ist und häufig zu emotional aufgeladener Sprache und untauglichen Reformvorschlägen einlädt. Andersons Überlegungen, so detailliert wie ausführlich, gelten als prägend für die Ansichten der derzeitigen Regierung über die Reform der Überwachungsgesetze. Er empfiehlt vor allem, alle Anordnungen von einem speziellen in einem neuen Gremium (der *Independent Surveillance and Intelligence Commission*) installierten *Judicial Commissioner* („Gerichtskommissar") gerichtlich genehmigen zu lassen. Allerdings ist das US-Modell keineswegs perfekt, da dort Ersuchen selten abgelehnt werden und es von der Bush-Administration auf der Suche nach großen Mengen von Verbindungsdaten sogar umgangen wurde.

9.3 RIPA und das Investigatory Powers Tribunal

Im Grunde haben Bürgerrechte und Freiheit von unnötiger Überwachung in Großbritannien ihre Grenze an der historischen Natur des *Common Law*, das eher den Schutz des Eigentums als der Privatsphäre hervorhebt. Privatsphäre ist etwas Existenzielles, und das britische *Common Law* befasst sich mit solch ephemeren Dingen nicht sehr gründlich. In der Regel gelten heimliche Durchsuchungen durch Beamte nicht deshalb als illegal, weil sie eine Verletzung der Privatsphäre wären, sondern weil es um das Eingreifen und Eindringen in fremdes Eigentum geht. Elektronische Überwachung hat wenig mit Eingriffen in fremdes Eigentum zu tun, weshalb es in Großbritannien gesetzlich ungenügend geregelt war, bis die Europäische Menschenrechtskonvention (EMRK) verabschiedet wurde.

Die Konvention, deren Bestimmungen nach und nach in britisches Recht übernommen wurden,

bietet der Privatsphäre größeren Schutz. In den 1980er erwies sich das Anzapfen von Telefonen, sofern nicht ordnungsgemäß autorisiert, als Verletzung von Artikel 8 EMRK – des Rechts auf Privatsphäre. Im Kern besagte die Rechtsprechung des Gerichtshofs in den 1980er Jahren, dass bei geplanten Geheimdienstaktivitäten entsprechende gesetzliche Regelungen vorhanden sein und die Behörden selbst eigene Rechtspersönlichkeit haben mussten, damit man bei ungerechter Behandlung Rechtsmittel einlegen konnte. In ganz Europa war man daher in den 1990er Jahre um rasche Aufnahme der Nachrichtendienste in die Gesetzbücher bemüht. In Großbritannien verlangt das Gesetz, dass Geheimdienste ihre Aktivitäten auf die Zwecke der nationalen Sicherheit, des wirtschaftlichen Wohls und der Verhütung von schweren Straftaten beschränken.

Wie gesehen hat das Gesetz zur Regelung der Telekommunikationsüberwachung (RIPA) bei Experten, Aktionsgruppen und auch bei David Anderson als IRTL einen schweren Stand. Aber es hat deutlich besser abgeschnitten als der ISC. Wenngleich komplex und heute veraltet, war es ein großer Schritt hin zur Kontrolle des Einsatzes verdeckter Ermittler, eingreifender (intrusiver) Überwachung und des Eindringens in fremdes Eigentum, zur Kontrolle von Agenten, Informanten und verdeckten Ermittlern aller Behörden. Die Urheber des Gesetzes waren erkennbar und anerkennenswert bemüht, Elemente der EMRK in seine Wirkprinzipien einfließen zu lassen. Die großartigen Grundsätze der Verhältnismäßigkeit und des geringsten Schadens bildeten den Kern, und die Verantwortlichen hatten nachzuweisen, dass Überwachung notwendig ist, um größeren öffentlichen Schaden abzuwenden. Außerdem war wichtig zeigen zu müssen, dass die nachrichtendienstlichen Erkenntnisse nicht durch weniger eingreifende Mittel erlangt werden konnten. Auch die Rechte der Agenten selbst erhielten erstmals die dringend nötige Aufmerksamkeit.

Noch wichtiger war, dass das RIPA einen Paradigmenwechsel förderte. Neben den Rechtsvorschriften, die den Nachrichtendiensten und Sicherheitsbehörden Rechtspersönlichkeit und Grundlagen gaben, hat es die Einstellungen der verantwortlichen Leiter verändert. Am 31. Oktober 2001 besuchten Abgeordnete, die zum Sonderausschuss des britischen Innenministeriums gehörten, das MI5-Hauptquartier im Thames House, um die Entwürfe neuer Antiterrorgesetze zu erörtern. Empfangen wurden sie von Stephen Lander, MI5-Generaldirektor, der sie mit seiner profunden Kenntnis der einschlägigen rechtlichen Grundlagen überraschte. Der Ausschusssekretär hielt fest: „Hätten man sich je träumen lassen, einem Generaldirektor des Sicherheitsdienstes zuzuhören, wie er mit Artikeln der Europäischen Charta der Menschenrechte förmlich um sich warf?“ (Mullin 2003, 234).

Wie wir gesehen haben, wurde mit dem RIPA auch ein „Gericht für die Geheimdienstaufsicht“ *(Investigatory Powers Tribunal,* IPT) geschaffen, das das *Security Service Tribunal,* das *Intelligence Services Tribunal* und das *Interception Tribunal* (eingerichtet zwischen 1985 und 1994 eingerichtet) ablöste. Das IPT ist zwar ein beachtenswertes nicht-öffentliches Gremium, dessen Aktivitäten schwer zu verfolgen sind, doch ist es potent und besitzt die Macht, Anordnungsersuchen abzulehnen, Daten zu vernichten und Entschädigungen zu gewähren. Wichtig ist hierbei, dass das Gericht gemäß Artikel 7 des *Human Rights Act* von 1998 eingebrachte Klagen gegen einen Nachrichtendienst verhandeln kann. Dieses Gesetz kann die Dienste auch einschränken, doch ist die mangelnde Transparenz des IPT hinsichtlich seiner Maßnahmen wiederum problematisch. Das IPT selbst hält die Wechselbeziehungen zwischen den verschiedenen Kreisen der einschlägigen Rechtsvorschriften für kompliziert; ihm zufolge sind sie für die Öffentlichkeit nahezu unverständlich.

Eine der wichtigen Erkenntnisse aus den Berichten der verschiedenen Ausschüsse war, wieviele Regierungseinrichtungen tatsächlich befugt waren, von verdeckter Überwachung Gebrauch zu machen. Dazu gehörten nicht nur die offenkundigen prätorischen Elemente, sondern alle Ministerien, Behörden und selbst die Kommunen. Der britische Ausschuss für Kommunikationsüberwachung berichtete 2008, dass nahezu 800 öffentliche Einrichtungen, darunter Organisationen des Nationalen Gesundheitsdienstes, jeden Tag durchschnittlich 1000 Anträge auf Kommunikationsüberwachung stellten, beispielsweise Abhören von Telefonen oder Abgreifen von Mobilfunkdaten, E-Mails oder Internet-Suchverläufe. Zu den befugten Institutionen gehören auch 474 Gemeinderäte, die in den letzten neun Monaten von 2006 rund 1700 Ersuchen um Zugriffe auf Mobilfunkdaten oder andere persönliche Daten stellten. Wenn also die EU den britischen Sicherheitsapparat in die neue Kultur der Regulierung eingeführt hat, dann war es das, was die oben beschriebenen Entwicklungen erleichterte (Garton Ash 2008).

Als Reaktion auf wiederholte Anfragen von Aktionsgruppen ließ das IPT im Februar 2015 eine Bombe platzen. Es urteilte, dass der GCHQ-Umgang mit von den NSA gewonnenen Erkenntnissen bis zum 5. Dezember 2014 gesetzwidrig war. An diesem Tag also hatte ein britisches Gericht erstmals gegen umfassende Aktivitäten eines der britischen Geheimdienste entschieden. Dies bedeutete für das GCHQ eine völlig andere Lage, hatte es doch nachdrücklich die „Gesetzmäßigkeit“ seiner Maßnahmen seit den 1990er Jahren betont. Dadurch, dass das Programm öffentlich bekannt war und dass es formal bestätigt wurde, erwies es sich nun als rechtmäßig. Die entscheidende Frage lautet hier: Wieviele Informationen über die Praktiken des GCHQ müssen verfügbar sein, um Bürgern ein schlüssiges System für Rechtsbehelfe zu ermöglichen – wie vom Europäischen Gerichtshof verlangt? Das IPT-Urteil gibt das allgemeinere Paradoxon der Berichtspflicht für Nachrichtendienste ganz gut wider, indem es betont, dass ein geheimes System der Überwachung eigentlich nicht geheim sein kann – und deshalb in seinen Umrissen öffentlich bekannt sein muss.

Die Aktionsgruppen halten sich mit Feiern der IPT-Feststellungen von Februar 2015 zurück. Das Urteil bedeutet nicht, dass die schlimmsten Vorwürfe der Snowden-Enthüllungen, etwa die maßlose Massenüberwachung, auf die Regierung zutreffen. Das IPT war sogar bemüht zu erklären, dass das Gegenteil der Fall ist: Die Überwachungsbefugnisse werden nur gegen jene geltend gemacht, die offenbar die Sicherheit Großbritanniens bedrohen. Allerdings liegt die Definition einer Bedrohung bei der Regierungsseite.

9.4 Die Rolle von Kampagnenorganisationen und Aktivisten

Zahlreiche Aktionsgruppen in Großbritannien neigen dazu, die massenhafte und „totale“ Überwachung durch NSA und GCHQ in den Vordergrund zu rücken. Wenig überraschend: Die Regierung tendiert dazu, dieser Behauptung zu widersprechen, und setzt dem entgegen, nur „massenhaften Zugriff“ zu verlangen. Die Frage, ob Maßnahmen durch einen Algorithmus oder durch Personen zur „Überwachung“ werden, hat sich insbesondere als philosophisches Problem erwiesen. Es unterstreicht ferner die Probleme der Definition und des technischen Verständnisses eines sich rasch wandelnden Bereichs.

Die meisten größeren Aktionsgruppen haben juristische Teams aus erfahrenen Menschenrechtsanwälten aufgebaut. Sie stimmen allgemein darin überein, dass die

Verteidigung von Freiheitsrechten in diesem Bereich vor allem durch eine sinnvolle Reform des RIPA realisiert würde, in Verbindung mit der konsequenten Durchsetzung seiner Regelungen und Einschränkungen, und nicht durch die Verbesserung der parlamentarischen Kontrolle. Konsens herrscht ferner darin, dass die Unterscheidung zwischen Inhalt und Verbindungsdaten einer gründlicheren Klärung bedarf. Verbindungsdaten, die nach dem RIPA weniger geschützt sind als Inhalte, umfassen heute z. B. aufgerufene Internetseiten, Adressenlisten der sozialen Medien und zahlreiche andere signifikante Merkmale der Online-Identität eines Bürgers. Meist wird behauptet, Großbritannien brauche hier eine Gesetzesänderung, um in diesem Bereich besseren Schutz zu gewähren. Auch Globalisierung ist ein problematischer Punkt, sodass die Unterscheidung zwischen interner und externer Kommunikation zu berücksichtigen ist.

Man hat überraschend geringes Interesse an den europäischen Entwicklungen gezeigt, etwa am langerwarteten „Safe Harbour"-Urteil des EGMR. Die meisten britischen Gruppen sind sich einig, dass ein besserer Schutz im Bereich der Massendaten nötig ist, wozu auch das Gebiet der Übermittlung von Daten an Drittstaaten gehört; doch betrachten sie dies eher als nationales, weniger als regionales Problem. Derzeit liegt dies weitgehend im Ermessen von Ministern; es wird darauf gedrungen, dass RIPA dahingehend zu ändern, dass es Artikel 8 der EMRK und sogar Artikel 10 zur Meinungsfreiheit stärker berücksichtigt. Im Grunde scheinen Gesetze über Spionage und Staatsgeheimnisse, die derzeit verbieten, dass Verdächtige ihre Aufgabe vor Gericht darlegen, zunehmend im Widerspruch zu Artikel 10 zu stehen. Eine Regierung wird sich Veränderungen hier wohl entgegenstellen und eher Transparenz von ihren Bürgern und nicht für sich fordern. So oder so werden wir wohl noch mehr und umfassendere Enthüllungen ebenso wie noch mehr technisch versierte Snowdens erleben.

Liberty, eine der bedeutendsten britischen Bürgerrechtsorganisationen, hat sich ebenfalls der Reform des RIPA-Überwachungsregimes gewidmet und zeigt sich besonders darüber beunruhigt, dass seine Bestimmungen durch den Austausch mit ausländischen Diensten umgangen werden. Sie stellt richtig fest: Dass diese Dinge nur durch die Snowden-Enthüllungen zutage kamen, lässt erhebliche Bedenken hinsichtlich der Effektivität von Kontrollmechanismen und Untersuchungsgremien wie IRTL und IPT aufkommen. Des Weiteren müsse der rechtliche Rahmen für die Überwachung überarbeitet werden, um Unterschiede in der Art der Daten zu berücksichtigen und die Einzelfall- statt der massenhaften Überwachung zu betonen. Es müsse ein System geben, dass zusätzliche transparente Vereinbarungen für den Informationsaustausch zwischen den Sicherheitsbehörden ermöglicht, die verhindern, dass Schutzbestimmungen von den Diensten listenreich umgangen werden. Auch richterliche Genehmigungen statt ministerieller Anordnungen hält *Liberty* für zentral (Ogilvie & Sankey, 2014).

Kurz gesagt teilen die wichtigsten Aktionsgruppen für den Schutz der Privatsphäre einerseits und der IRTL andererseits eine relativ breite gemeinsame Grundlage. Aber jenseits der Aktionsgruppen gibt es weitere Bereiche des digitalen Aktivismus. Bislang wurden diese Randgruppen von den Medien und der Wissenschaft meist nicht weiter beachtet. Aber wahrscheinlich werden wir in den nächsten zehn Jahren einen routinemäßigen digitalen Aktivismus erleben. Wenn der den Staat beobachtende Bürger, der „umgekehrte Blick", sich in den letzten zehn Jahren als normal etabliert hat, dann ist der DIY-Cyberkrieg vielleicht die nächste Phase? Aller Wahrscheinlichkeit nach wird sich die bereits schärfere Auseinandersetzung in digitalen Netzen soweit intensivieren, dass digitaler Aktivismus und Cyberkrieg miteinander zu verschmelzen beginnen. Ein interessantes Phänomen dabei ist, dass die Verbreitung entsprechender Technologien dem einzelnen Bürger und Protestler ermöglicht,

das Morgen zu planen (Karatzogianni 2014).

10. Fazit und Empfehlungen

10.1 Von „Sicherheit schaffen" zu „Sicherheit organisieren"

Regierungen müssen zehn Jahre vorausblicken. Wir steuern in eine neue Situation, in der wir die gesellschaftlichen Implikationen der wissensintensiven Sicherheit durchdenken müssen. Vieles in der Dynamik der Snowden-Affäre verdankt sich der Erkenntnis, dass Geheimdienstarbeit nicht mehr nur zur Domäne der Nachrichtendienste gehört, sondern dass hier auch privatwirtschaftliche Anbieter – zuweilen selbst multinationale Unternehmen – eine Rolle spielen. Künftig werden große Datensätze von kleinen Gruppen oder gar Einzelnen analysiert. Die Staaten werden Sicherheit in der digitalen Welt nicht mehr „herstellen", sondern nur noch koordinieren und „kuratieren" (Hall & Zarro 2012).

10.2 Sich rüsten für eine transparentere Gesellschaft

Im Zeitalter allgegenwärtiger Daten und Datensammlung müssen wir uns auf eine Gesellschaft einstellen, in der die Menschen weniger Privatsphäre haben, Unternehmen ihre Geschäftsgeheimnisse weniger schützen können und Regierungen ihrer Möglichkeiten der Geheimhaltung weitgehend beraubt sind. Die Herausforderung besteht darin, dafür Sorge zu tragen, dass wissensintensive Sicherheit eine offenere, wohlhabende und nachhaltige Gesellschaft fördert. Transparenz birgt eigene Probleme, aber wir werden die Uhr wohl nicht mehr zurückdrehen können. Stattdessen müssen wir dafür sorgen, dass unsere Daten in der Breite und demokratisch genutzt werden. Wir müssen gründlich über die wachsende Bedeutung der Unternehmen und ihre Konsequenzen für die demokratische Kontrolle der Sicherheit nachdenken. Ein Ende weitverbreiteter Bespitzelung ist wohl unwahrscheinlich, hingegen brauchen wir viel bessere Kontrolle und Regulierung, um das Vertrauen der Öffentlichkeit zu erhalten.

10.3 Autoritäre Staaten und Kriminelle

Aktionsgruppen sind der Auffassung, dass personenbezogene Daten nur zum Schutz der nationalen Sicherheit gesammelt werden dürfen – mit Zustimmung der Betroffenen oder durch Antrag auf eine gerichtliche Anordnung auf der Grundlage eines Anfangsverdachts. Nur haben die Snowden-Enthüllungen ein Spionage-Wettrüsten ausgelöst; viele Länder, die bisher keine Systeme wie „Tempora" und „Prism" hatten, beschaffen sie nun. Paradoxerweise hatten Snowdens Enthüllungen den unbeabsichtigten Effekt, das Ausmaß der Ausspähung von Bürgern weltweit zu vergrößern. Bemühungen, den Export von Überwachungstechnologie an autoritäre Regime zu verhindern, sind so gut wie gescheitert. Analysetechnik wird heute weiterverbreitet, das Ausspähen, auch noch in größerem Maßstab, wird billiger und leichter. Bürger werden sich zunehmend an ihre Sicherheitsbehörden wenden, um besser gegen die heimtückischsten dieser

Aktivitäten oder gegen Computerkriminalität geschützt zu werden.

10.4 Verbesserte Kontrolle und informelle Aufsicht

Auf kurze Sicht braucht Großbritannien viel bessere juristische Kontrollmechanismen, bei denen Anordnungen durch Gerichte, nicht durch Minister genehmigt werden, und idealerweise braucht es auch einen Generalinspekteur. Dies würde die glanzlose Leistung des ISC ausgleichen. Die begrenzten Veränderungen bei ministeriellen Anordnungen, wie vom ISC vorgeschlagen, bieten kaum besseren Schutz. Am strittigsten ist wohl das Thema schwindender Geheimhaltung: Die Regierung wird es ablehnen, Whistleblowern, die gesetzwidrige Überwachungsaktivitäten aufdecken, glaubwürdigen, wirksamen Schutz zu gewähren. Natürlich ist die „Regulierung durch Enthüllung" ein unsicheres Geschäft mit oft unbeabsichtigten Folgen. Die effizienteste Maßnahme für die EU zur Verbesserung der Kontrolle wäre, für mehr rechtliche Sicherheit in diesem Bereich zu sorgen, doch werden nationale Regierungen versuchen, Vorbehalte geltend zu machen, ähnlich jenen in den USA, die Fragen der nationalen Sicherheit vom Whistleblower-Schutz trennen.

10.5 Internationale Kontrolle

Eine der größten Herausforderungen bildet der länderübergreifende Informationsaustausch zwischen Nachrichtendiensten sowie auf multinationaler Grundlage durchgeführte Geheimdienstoperationen. Dies zu untersuchen halten nationale Ausschüsse für besonders schwer. Für dieses schwierige Problem wäre ein Generalinspekteur mit multinationalem Auftrag die beste Lösung. Auch dies wird bei den Regierungen auf Ablehnung stoßen; sie werden sich jedoch damit auseinandersetzen müssen, dass sich, sofern sie keine effektive multinationale Kontrolle gewährleisten, Menschenrechtsanwälte, Medien und internationale Gerichte – oft in Kooperation –, statt ihrer munter damit befassen.

10.6 Ende-zu-Ende-Verschlüsselung („E2EE")

Auf lange Sicht werden wir wahrscheinlich lebhafte technologische Anstrengungen der Wissenschaftsgemeinde erleben, die Überwachung zurückzudrängen. Internetanbieter und Dotcoms sind insbesondere über das Verhalten der NSA verärgert. Eine neue Generation von Kryptographen widmet sich heute der Aufgabe, die Ende-zu-Ende-Verschlüsselung („E2EE") voranzubringen. Die Clipper-Chip-Affäre lässt vermuten, dass Regierungen diese Entwicklung wohl kaum werden aufhalten können. Der britische Premierminister David Cameron verlangt von allen Diensten, die eine solche Verschlüsselung verwenden, der Regierung, den Nachrichtendiensten und den Vollzugsorganen Hintertüren zu öffnen, die ihnen eine Kommunikationsüberwachung ermöglichen. Tatsächlich haben wir eher einen begrenzteren Zugang zu Verbindungsinhalten und einen erweiterten Zugriff auf Verbindungs- und Geo-Positionsdaten zu erwarten. Historisch gesehen werden die Parameter der Informationsbeschaffung eher von der Technologie als von Gesetz oder Politik bestimmt. Man vermutet, dass dies die Richtung ist, in die uns die Technologie in den nächsten zehn Jahren führt. Vielleicht wird eine Situation, wo Metadaten in größerem Umfang verfügbar sind, auf Inhalte aber schwerer zuzugreifen ist, einen unsicheren Waffenstillstand in den zunehmenden Auseinandersetzungen um Privatsphäre und Geheimhaltung bringen.