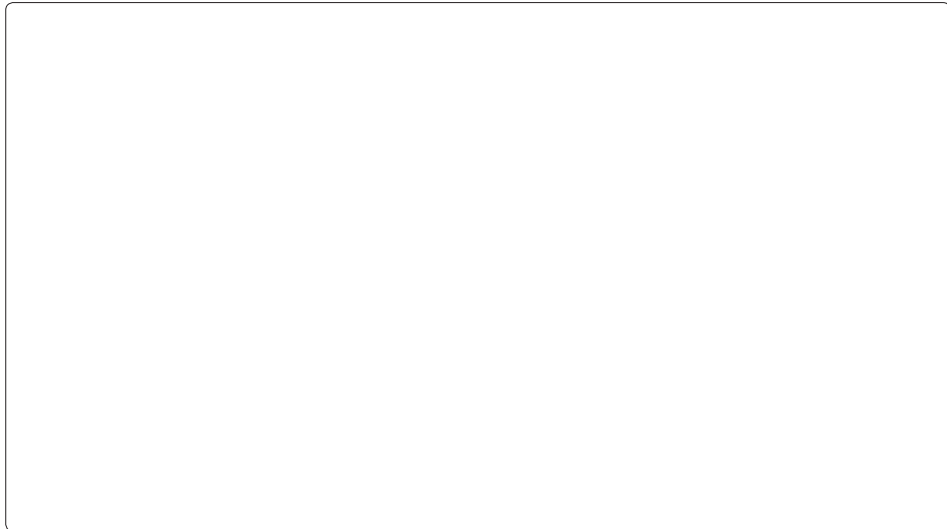




Schriftenreihe  
Forschungsforum Öffentliche Sicherheit





# **Die gesellschaftliche Konstruktion von Sicherheit**

Zur medialen Vermittlung und Wahrnehmung der  
Terrorismusbekämpfung

Susanne Krasmann, Reinhard Kreissl,  
Sylvia Kühne, Bettina Paul, Christina Schlepper





Forschungsforum Öffentliche Sicherheit

Hrsg: Jochen Schiller, Lars Gerhold, Saskia Steiger, Helga Jäckel

Schriftenreihe Sicherheit Nr. 13, März 2014

print: 978-3-944675-02-2 online: 978-3-944675-03-9

Anschrift:

---

Freie Universität Berlin

Tel: +49 (0)30 838 57367

Carl-Heinrich-Becker Weg 6-10

Fax: +49 (0)30 838 4 57367

12165 Berlin

[www.schriftenreihe-sicherheit.de](http://www.schriftenreihe-sicherheit.de)

[kontakt@schriftenreihe-sicherheit.de](mailto:kontakt@schriftenreihe-sicherheit.de)

---

Über die Autoren:

Prof. Dr. Susanne Krasmann ist Professorin für Soziologie am Institut für Kriminologische Sozialforschung, Fachbereich Sozialwissenschaften der Universität Hamburg, und Vorsitzende des ISIP e.V. Arbeitsschwerpunkte: Critical Security Studies; Recht und Staatlichkeit; Wissenssoziologie; Sozialtheorie.

PD Dr. Reinhard Kreissl ist Mitarbeiter am Institut für Rechts- und Kriminalsoziologie in Wien. Arbeitsschwerpunkte: Soziologie sozialer Kontrolle, Kriminologie, Rechtssoziologie.

Sylvia Kühne ist wissenschaftliche Mitarbeiterin am Institut für Kriminologische Sozialforschung der Universität Hamburg im von der Deutschen Forschungsgemeinschaft geförderten Projekt „Biometrie als ‚soft surveillance‘. Die Akzeptanz von Fingerabdrücken im Alltag“.

Dr. Bettina Paul ist wissenschaftliche Mitarbeiterin am Institut für Kriminologische Sozialforschung der Universität Hamburg und Vorsitzende des ISIP e.V. Sie leitet das BMBF Projekt „Gesellschaftliche und wirtschaftliche Auswirkungen neuer Sicherheitsmaßnahmen im Fährverkehr“ (Teilprojekt von VESPER+). Arbeitsschwerpunkte: Drogentests, Maritime Sicherheit, visuelle Wissenssoziologie

Christina Schlepper ist Geschäftsführerin des Instituts für Sicherheits- und Präventionsforschung und wissenschaftliche Mitarbeiterin am Institut für Kriminologische Sozialforschung der Universität Hamburg im vom Bundesministerium für Bildung und Forschung geförderten Projekt „Gesellschaftliche und wirtschaftliche Auswirkungen neuer Sicherheitsmaßnahmen im Fährverkehr“.

Kontakt zu den Autoren:

---

Institut für Sicherheits- und Präventionsforschung

Bogenallee 11

20144 Hamburg

[isip@uni-hamburg.de](mailto:isip@uni-hamburg.de)





## Inhaltsverzeichnis

1. Sicherheit als modernes Problem .....	9
1.1    Krise der Sicherheit .....	9
1.2    Risiken, Katastrophen und das Konzept der zivilen Sicherheit .....	14
1.3    Sicherheit expandiert: Über die Vervielfältigung des Möglichen.....	22
1.4    Ethik der Sicherheit.....	26
2.    Bedrohungs- und Risikowahrnehmungen in der Bevölkerung.....	31
2.1    Methodische Herangehensweisen .....	32
2.2    Zentrale Ergebnisse zur Bedrohungs- und Risikowahrnehmung.....	33
2.2.1    Allgemeine Bedrohungswahrnehmung terroristischer Anschläge .....	33
2.2.2    Persönliche Bedrohungswahrnehmung terroristischer Anschläge .....	39
2.2.3    Risikowahrnehmung terroristischer Anschläge.....	40
2.3    Kritik und methodische Probleme.....	45
3.    Die mediale Vermittlung von Unsicherheit .....	49
3.1    Konstruktionen der Bedrohung und die Rolle der Medien .....	50
3.2    Mediale Darstellungen von terroristischen Bedrohungen.....	52
3.3    Mediale Rezeption von terroristischen Bedrohungen .....	56
3.4    Perspektiven der Medienanalyse.....	57
4.    Sicherheit im Fluchtpunkt von 9/11.....	63
4.1    Sicherheitspolitik und Terrorismus .....	63
4.1.1    Ausdehnung der Vorfeldkriminalisierung.....	64
4.1.2    Institutionelle Aufrüstung und Vernetzung der Sicherheitsbehörden .....	65
4.1.3    Einführung von neuen und Erweiterung von bestehenden Befugnissen ..	66
4.1.3.1    Erfassung von Bankdaten.....	67
4.1.3.2    Erfassung des Reiseverhaltens .....	68



4.1.3.3	Erfassung des Kommunikationsverhaltens und deren Inhalte .....	69
4.1.3.4	Erfassung von „Terrorverdächtigen“ .....	72
4.2	Akzeptanz von Sicherheitsmaßnahmen .....	79
4.2.1	Zentrale Ergebnisse zu Bewertungen einzelner Sicherheitsmaßnahmen .	80
4.2.1.1	Akzeptanz des Zugriffs auf Bankdaten .....	81
4.2.1.2	Akzeptanz der Kontrolle des Reiseverhaltens.....	83
4.2.1.3	Akzeptanz der Registrierung des Kommunikationsverhaltens .....	84
4.2.1.4	Akzeptanz von Datenbanken und Listen.....	85
4.2.1.5	Akzeptanz weiterer Maßnahmen.....	86
4.2.2	Zentrale Ergebnisse zu Bedingungen und Grenzen der Akzeptanz .....	90
4.2.2.1	Bedrohungswahrnehmungen und Sicherheitserwartungen .....	90
4.2.2.2	Sicherheitsräume, (un)normale Kontrolle und die Situation ‚selbst‘	91
4.2.2.3	(Un-)Sichtbare Kontrolle .....	95
4.2.2.4	Was kostet die Freiheit? Akzeptanz zwischen (fehlendem) Widerstand und positiver Bewertung.....	96
4.2.3	Kritik und methodische Probleme .....	101
5.	Akzeptanz und Vertrauen .....	105
5.1	Vertrauen im Schnittfeld von Sicherheit und Freiheit .....	105
5.2	Institutionalisierung von Misstrauen seit 9/11 .....	107
5.2.1	Vertrauensverluste der Bürger in sich selbst.....	109
5.2.2	Vertrauensverluste der Bürger in ihre Mitmenschen.....	110
5.2.3	Vertrauensverluste der Bürger in den Staat.....	111
5.3	Sicherheitsmaßnahmen und das Vertrauen der Bürger .....	112
6.	Zusammenfassung und Empfehlungen.....	119
	Literatur.....	123
	Quellen.....	147



## Tabellenverzeichnis

Tabelle 1: Beispielfragen zur Erhebung der Bedrohungs- und Risikowahrnehmung..	33
Tabelle 2: Eurobarometer Survey 2011 zur Sicherheitslage.....	44
Tabelle 3: Abrufe von Bankkontodaten durch verschiedene Behörden 2004 bis 2012	67
Tabelle 4: Wie bewerten die Bürger die folgenden Kontroll- und Überwachungstechnologien? .....	81
Tabelle 5: Zustimmung und Ablehnung der folgenden sicherheitspolitischen Maßnahmen durch den Bürger: .....	82
Tabelle 6: Häufigkeiten praktizierter und intendierter Schutzmaßnahmen der Bürger gegen Kontroll- und Überwachungstechnologien.....	98
Tabelle 7: Empfinden von Kontrollverlusten.....	100
Tabelle 8: Häufigkeiten der Antworten auf die Frage nach dem „Vertrauen in die Regierung“ .....	113
Tabelle 9: Glaube an einen vertrauenswürdigen Umgang mit Daten durch die Behörden .....	114
Tabelle 10: Glaube an einen vertrauenswürdigen Umgang mit erhobenen Daten durch nicht-staatliche Institutionen .....	116





## Abbildungsverzeichnis

Abbildung 1: Entwicklung der Angst vor terroristischen Anschlägen von 1996 bis 2011 .....	34
Abbildung 2: Vergleich R+V- und ISIP-Befragung 2009 – Häufigkeit der Antworten auf die Frage nach „großer Angst“ .....	35
Abbildung 3: Vergleich R+V- und MPI-Befragung 2012 – Häufigkeit der Antworten auf die Frage nach „großen Sorgen“ .....	36
Abbildung 4: Perzipierte Anschlagswahrscheinlichkeit auf verschiedene Verkehrsmittel .....	41
Abbildung 5: Wichtigkeit von Maßnahmen für das Sicherheitsempfinden im Fährverkehr .....	87
Abbildung 6: Maßnahmen mit hoher Sicherheitszuschreibung im Fährverkehr bei Gefahrenstufe 2 .....	88
Abbildung 7: Sicherheitszuschreibungen und Belästigungsgefühl bei Maßnahmen im Fährverkehr .....	93



# 1. Sicherheit als modernes Problem

## 1.1 Krise der Sicherheit

Sicherheit ist in der Krise. Diese Beobachtung legen die sozialwissenschaftlichen Diskussionen nahe, die gegenwärtig um ein neues Verständnis von Sicherheit ringen. Denn als krisenhaft lässt sich die Wahrnehmung einer „anhaltenden Neuheit“ bestimmen, die aber noch im Übergang ist (Koselleck 1982, S. 648). Krisen gehen mit Unruhe oder Verunsicherungen einher, weil das Alte so nicht mehr gilt, das Neue aber noch nicht gefunden ist. Krisen bezeichnen insofern einen Zwischenzustand, der um Sinngebung ringt und darin gleichermaßen „anschlußfähig wie anschlußbedürftig, sinnpräzisierend aber auch sinnsuchend“ ist (ebd., S. 649).

Die Krise der Sicherheit äußert sich zunächst einmal in der Wahrnehmung einer Diskrepanz zwischen immer mehr Sicherheitsambitionen einerseits, die andererseits aber eben dieses Versprechen, (mehr) Sicherheit zu bieten, nicht einlösen können. Sie sorgen eher im Gegenteil für mehr Verunsicherung oder neue Formen der Einschränkung. Sicherheit, so etwa Christopher Daase, Philipp Offermann und Valentin Rauer (2012, S. 7) stellvertretend für viele<sup>1</sup>, sei zur „neuen gesellschaftspolitischen Leitvokabel“ avanciert, während die Ideen der „Freiheit, Aufklärung und Emanzipation“ darunter an Bedeutung verloren hätten. Sicherheit, so auch die internationale Diskussion, müsse wieder eingehegt und „zivilisiert“, nämlich nicht nur als ein Vehikel für immer mehr staatliche Eingriffsbefugnisse, sondern vielmehr als ein elementares öffentliches Gut verstanden (Loader & Walker 2007), und grundsätzlich müssten Sicherheit und Menschenrechte miteinander „versöhnt“ werden (vgl. Goold & Lazarus 2007, S. 15; für die deutsche Diskussion etwa: von Arnim et al. 2002). Sicherheit, das deuten diese Argumente an, entfaltet offenbar sich selbst fortschreibende Mechanismen. Als „Wertidee“ (Kaufmann 2012) tendiert sie dazu, andere zentrale Prinzipien liberal-demokratisch verfasster Gesellschaften zu überlagern.

So sieht sich auch die Kriminologie von einer „Obsession“ mit Sicherheit dominiert (vgl. Zedner 2009, S. 1), die ihr Interventionsfeld rundheraus umschreibt. Generell ist hier nämlich eine Verschiebung von einer reaktiven zur proaktiven Ausrichtung zu beobachten. Probleme der Kriminalität werden weniger unter den Vorzeichen des Rechts in den Kategorien von Norm und Abweichung verhandelt und in Reaktion auf Straftaten (*post crime*) *behandelt*, vielmehr als Risiken und abstrakte Bedrohungen ins Visier genommen, die es in ihrem Niveau und ihrer Verteilung zu *regulieren* bzw. unter dem Vorzeichen der Sicherheit im Vorwege (*pre crime*) abzuwenden gilt

---

<sup>1</sup> Etwa: Conze (2005); Singelstein & Stolle (2006) für die bundesrepublikanische Situation; für einen internationalen Kontext: Garland (2008a).



(Zedner 2007). Kriminal- und Sicherheitspolitik verschmelzen zusehends und entwickeln in einem „Bekämpfungsrecht“ (Frankenberg 2005) erweiterte Eingriffsbefugnisse im Vorfeld von konkreten Gefahren, Straftaten oder auch einem qualifizierten Verdacht.

Als ein Katalysator der jüngsten Entwicklungen werden zu Recht vor allem die politischen Reaktionen auf den internationalen Terrorismus ausgemacht, die mit Beginn des 21. Jahrhunderts eine Reihe neuer Sicherheitsgesetze und Eingriffsermächtigungen freigesetzt haben. Das traditionell liberale Verständnis rechtsstaatlicher Intervention, die eher restriktiv auf die Gefahrenabwehr geeicht ist, hat sich unterdessen, so die Kritik, auf eine „präventionsstaatliche“ Ausrichtung auf den Gefahrenvorgriff hin verlagert (Huster & Rudolph 2008). Darin lässt sich allerdings auch eine kontinuierliche Entwicklung erkennen, die im Rückblick nur von je spezifischen Krisenphänomenen wie den politischen (nationaler Terrorismus), wirtschaftlichen und ökologischen Krisenerfahrungen der 1970er und 1980er Jahre sowie neuen grenzüberschreitenden Herausforderungen seit den 1990er Jahren befördert wurde. Neue Bedrohungslagen wurden so skizziert („Organisierte Kriminalität“, „Illegale Migration“), neue Bereiche des Strafrechts entdeckt (z.B. Umwelt), aber auch andere Kategorien der Beschreibung dominant (z.B. Risiken) sowie neue Technologien (Verfahren, Techniken und Praktiken der Kontrolle und Überwachung) entwickelt.

Sicherheit, so die einhellige Beobachtung, deutet schon längst nicht mehr nur auf das Feld der klassischen „Staatsaufgabe“ (Grimm 1996) im Sinne des Schutzes vor „inneren“ und „äußeren“ An- und Übergriffen hin. Sie ist nicht mehr nur polizeiliche und militärische Aufgabe, aber auch nicht sozialpolitisch im Sinne der Herstellung von „sozialer Sicherheit“ konnotiert. Der „erweiterte Sicherheitsbegriff“ (Daase 2009), der sich in den vergangenen Jahrzehnten durchgesetzt hat, erstreckt sich auf die vielfältigsten Problembereiche und Interventionsfelder von der Umwelt bis hin zur „menschlichen Sicherheit“ (Human Security) und bringt dabei nicht nur neue staatliche Eingriffsbefugnisse, sondern auch neue Verpflichtungen hervor. Zugleich verschieben sich die Zuständigkeiten. Sicherheit, die zunehmend zu einer inter- und supranationalen Angelegenheit wird, verändert die „Sicherheitsarchitektur“ (Würtenberger et al. 2012). Neue Sicherheitsbehörden entstehen und neue Kooperationen werden möglich. Zugleich diffundiert die Verantwortung für Sicherheit auf die Ebene kommunaler Einrichtungen bis hin zum individuellen Bürger. Dabei treten nicht nur neue Adressaten, sondern auch neue Akteure wie etwa private Sicherheitsanbieter und Nicht-Regierungsorganisationen auf den Plan (Daase & Deitelhoff 2013). Spiegelbildlich durchdringt Sicherheit auf diese Weise zunehmend unser Alltagsleben und prägt vor allem in der Wahrnehmung von Risiken das gesellschaftliche „Sicherheitsbewusstsein“ (Conze 2012, S. 454).



Auch die Forschung partizipiert an diesen Entwicklungen, und die Programme von EU und BMBF involvieren nicht nur die Sicherheitsindustrie, sondern auch die Sozialwissenschaften. Auch diese ist ein Medium der Deutung und Kommunikation von Sicherheitsfragen und ein Parasit. Sie gehört und gehört doch nicht dazu, sie akzeptiert die Bedingungen der Forschung und sucht sie doch zu unterlaufen und in eine andere Richtung zu bringen. So sind die bekannten Paradoxien der Sicherheit keineswegs nur technologischer Art, sondern vor allem soziale Phänomene: Sicherheitstechniken produzieren Risiken nicht nur im objektiven Sinne „nichtintendierte[r] Folgen und Nebenfolgen“ (Münkler 2010, S. 11; Beck 1986) oder einer höheren Verletzlichkeit und Anfälligkeit komplexer Systeme, als vielmehr selbstreflexiv, etwa wenn Sicherheitstechniken riskanteres Verhalten und in der Folge sogar mehr oder schwerere Unfälle provozieren; oder wenn Überwachungstechnologien nicht mehr Sicherheit, sondern auch Unsicherheit vermitteln; oder wenn Gesellschaften, die sich in Sicherheit und Wohlstand wähnen können, sich als umso verletzlicher erleben und noch höhere Sicherheitsstandards einfordern.

Sicherheit ist selbst eine Technologie der Steuerung menschlichen Verhaltens, und genau hier setzt auch der Beitrag sozialwissenschaftlicher Forschung ein. So liest sich der Aufstieg des Securitization-Ansatzes, der aus dem politikwissenschaftlichen Schwerpunkt der „Internationalen Beziehungen“ und ihrer Subdisziplin der (*Critical Security Studies*) hervorgegangen ist (Buzan et al. 1998; Balzacq 2011), gleichermaßen als Indikator wie Motor eines erweiterten Verständnisses von Prozessen der „Versicherheitlichung“, die nicht nur „top down“ von staatlichen Akteuren, sondern interaktionistisch auch „bottom up“ als Deutungs- und Konstruktionsprozesse von der Bevölkerung ausgehen. Politisch wie theoretisch ist Sicherheit zur Konstruktionsleistung geworden.

Nun zeigt sich das Krisenhafte im Feld der Sicherheit zuallererst darin, dass sich herkömmliche Deutungsmuster und Kategorien verschieben und diffundieren. Das betrifft elementare Unterscheidungen und Grenzbestimmungen, wie etwa die zwischen innerer und äußerer Sicherheit, polizeilichen und militärischen Belangen, die für das Denken einer modernen Sicherheitsordnung (von Trotha 2010) bestimmend sind und die nun tendenziell ununterscheidbar werden oder verschwimmen. Ein „erweiterter Sicherheitsbegriff“ wird dann einerseits zum Synonym dafür, dass mit den Unterscheidungen auch die rechtlich bestimmten Begrenzungen von Eingriffsbefugnissen erodieren und Sicherheit umso ungezügelter zum Vehikel von Kontroll- und Interventionsambitionen werden kann. Zugleich ist die begriffliche Diffusion Voraussetzung und Antrieb für die Durchsetzung neuer Sicherheitsordnungen, auch im globalen Kontext. Die aktuelle Diskussion um Drohneneinsätze ist hier exemplarisch. Denn Akzeptanz und Abwehr artikulieren sich abhängig von der Zielsetzung (humanitärer Einsatz, Aufklärung, Überwachung, Bekämpfung) und je nachdem, ob dabei ein polizeiliches



oder militärisches Vorgehen vorausgesetzt wird, während die Drohnentechnologie ihrerseits prinzipiell beides möglich erscheinen lässt und sich überdies auch für zivile Einsätze eignet (Kahn 2013; Krasmann 2012a). Andererseits ist Verunsicherung wesentlich davon mitbestimmt, dass wir Neues und Unbekanntes nicht einordnen, also nicht mit unseren Erwartungen und vertrauten Deutungssystemen in Einklang bringen können. Prozesse der Entdifferenzierung bis hin zur Ununterscheidbarkeit zentraler Kategorien einer politischen Ordnung sind deshalb, zumal im Feld der Sicherheit, nicht nur Indikatoren für eine Krise eben dieser Ordnung, sondern auch für eine Verunsicherung eben angesichts unzulänglicher Möglichkeiten der Unterscheidung und Identifizierung (Rauer 2012).

Sicherheit ist demnach in doppelter Hinsicht als ein spezifisches modernes Problem zu begreifen. Zum einen entwickelte sich unser heutiges Verständnis von Sicherheit erst mit der Entstehung des modernen Staates (Conze 1984), einschließlich seines spezifischen Begriffs von territorial und rechtlich gebundener Souveränität, den zugehörigen dichotomen Unterscheidungen wie innere und äußere Sicherheit, Friedens- und Kriegszeiten, sowie einer liberal-demokratischen Rechtstradition, die unter Sicherheit eben auch Rechtssicherheit versteht; die Sicherheit nicht ohne Freiheit denken will; und die nicht ohne Grund zögerlich darin ist, Sicherheit selbst als ein Grundrecht zu etablieren, das sich dann allzu leicht vor individuelle Freiheitsansprüche schiebt und letztlich die Ausdehnung staatlicher Eingriffsbefugnisse befördert (Lepsius 2004). Sicherheit war in diesem Sinne immer schon zu zivilisieren, und das gilt auch und gerade dann, wenn sie im Namen der Sicherung der Freiheit auftritt. Zum anderen verweist die Etymologie des Begriffs – lat. *securitas*: „ohne Sorge“, im weitesten Sinne frei von Furcht, Beunruhigung oder existenzieller Angst – in ihrer philosophischen Bedeutung und dem deutlich subjektiv-psychologischen Akzent (vgl. Conze 1984, S. 832) auf ein spezifisch modernes Denken und dessen Verhaftung im Möglichen – im temporalen wie im modalen Sinn – selbst hin.<sup>2</sup>

Wenn die Krisenwahrnehmung eines sich potenziell unendlich ausdehnenden Sicherheitsfeldes nunmehr von der Suche nach einer Neubestimmung getrieben ist, so lässt diese sich stellvertretend mit Wolfgang Bonß (2010, S. 58f.) auf den Begriff bringen. Wir sollten uns, so das Plädoyer, von der „Idee der Möglichkeit vollständiger

---

<sup>2</sup> Wie der Literaturwissenschaftler Burkhardt Wolf (2011, S. 19) herausgearbeitet hat, beinhaltet der Begriff der „Modernität“ gleichermaßen das Moment des Tempus wie des Modus. *Modernus* leitet sich aus dem Lateinischen *modo* ab: „eben noch, eben erst“, und bezeichnet damit gerade „jene Art Zwischenzustand, in dem sich [...] das Moderne präsentiert: als etwas, das sich eben noch aus dem Gegebenen und Gewissen herausgeschält und eben erst in das Künftige und Kommende eingeschrieben hat. [...] Zirkulär mit seiner jeweiligen Zukunft verknüpft, wird das Handeln und Entscheiden selbst kontingent. Hatte es eben noch zureichende Gründe, so müssen sich diese eben erst als solche erweisen. Weniger vor einer bestimmten Wirklichkeit, als vielmehr gegenüber jenen Möglichkeiten hat sich also Modernität zu bewähren.“



Sicherheit“ verabschieden und stattdessen „eine ‚neue Kultur der Unsicherheit‘“ gegenwärtigen. Während noch ungewiss ist, wie eine solche Kultur überhaupt zu gestalten wäre, ist die Unsicherheit selbst uns nunmehr offenbar „sicher“ (ebd., S. 59).

Im doppelten Sinne erweist diese Vision einem modernen Denken ihre Referenz, denn die Vorstellung gesellschaftlicher Steuerbarkeit ist diesem ja ebenso eingeschrieben wie die Selbstreflexivität – als Fähigkeit und Praxis, „das Denken zu denken“ (Horkheimer & Adorno 1971, S. 26). Modernität beinhaltet die Idee der Machbarkeit und Beherrschbarkeit (Kaufmann 2003) – einschließlich der Idee, „vollständige Sicherheit“ überhaupt herstellen zu können – ebenso wie deren Kritik – einschließlich der Forderung, uns von eben dieser Machbarkeitsvorstellung zu verabschieden. Es beinhaltet ferner die Vorstellung einer eindeutigen Ordnung und ihrer Begründung (Bauman 1992) – einschließlich der Vorstellung, eindeutig Grenzen ziehen zu können etwa zwischen Friedens- und Kriegszeiten, militärischen und polizeilichen Aktionen – ebenso wie die Reflexion auf die Kontingenz der Ordnungen und die Brüchigkeit jeder Sinnstiftung (Stäheli 2000) – einschließlich der Gegenwärtigung, dass der moderne Rechtsstaat eher ein Ideal denn eine Realität ist: eine „hilfreiche Fiktion“ (von Trotha 2002, S. 354), die als solche allerdings zugleich Voraussetzung der Realisierung von Rechtsstaatlichkeit ist (Simon 2008).

Die Moderne beschreibt sich, noch einmal mit Bonß (2010, S. 33), buchstäblich wie im übertragenen Sinne als die gesellschaftliche Erfahrung und Fähigkeit der „Entdeckung neuer Welten“, wie sie insbesondere für das 17. Jahrhundert prägend war und die zugleich notwendig mit der „Zerstörung alter Sicherheiten“ und Gewissheiten einhergehen musste. Im Kern steht das moderne Denken für die Entbindung des Menschen aus einer ihm übergeordneten Ordnung. Der Mensch, wie es Michel Foucault (1974) in der *Ordnung der Dinge* beschreibt, taucht gleichsam auf als Erkennender und Schöpfer seiner eigenen Welt, für die er folglich selbst verantwortlich zeichnet, ohne indes je ihr Souverän zu werden oder sie je vollständig erfassen zu können. So erkennt der Mensch sich als Autor seiner Sprache, die ihm doch stets vorgängig bleibt, als Macher seiner Geschichte, die sich ihm doch immer wieder entzieht, oder als Entdecker der Gesellschaft, die im selben Moment ihr Eigenleben ausweist. Die Moderne zeugt von der Situiertheit des Menschen in seiner eigenen Geschichte, und Sicherheit ist die komplementäre Problematisierung dieser Entbindung des Menschen und seiner Erfahrung der Kontingenz.

Die Krise der Sicherheit verweist insofern nicht auf eine „objektive“ Zunahme von Unsicherheiten, sie muss im Effekt auch nicht einmal eine gesteigerte Verunsicherung bedeuten. Sie ist vielmehr zuallererst Ausdruck einer Krise des modernen Selbstverständnisses der Machbarkeit wie Zeugnis einer Selbstreflexivität, die sich erneut in ihrer eigenen Begrenztheit erkennt und darin allerdings vielleicht gewahr wird, dass Nichtbeherrschbarkeit nicht die Ausnahme, sondern der Normalfall ist. Die Krise der



Sicherheit weist uns daher zunächst einmal auf uns selbst zurück, und genau hierin liegt vielleicht eine vornehmliche Herausforderung für die sozialwissenschaftliche Analyse, nämlich herauszuarbeiten, wie Gesellschaften nicht nur mit Unsicherheit und Ungewissheiten umgehen, sondern wie sie sich über die Problematisierung derselben auch selbst beschreiben und konstituieren.

Dabei bringt die *Regierung* der Sicherheit (Foucault 2004), die stets auch ein Kontrolldiskurs ist, bestimmte Formen der Subjektivierung hervor. Dies nicht nur weil die Rede von der Sicherheit stets auch ihr Gegenteil, die Unsicherheit, evoziert und insofern unsere Wahrnehmung und unser Verhältnis zur Welt prägt. Vielmehr ist die Regierung der Sicherheit selbst eine Praxis, die an bestimmte Techniken und Verfahren gebunden ist. Die „Konstruktion“ von Sicherheit reduziert sich demnach nicht auf Deutungsprozesse und sie vollzieht sich nicht nur in der sozialen Interaktion. Das Verhältnis zwischen Bürger und Staat gestaltet sich vielmehr selbst im Medium von Technologien, die auf bestimmten Formen des Wissens beruhen und ihrerseits Gegenstands- und Interventionsfelder produzieren. Zu untersuchen wäre demnach zuallererst genau dies, wie sich ein Feld der Kontrolle und Intervention unter dem Vorzeichen von Sicherheit konstituiert, das die Subjekte und Objekte des Regierens in je bestimmter Weise zuschneidet und konfiguriert und aus den Bürgern zum Beispiel Datenträger, gefährliche Objekte oder auch zivilgesellschaftliche Akteure macht. Neue Konzepte der Bewältigung von Problemen der Sicherheit, die wir erfinden, zeugen in diesem Sinne weniger von einer neuartigen „Natur“ der Bedrohung, sie sind vielmehr zuallererst Epiphänomene der Organisation unseres sozialen Lebens selbst. Und der Zugschnitt der „Staatsaufgaben“ und -befugnisse wäre dann nicht nur im Verhältnis zur gesellschaftlichen Ordnung und ihren Werten auszuloten (vgl. Grimm 1996, S. 10), sondern auch als eine Frage des techno-politischen Arrangements zu lesen.

## 1.2 Risiken, Katastrophen und das Konzept der zivilen Sicherheit

In der Sicherheitsforschung ist das Erdbeben von Lissabon im Jahr 1755 emblematisch für die Wende zur Moderne (so auch Felgentreff et al. 2012). Denn die Katastrophe in Verbindung von Erdbeben, Großbrand und Tsunami führte damals nicht nur zur weitgehenden Zerstörung der portugiesischen Hauptstadt. Sie erschütterte vielmehr auch nachhaltig die Vorstellung von einer gottgegebenen Ordnung. Für das Desaster konnte niemand verantwortlich gemacht werden, es ließ sich aber auch kaum befriedigend als Schicksalsschlag oder bloßer Zufall erklären und mündete schließlich in die Einsicht, dass man „sein Schicksal selbst in die Hand nehmen musste“ (Nassehi 2012, S. 35). Die „aufgeklärte Gesellschaft“ entwickelte wissenschaftliche Zugänge, in Reaktion auf die Katastrophe von Lissabon insbesondere die moderne Seismologie. Wenn die Verknüpfung von Bevölkerungsstatistik und Wahrscheinlichkeitsrechnung dabei die



Voraussetzung für die Etablierung von Risikotechnologien bildete, so veränderten diese die Wahrnehmung und Zuschreibung von Unglücksfällen völlig. Gegenüber dem schicksalhaften Ereignis und der Schuld, die an die Sünde geknüpft ist, kommt nun *das soziale Verhältnis* in den Blick. Der Unfall wird zum Inbegriff einer Normalisierung von Unglücksfällen, die zuallererst darauf verweisen, „dass wir in Gesellschaft leben“ (Ewald 1993, S. 21). Unfälle hat es zweifelsohne schon „immer gegeben“ (ebd., S. 16). Doch seine spezifische Bedeutung erhält der Begriff im 19. Jahrhundert, in dem er als systematisches Beiproduct und regelhafte Erscheinung moderner Vergesellschaftung und industrieller Produktivität erkannt wird. Der Unfall wird zum Risiko.

Das Risikokalkül, das den Unfall buchstäblich zu einer berechenbaren Erscheinung macht, ist die Voraussetzung etwa für die Sozialisierung von Risiken im Instrumentarium der Versicherung, allerdings auch für neue Formen individueller Verantwortbarkeit. Das Moment der Moral ist im Konzept des Risikos wohl enthalten, wie Niklas Luhmann (1993) in der Unterscheidung von Gefahren und Risiken verdeutlicht hat. Interessanterweise wiederholt sich in dieser Unterscheidung theoretisch die Verschiebung, die sich im 18. Jahrhundert im veränderten Verständnis der Katastrophe abzeichnet. Denn die Gefahr ist das, was von außen hereinbricht. Sie ist insofern subjektunabhängig und liegt außerhalb unseres Einflussvermögens. Als ein Verfahren ist das Risiko hingegen ein Artefakt, es ist menschengemacht. Zugleich produziert es in dem Maße, in dem es an ein Wissen gebunden ist, Handlungsaufforderungen und Zurechenbarkeiten. Das einfache Beispiel, das Luhmann selbst anführt, ist der Regenschirm. Sobald man ihn zu Hause lässt, ist man sozusagen selber schuld, wenn man nass wird. Die Nachteile liegen bei der „eigenen Entscheidung“ (ebd., S. 327). Freilich ist die Wahrnehmung ebenso wie die Zurechnung von Gefahren und Risiken gesellschaftlich verteilt. Ein und derselbe Sachverhalt kann für den Einen ein Risiko, das er oder sie selbst produziert (das riskante Verhalten des Autofahrers oder die risikofreudige Investition des Unternehmers), für den Anderen (Verkehrsteilnehmer, Arbeitnehmer) aber eine Gefahr, die er oder sie nicht in der Hand hat und der man ausgesetzt ist, bedeuten (vgl. Bonß 2010, S. 43).

Wenn das Risikokalkül sich für die Berechenbarkeit von Unglücksfällen und Widerfähnissen verbürgt, so geht damit indes nicht zugleich ein Mehr an Sicherheit und Gewissheiten einher, eher im Gegenteil. Mit dem Wissen um Risiken und vor allem dem Wissen-Können um mögliche Risiken expandiert auch die Risikowahrnehmung und steigen die Entscheidungsanforderungen. Wiederum ist dies gleichermaßen eine Frage von Deutungsprozessen wie auch Effekt der Risikotechnik selbst. Diese „virtualisieren“ die Wirklichkeit gleichsam, spalten sie „in einen abstrakten Raum von Möglichkeiten [auf], die prinzipiell offen sind, kombiniert und kalkuliert werden können“ (Bonß 2010, S. 44). Die Gegenwart wird kontingent (Luhmann 1991).





Zugleich ist im Prozess der Moderne zu beobachten, wie die frühere, durchaus positive Assoziation von Risiken im Kontext von Glücksspielen und Unternehmertum als Wagnis und Chance oder möglicher Verlust verschwindet – und sich stattdessen die negative Assoziation des Unerwünschten an den Begriff heftet. Mit der Vervielfältigung des Risikodiskurses in der Gegenwart avancieren Risiken gewissermaßen zur modernen Form der Wahrnehmung von Gefahren und Übeln oder auch einem individuellen Schicksal (vgl. Fox 1999, S. 12) – und verweisen uns wiederum auf uns selbst zurück, auf unsere eigene Verantwortlichkeit oder auch ein erneutes Ausgesetztsein. Das Risiko wird zu einer Gefahr, nicht weil es noch nicht berechenbar ist, sondern weil es im Überfluss der Informationen nicht mehr handhabbar erscheint. Der Risikodiskurs erweist sich insofern als eine Technologie des Regierens, die dazu angetan ist, uns in Bewegung zu halten und uns in die Pflicht zur Information über die wechselnden wissenschaftlichen Untersuchungsergebnisse und die je adäquate Lebensweise aufzuerlegen.

Insofern tut man aus sozialwissenschaftlicher Sicht gut daran, Risiken und Ungewissheiten weder als real (objektiv gegeben) noch als unwirklich (bloß subjektiv) zu begreifen, vielmehr als die Weisen, in denen wir uns die Realität vorstellen und die Zukunft antizipieren (vgl. O'Malley 2004, S. 15; Dean 1998); in denen wir uns die Welt begreifbar und handhabbar – oder auch komplizierter – machen; und in denen wir uns über Sicherheit regieren lassen. Die entscheidende Frage für die Analyse der „Konstruktionen von Un-Sicherheit“ ist dann, auf welchen Annahmen und welchem Wissen unsere Einschätzungen beruhen und welche Erfahrungen und Erwartungen unsere Sichtweisen und unser Handeln in der Antizipation von Gefahren und Bedrohungen in der Gegenwart anleiten. Das Wissen, das hier inspiziert wird, ist also kein objektives Wissen im Sinne eindeutiger, einhelliger und kompilierbarer wissenschaftlicher Erkenntnis, vielmehr ein gesellschaftlich je objektiviertes Wissen, das sich in entsprechenden Diskursen, Techniken und Verfahren der Regierung von Sicherheit vermittelt.<sup>3</sup> Erst in dieser Perspektive wird es umgekehrt möglich, die einschneidenden Veränderungen, die sich im Feld der Sicherheit in den letzten Jahren vollzogen haben, wiederum als menschengemachte und also von uns selbst hergestellte zu begreifen. Wenn sie in diesem Sinne auch beeinflussbar sind, so freilich gerade nicht im Sinne einer Erneuerung der Machbarkeitsidee, sondern vielmehr der Selbstreflexivität, die uns uns selbst in unserer Situiertheit zu erkennen gibt. In welcher Sicherheitslage also befinden wir uns in unserer Gegenwart?

In der Sicherheitspolitik ist der Topos der zivilen Sicherheit in den letzten Jahren zum Schlüsselbegriff avanciert (Zoche et al. 2011). Mit ihm verbinden sich nicht nur eine

---

<sup>3</sup> Wie Christopher Daase (2012, S. 39) zu Recht feststellt, macht es aus sozialwissenschaftlicher Sicht deshalb wenig Sinn, zwischen subjektiver und objektiver Sicherheit zu unterscheiden. Letztere ist ihrerseits ein Artefakt.



institutionelle Neuorganisation des Sicherheitsapparats, sondern auch ein neues Denken von Gesellschaft und ebenso ein neues Verständnis dessen, was als sicherheitsrelevant einzustufen ist. Zentral ist jetzt die Vorstellung einer hochgradig verletzlichen Gesellschaft, wobei nun weniger die Bevölkerung, Staat und Nation im Visier stehen als vielmehr „kritische Infrastrukturen“. Diese markieren Schlüsselorte des Handels wie etwa Häfen, vor allem aber Schlüsseltechnologien wie Computer und Internet, die Informationen übertragen und so auch die Versorgung der Bevölkerung, der Wirtschaft und der politischen Steuerungsorgane sichern. Der „Ausfall oder [die] Beeinträchtigung“ kritischer Infrastrukturen, so heißt es etwa in einem Strategiepapier des Bundesinnenministeriums (BMI 2009, S. 3), können „nachhaltig wirkende Versorgungsengpässe“ und schließlich „erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ nach sich ziehen. Die Sicherung der Versorgung zeigt sich hier gleichermaßen als Sicherung der Ökonomie, des Wirtschaftsstandorts, wie zum Schutz und zur Sicherheit der Bevölkerung. Ökonomie und Soziales überlagern sich ununterscheidbar im Konzept „kritischer Infrastrukturen“.

Damit verändert sich auch das Verhältnis von Bürger und Staat, denn das Konzept der zivilen Sicherheit entwirft eine neue Verantwortungsstruktur, in der die Bürger verstärkt selbst für ihre Sicherheit sorgen sollen bzw. staatlicherseits verstärkt in die Sicherheitsvorsorge einbezogen werden. Ziel ist es, „die Widerstandsfähigkeit der Gesellschaft“ zu stärken, wie es in einem Programmpapier der Bundesregierung (BMBF 2012, S. 10) beispielhaft heißt, und so „die Robustheit und Sicherheit kritischer Infrastrukturen sowie die Fähigkeit der Bevölkerung zum Überwinden von Krisensituationen zu erhöhen.“ Das fachmännische Zauberwort hierfür ist die Resilienz, die nicht nur Widerstandsfähigkeit, sondern auch Anpassungs- und Handlungsfähigkeit umfasst, wie es wiederum ein Forschungsbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe formuliert: „die Fähigkeit, sich veränderten Umweltbedingungen anzupassen und während bzw. nach einem Schadensereignis die eigene Handlungsfähigkeit aufrechtzuerhalten bzw. wiederherzustellen“ (Goersch & Werner 2011, S. 31).

Gleichzeitig verändert sich in der Programmatik der zivilen Sicherheit auch der Adressat. Standen klassisch der (territorial gebundene) Nationalstaat und seine Bevölkerung im Fokus der Sicherheitsbemühungen, so konzentrieren diese sich jetzt eher auf Prozesse und Abläufe. Mit dem Problem der „Vulnerabilität“ von Infrastrukturen und entsprechenden Dienstleistungen rücken typischerweise Zielsetzungen wie die, die Warenketten zu sichern (und nicht etwa die Orte des Handels selbst), in den Vordergrund.<sup>4</sup> *Safety* im Sinne der Betriebssicherheit und *security* im Sinne des Schutzes vor äußeren Angriffen werden tendenziell ununterscheidbar. Analog hierzu werden auch

---

<sup>4</sup> So lautet etwa ein vom BMBF vorgegebenes Rahmenthema der Forschung, siehe unter <http://www.bmbf.de/de/15034.php> [14. August 2013].



die Bürger jetzt weniger als die Gesellschaft (als Ganze) adressiert. Im Programm der zivilen Sicherheit fungieren sie vielmehr als eine Art Scharnier oder aktivierbare Multitude. Elementar ist die Konnektivität. Darunter verändern sich auch die Formen der Kommunikation, die sich weniger vertikal von Staat und Regierung an die Bevölkerung richten. Entscheidend ist vielmehr die kommunikative Vernetzung in der Bevölkerung selbst. Computer oder Smartphone, Internet, Web-Foren oder Twitter sind die Medien, in denen sich die Vielen im Katastrophenfall selbst organisieren und horizontal untereinander verständigen oder auch, bestenfalls, Informationen etwa über die Lage vor Ort (z.B. über Twitter) an staatliche Behörden, also eher von unten nach oben, weiterleiten sollen. Crowdsourcing ist das Stichwort (Howe 2006). „Die Menge“, so die neue sozialwissenschaftlich untermauerte Einsicht, ist, sofern sie sich nur hinreichend heterogen zusammensetzt, klüger als der einzelne Experte (Surowiecki 2007). Mit dem Fokus auf „kritische Infrastrukturen“ verändern sich auch die Formen der Intervention, die sich auf komplexe Systeme einstellen müssen.

Das Konzept der Resilienz kam bereits in den 1970er Jahren im Rahmen des ökologischen Denkens, aber auch neoliberaler Theorie auf (insbesondere bei Hayek, siehe Walker & Cooper 2011). Doch zentrale Bedeutung in der Sicherheitspolitik hat es erst nach den Anschlägen von 9/11 erlangt, zunächst in den USA, mittlerweile aber auch hierzulande. Man kann es als ein strategisches Konzept des Umgangs mit Bedrohungen begreifen, das sich bezeichnenderweise auf komplexe, anpassungsfähige Systeme bezieht, die mutmaßlich nur begrenzt steuerbar und überdies permanent mit Unsicherheiten konfrontiert sind. Die „Kultur der Resilienz“ operiert deshalb nicht mehr mit statistisch kalkulierbaren Risiken (Amoore & de Goede 2008). Sie geht davon aus, dass die Krise eine Art Dauerzustand ist. Unvorhergesehene Notsituationen können prinzipiell immer entstehen (*emergency emergence*), wir sind der möglichen Katastrophe jederzeit ausgesetzt. Deshalb ist unsere ständige Wachsamkeit ebenso gefragt wie unsere Fähigkeit, auf das Unvermeidliche eingestellt und vorbereitet zu sein (*preparedness*). Weil wir „nicht mehr an den Ursachen“ ansetzen können, wird die Fähigkeit umso wichtiger, „mit widrigen Bedingungen zurecht zu kommen“ (Bröckling 2012, S. 103) und schließlich auch entsprechend antworten zu können (*resilience*) (Lentzos & Rose 2008).<sup>5</sup> Verantwortlich werden wir in diesem Sinne

---

<sup>5</sup> Mit dem Begriff der *preparedness* verbindet sich insofern ein gewisser Rückzug. Das Bemühen zielt nicht mehr darauf, das Eintreten einer Gefahr zu verhindern, sondern nur noch deren zerstörerische Folgen zu gegenwärtigen. Bröckling (2012) schreibt den Prinzipien deshalb auch eine gewisse hierarchische Ordnung zu: Anders als das Prinzip der Resilienz, das nicht nur auf Schutz, sondern auf Optimierung aus ist und Aktivierung voraussetzt (Lentzos & Rose 2008), figuriert die Preparedness in einem Szenario der Katastrophe, auf die man ihrerseits nicht mehr Einfluss nehmen kann. Tatsächlich lösen sich beide Prinzipien im gegenwärtigen Regime der Regierung von Sicherheit jedoch nicht ab, sondern gelten gleichermaßen als mögliche Re-Aktions-



vollkommen selbst. François Ewald (1998) erkennt den Paradigmenwechsel, der sich hiermit in der Regierung der Sicherheit anzeigt, in der Verschiebung vom Rationalitätstypus der Prävention hin zur „Vorbeugung“. Die „Rückkehr der Katastrophe“, die nunmehr als menschengemacht erscheint, stellt das solidarische Prinzip der Versicherung, das für die zweite Hälfte des 20. Jahrhunderts bestimmend war, sowie überhaupt die Berechenbarkeit und Versicherbarkeit von Risiken in Frage. Vorbeugung ist geboten angesichts unkalkulierbarer Risiken, von denen man nicht weiß, ob, wann und wie der Schaden eintreten wird,<sup>6</sup> während man aber gleichzeitig mit enormen Schäden sowie „irreparablen und irreversiblen Folgen“ rechnen muss (Kaufmann 2011, S. 103). Wissen, Erfahrung und mathematisches Kalkül bilden nicht länger die hinreichende Grundlage von Sicherheitsstrategien. In einer Situation „radikaler Ungewissheit“ (Kessler & Werner 2008) sind vielmehr Techniken der Imagination angezeigt, die den schlimmsten und eigentlich unvorstellbaren Fall zu antizipieren suchen. Das ist der Paradigmenwechsel von Risiko- zu Szenariotechniken.<sup>7</sup>

Zivile Sicherheit begründet sich im Schnittfeld der klassischen Aufgabenbereiche der Inneren Sicherheit, der Kriegsführung sowie des Katastrophenschutzes (vgl. Kaufmann 2011, S. 102). Damit befördert das Konzept eine umfassende Restrukturierung der Sicherheitsarchitektur, die sich insbesondere im 21. Jahrhundert vollzogen hat. Institutionell sichtbar wurde sie in den USA etwa mit der Gründung der „Homeland Security“, die nunmehr Grenzschutz, Terrorismusbekämpfung und Katastrophenschutz unter sich vereint; und hierzulande etwa in der Neukonfigurierung des „Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe“ (BBK) im Jahr 2004. Zugleich fügt sich das Konzept der kritischen Infrastrukturen auch in einen Paradigmenwechsel in der Kriegsführung ein, die genau genommen keine Kriegsführung mehr ist. Denn wir

---

und Aktivierungsformen: Nicht das Vermeiden der Gefahr, sondern die entsprechende Antwort, auf die man vorbereitet sein muss, ist entscheidend (Lakoff 2006).

<sup>6</sup> Der Begriff der *precaution*, der in den 1980er Jahren im Kontext der europäischen Umweltpolitik aufkommt, wird ins Deutsche mal mit „Vorbeugung“ (Ewald 1998), mal mit „Vorsorge“ (Sunstein 2007) übersetzt. Das *precautionary principle* steht für einen Rationalitätstypus, der, immer noch in Abwägung mit den ökonomischen Kosten, „Maßnahmen zum Schutz vor potentiellen Gefahren“ auch und gerade in dem Moment vorsieht, in dem wissenschaftlich gesehen ungewiss ist, ob die Gefahren auch tatsächlich eintreten werden und von welchen Faktoren das abhängig ist (ebd., S. 13). Die Bedrohungen werden zwar erkannt, aber sie können wissenschaftlich nicht ermessen und gemessen werden. Die Entscheidung zu handeln, wird zu einer *notwendigen Entscheidung* „aufgrund wissenschaftlicher Ungewissheit“ (Ewald 1998, S. 20).

<sup>7</sup> Zu Recht wird verschiedentlich darauf hingewiesen, dass dieses Bewusstsein „radikaler Ungewissheit“ keineswegs eine neue Erscheinung, sondern aus der ökonomischen Theorie hinlänglich bekannt ist (Bonß 2010, S. 44f.; Kessler & Werner 2008, S. 294; O'Malley 2004, S. 13ff.). Die entscheidende Frage hier ist jedoch, welches Bewusstsein in einer bestimmten Zeit und in politischen Programmen dominant wird und sich mit der Vorstellung der Irreversibilität und eines „nicht-anders-Könnens“ verbindet.



haben es nicht mehr mit der spezifisch modernen Vorstellung einer Konfrontation zweier souveräner Staaten oder auch einer förmlichen Kriegserklärung zu tun (Werber 2010). Aufstands- und Terrorismusbekämpfung rechnen vielmehr mit einer asymmetrischen Konstellation, die es zu „re-symmetrieren“ gilt (Münkler 2013), und das heißt, vor allem auf die Identifikation modular organisierter, polyzentrischer Netzwerke mit netzwerkförmig organisierten Strategien und Taktiken zu antworten (Arquilla & Ronfeldt 2001).

Genau hierin verbinden sich innere und äußere Sicherheit, die nun gleichermaßen mit komplexen Systemen, wie kritischen Infrastrukturen oder terroristischen Netzwerken, und deren konzertierten Operationen befasst sind (Galloway & Thacker 2007; Zebrowski 2009). Medium der Kontrolle und Intervention sind dann nicht in erster Linie Recht und Normen, welche die Öffentlichkeit oder den Einzelnen adressieren, als vielmehr indirekte und informelle Formen der Regulierung von „Lebensmilieus“ bzw. von Mechanismen und Organisationsformen komplexer Systeme. Entsprechende Rationalitäten der Intervention sind auf der einen Seite Preparedness und Resilienz, die auf die selbst-organisierenden und -wiederherstellenden Kräfte des sozialen Lebens selbst (vgl. Chandler 2013, S. 211), und auf der anderen Seite prä-emptive Interventionen, die auf emergierende, nicht-lineare und kontingente, Bedrohungen zielen.

Kontrolle wird unterdessen ihrerseits modular, technologische Entwicklungen und das neue „Denken des Sozialen“ in Kategorien von Infrastrukturen und Verknüpfungen spielen hier ineinander. Die Kontrolltechnologien verstreuen und vervielfältigen sich, sie werden mobiler und in gewisser Weise zugleich auch unscheinbarer (Murakami Wood 2011). Insbesondere mit der Automatisierung bzw. Digitalisierung geht eine qualitative Veränderung einher. Formen der Kontrolle und Überwachung, die sich in automatische Systeme einprogrammieren lassen und so einschreiben, werden immanent und tendenziell opak (Zebrowski 2009) – was für die gegnerischen Netzwerke gilt, zeigt sich umgekehrt auch an den Netzwerken der Kontrolle: „The nonhuman quality of networks is precisely what makes them so difficult to grasp.“ (Galloway & Thacker 2007, S. 5)

Ausgehend von der Beobachtung, dass in modernen Gesellschaften jeder Bürger wie ein undichter Behälter kontinuierlich Datenspuren hinterlässt, die in entsprechenden Datenbanken gesammelt und verknüpft werden können, hat sich im Bereich der *Surveillance Studies* (Lyon 2007) der Begriff der Data Doubles (Lyon 2010) eingebürgert. Gemeint sind damit virtuelle Doppelgänger, Datenstrukturen, die Informationen über reale Personen vereinigen – über Konsumgewohnheiten, Mobilitätsmuster, behördlich registrierte Auffälligkeiten und sonstige den realen Einzelnen zuzuschreibende Besonderheiten. Solche Informationen dienen dazu, Personen zu kontrollieren, zu identifizieren, sie bestimmten Gefährdungs- oder Konsumklassen zuzuordnen, ihnen Zugang zu Dienstleistungen oder Orten zu gewähren oder zu verweigern.



Der Nettoeffekt dieser Entwicklung ist als Dangerisation beschrieben worden (Lianos & Douglas 2000). Die reale Person in ihren sozio-kulturellen Bezügen verschwindet aus dem Blickfeld, sie steht als Erscheinung a priori unter Verdacht bis zum Beweis des Gegenteils. Dieser Beweis wird erbracht über eine digitale Identität. Das Paradebeispiel für diesen Typ der mediatisierten Interaktion ist der Geldautomat, der ohne Ansehung der realen Person erst dann die gewünschte Dienstleistung erbringt, wenn sich sein materielles Gegenüber durch einen PIN Code ausgewiesen, also entverdächtigt hat. Diese Art oder dieses Format von „verdachtsgeleiteter“ Interaktion breitet sich in den mundanen Alltag aus, zu dessen Bewältigung die unterschiedlichsten Identitätsartefakte benötigt werden.

Bezogen auf die Frage nach der Bedeutung dieser Entwicklung hin zu einer medial vermittelten Persona, bei der die reale Person hinter maschinenlesbaren Codes verschwindet, zeigt sich für die gesellschaftliche Konstruktion von Sicherheit, dass die Entscheidung, ob eine Person oder Situation vertrauenswürdig und daher für weitere Kommunikation oder den sozialen Verkehr anschlussfähig ist, nur durch den Umweg über abstrakte Systeme beantwortet werden kann. Die gesellschaftliche Wirkung dieser Entwicklung ließe sich als Entwertung evolutionär erprobter und kulturell eingeübter Routinen der Einschätzung von Situationen interpretieren. Giddens (1991) hat hier den Begriff des Verlusts der ontologischen Sicherheit geprägt. So treten die Akteure der Kontrolle in den Hintergrund – die Generierung von Verdacht wird den Maschinen, welche die Daten scannen, überlassen; menschliche Interaktionen und Aushandlungsprozesse reduzieren sich auf anonyme Entscheidungsprozesse in der Codierung von „ja – nein“, „adäquat – inadäquat“ (Aas 2004) –, und überdies sind die diesen Prozessen und Prozeduren zugrundeliegenden Normen selbst schwer zu identifizieren. Dabei ist zum einen eine Umkehr des Prinzips der Unschuldsvermutung zu beobachten – wer technisch als verdächtig detektiert wird, muss sich rechtfertigen. Zum anderen scannen die automatisierten Überwachungstechnologien nicht nur einfach zuvor festgeschriebene Normen, vielmehr generieren sie in der Detektion von Unregelmäßigkeiten auch ihrerseits Normen (Amoore 2008). Aus Verdachtsklärung im Sinne der klassischen Gefahrenabwehr und Strafverfolgung wird Verdachtsschöpfung (Pütter et al. 2005) im Gefahrenvorgriff, die sich technisch herstellt.

Die Frage der Sicherheit wird mit diesen Entwicklungen indes nicht eingedämmt, eher weiten Sicherheitsbelange sich im Raster von Wissenstechniken der Antizipation von Gefahren und vor allem abstrakten Bedrohungen aus.



### 1.3 Sicherheit expandiert: Über die Vervielfältigung des Möglichen

Schon das Risikodenken geht in gewisser Weise mit einer Ausdehnung von Sicherheitsbelangen einher. Nichts ist „an sich“ ein Risiko, wie François Ewald (1993, S. 210) angemerkt hat, prinzipiell kann aber alles zum Risiko werden: „alles hängt ab von der Art und Weise, in der man die Gefahr analysiert, das Ereignis betrachtet“. Denn Risikotechnologien abstrahieren von konkreten Gefahren ebenso wie von konkreten Individuen. Sie operieren „mit Faktoren, mit statistischen Korrelationen heterogener Elemente. Sie dekonstruieren das konkrete Subjekt der Intervention und konstruieren ein Kombinatorium aller risikoträchtigen Faktoren“, so Robert Castel (1983, S. 61). Umgekehrt können die Risikomerkmale auf ein konkretes Individuum bezogen werden, das so zum Gegenstand messbarer Risikofaktoren wird. Dabei sind diese Merkmale für sich genommen neutral. Nicht der Normverstoß selbst steht hier im Mittelpunkt, sondern die Abweichung von einer empirisch beobachtbaren Regelmäßigkeit und einer so verstandenen „Normalität“. So gilt es für sich genommen weder als verwerflich noch als gefährlich, eine bestimmte Zahlweise, bestimmte Speisen oder bestimmte Kleidung zu bevorzugen oder häufig in bestimmte Länder zu reisen usw. Unter bestimmten Voraussetzungen können solche Kriterien jedoch zu Risikofaktoren werden und die Grundlage für die Identifizierung von Risikogruppen bilden. Eine einzelne Person kann sich dann unter eine bestimmte Risikogruppe subsumiert finden, wenn bereits einige der Merkmale auf sie zutreffen. Dies wiederum kann bestimmte Maßnahmen zur Abwendung der erwarteten Gefahr rechtfertigen, selbst wenn (noch) keine konkreten Anhaltspunkte für deren Eintreten zuhanden sind. Denn Grundlage des Risikokalküls sind ja Wahrscheinlichkeiten und Faktoren, die ihrerseits nicht unmittelbar und schon gar nicht zwingend mit der Gefahr bzw. der antizipierten Straftat in Zusammenhang stehen müssen. So hat man in den 1970er Jahren festgestellt, dass terroristische Gruppierungen, um nicht aufzufallen, die Stromrechnung für konspirative Wohnungen vorzugsweise bar bezahlten – und daraus Anhaltspunkte für die Rasterfahndung entwickelt.

Während das Prinzip der Risikotechnik darin besteht, Gefahrenprognosen auf der Grundlage von Erfahrungen mit vergangenen Ereignissen und den dort ausgemachten Zusammenhängen vorzunehmen, sucht die sogenannte Szenariotechnik sich genau hiervon zu lösen. Sie empfiehlt sich ja auf der Basis der Annahme, dass die probabilistische Methode im Hinblick auf unvorhersehbare Katastrophen untauglich geworden ist. Erklärtes Ziel ist es, systematisch unsere Denkgewohnheiten und die Grenzen unserer Vorstellungskraft aufzubrechen, um das „Unvorstellbare vorstellbar“



zu machen.<sup>8</sup> Dabei ist die Szenariotechnik, die auf die Fähigkeit, die Phantasie spielen zu lassen, setzt, ihrerseits durchaus nicht neu. Ihre Genealogie verweist in die Zeit des Kalten Krieges zurück, als man die möglichen Folgen eines atomaren Angriffs vor Augen hatte (Ghamari-Tabrizi 2005; Opitz & Tellmann 2011). Sie gewann jedoch vor allem mit einer neuen Krisendiagnose angesichts der Terror-Anschläge von 2001 an Popularität. So hatte in den USA der vom Kongress und dem Präsidenten in Auftrag gegebene Bericht der 9/11-Kommission den Sicherheitsbehörden einen „Mangel an Vorstellungskraft“ attestiert (vgl. *The 9/11 Commission Report* 2004, S. 339-360). Weil man sich einfach nicht habe vorstellen können, dass zivile Flugzeuge zum Werkzeug von Selbstmordattentätern werden könnten, hatte man selbst die vorliegenden Geheimdienstinformation und Anzeichen der kommenden Gefahr nicht richtig lesen können. US-amerikanische Einrichtungen sahen es deshalb als geboten an, in der Antizipation von Bedrohungen auch auf fiktives Material aus der Unterhaltungsindustrie zurückzugreifen: Die Katastrophe ist Teil unseres kulturellen Repertoires und in der Literatur wie vor allem in Hollywoodfilmen bereits vorweggenommen (Der Derian 2005; Sarasin 2004). Fiktion und Realität miteinander zu verschmelzen, wird Methode. Entscheidend ist nicht der wahrscheinliche, sondern der mögliche denkbare Fall. Anders als die Risikotechnik, die auf eine Treffsicherheit in der *Prädiktion* geeicht ist, operiert die Szenariotechnik mit der *Prämediation* (Grusin 2004),<sup>9</sup> der es in der Vorausschau um möglichst extreme Visionen und letztlich eine „Vervielfältigung des Möglichen“ geht: Der Phantasie sind prinzipiell keine Grenzen gesetzt. Wenn man zur Beschreibung dieser Differenz auf wissenschaftstheoretische Begriffe zurückgreifen will, dann arbeitet die Vorhersage, die Prädiktion, gewissermaßen mit dem Prinzip der Veridiktion: Sie geht von einer Wahrheit aus, die man richtig treffen kann und soll (während man ansonsten eben falsch: daneben liegt). Die Prämediation produziert demgegenüber, wie es in der ethnographischen Forschung heißt, eine Art Verisimilitude. Sie verdoppelt die Realität in der Imagination, in der Welt des Fiktiven, die ihrerseits gerade darin realitätsmächtig ist, dass sie die reale Welt überzeugend erfahrbar, vorstellbar und fühlbar macht.

Nun mag man solche Ansätze als Spezialerscheinung post 9/11 lesen. Doch spielen Szenarien nicht nur in der politischen Sicherheitsdebatte und in der Sicherheitsgesetzgebung eine zusehends größere Rolle, sondern auch in der institutionalisierten

---

<sup>8</sup> Die Formel *Thinking about the Unthinkable* geht auf den Physiker Herman Kahn zurück, der seinerzeit als Systemanalytiker in der *RAND Corporation* mit der Aufgabe befasst war, Strategien der Zivilverteidigung für den Fall eines atomaren Angriffs zu erarbeiten (Ghamari-Tabrizi 2005; Opitz & Tellmann 2011).

<sup>9</sup> Mit dem Begriff der Prämediation – in Anlehnung an den der Mediation bzw. Mediatisierung – betont Richard Grusin (2004), dass jegliches Wissen, Wahrheit und Fakten mediatisiert sind. Sie sind niemals unabhängig von Praktiken, Techniken und Verfahren der Wissenserzeugung und Vermittlung.





Sicherheitspolitik. Der Flugkörper, der am Kernkraftwerk detoniert, der von Terroristen entführte Panzer, der auf ein Chemiewerk zurollt, die Verseuchung des Grundwassers mit Viren, das sind Szenarien, die alltagsweltlich so oder ähnlich bereits aus der politischen Debatte vertraut sind. Szenarien und Simulationen bestimmen überdies auch systematisch die vom BBK seit 2004 organisierten Planspiele, die auf das Feld der zivilen Sicherheit übertragen, was einst eher im militärischen Bereich stattfand: das Einüben des Katastrophenfalls. So findet die groß angelegte „Länderübergreifende Krisenmanagement Exercise“ (LÜKEX) etwa alle zwei Jahre unter der Überschrift jeweils als möglich identifizierter Krisenszenarien wie z.B. „Außergewöhnliche biologische Bedrohungslage“ (2013), „Bedrohung der Sicherheit der Informationstechnik durch massive Cyber-Attacken“ (2011), „Terroristische Bedrohung mit konventionellen Sprengstoffen, chemischen und radioaktiven Tatmitteln („schmutzige Bombe““ (2009/10) statt.<sup>10</sup> In der Zusammenarbeit mit Behörden und Privatunternehmen besteht das Ziel hauptsächlich darin, Kaskadeneffekte von Störungen auszuloten und politische Entscheidungsträger bzw. Führungskräfte auf diese komplexen Anforderungen der Identifikation von Problemen und Gefahrenlagen, der Entscheidung, Organisation und Kooperation zwischen den verschiedenen Entscheidungsebenen und -trägern vorzubereiten.

Während die Übung in solchen Planspielen den fiktiven Bias von Szenariotechniken gleichsam im Realen verankert, ist das Szenariodenken selbst umgekehrt dazu angelegt, mögliche Sicherheitsanforderungen weiter fortzuschreiben. Niemand hat diese Logik wohl treffender in die Realität zu setzen gewusst als Donald Rumsfeld, der auf einer Pressekonferenz im Nato-Hauptquartier in Brüssel im Jahr 2002 zur Charakterisierung der neuen Sicherheitslage die Formel von den *unknown unknowns* ins Spiel brachte. Die Formel ist Sprechakttheorie *in vivo*, denn im Moment ihres Ausspruchs bringt sie selbst zur Existenz, was sie behauptet. Möglich ist das, weil sie eine neue, unbekannte Bedrohungsdimension antizipiert, die in ihrer Abstraktheit unwiderleglich ist. So sehr die nächste Katastrophe unvorhersehbar und unkalkulierbar ist (Massumi 2007) – wir wissen oder ahnen noch nicht einmal (*unknown*), wer oder was wann und in welcher Weise (*unknowns*) einen ungeheuren Schaden wird anrichten können – so gewiss ist zugleich, dass sie möglich und folglich zu gewärtigen ist. Die Katastrophe muss nach Möglichkeit abgewendet werden, noch bevor erste Anzeichen einer Gefahr überhaupt auftauchen können. Das ist die Ratio des Vorgriffs (*pre-emption*), von dem Bestreben beseelt, jedes Risiko auszuschließen (vgl. Amoores & de Goede 2008, S. 11).<sup>11</sup>

---

<sup>10</sup> Siehe [http://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/TT\\_Luekex\\_ueberblick.html](http://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/TT_Luekex_ueberblick.html) [11. September 2013].

<sup>11</sup> Unter dem Begriff der *precaution* werden das Prinzip der Vorbeugung im Sinne Ewalds und des Vorgriffs (*pre-emption*) vielfach gleichgesetzt. Man muss indes einen Unterschied darin sehen, dass



Wir müssen also, streng genommen, handeln, intervenieren, bevor wir den Gegner bzw. die Gefahr überhaupt kennen und erkennen können. Dabei ist die Pointe jener Denkfigur, dass ihre Aussage sich auch gleichsam selbst verifiziert. Denn weil die Bedrohung per definitionem unvorhersehbar und unkalkulierbar ist, beweist die Abwesenheit von konkreten Anhaltspunkten für die Bedrohung (z.B. eines terroristischen Anschlags), Rumsfelds Logik zufolge, noch lange nicht, dass auch die Bedrohung abwesend ist. Sie ist, im Gegenteil, potenziell existent: “an absence of any evidence of threats is not evidence of absence of threats”.<sup>12</sup>

Wenn Szenariotechniken dieses Prinzip der Vervielfältigung des Möglichen im Modus der Antizipation von Bedrohungen kultivieren, so ist dieses jedoch keineswegs auf jene beschränkt, der Logik des Sicherheitsdenkens vielmehr generell inhärent. Denn Sicherheit lässt sich nicht in Besitz nehmen, eher entgleitet sie uns in dem Moment, in dem wir sie denken. Zwar kann ich mich in diesem Augenblick sicher fühlen, doch kann ich nicht wissen, ob das so bleiben wird. Ungewissheit ist insofern unaufhebbarer Bestandteil der Sicherheit, das Unvorhergesehene ihr ständiger Begleiter. Sicherheit steht stets zur Disposition. Dies liegt zunächst in ihrer eigenartigen temporalen Bestimmung begründet. Sicherheit bezieht sich auf eine Zukunft, die notwendig unbekannt ist und die überdies unter dem Vorzeichen einer Bedrohung steht. Sie verbindet sich insofern mit einer gewissen Dringlichkeit. „Prävention und Vorsorgegedanke“, so Oliver Lepsius (2010, S. 47) mit Blick auf die Folgen für das Recht, „sind ihrer Natur nach tatsachenavers, denn sie wollen, daß bestimmte Tatsachen erst gar nicht eintreten. Wer vorsorgen will, muß Gefahren wittern, wo noch keine sind. Deshalb lassen wir bei der Rechtfertigung präventiver Maßnahmen im Bereich des Tatsächlichen Abstriche zu. Man kann nicht warten bis Endgültiges passiert; es muß gehandelt werden, bevor es zu spät ist. Im präventiven Bereich wird das Handeln daher von Vermutungen und Prognosen geleitet“. Dabei bleiben Techniken der Risikoprognose und vor allem die Rhetorik und das Denken in Kategorien von Risiken auch dann noch gesellschaftlich virulent, wenn sich zusehends die Einsicht in die Unkalkulierbarkeit von Risiken bzw. die Unzulänglichkeit des Risikokalküls durchsetzt (vgl. Amoores & de Goede 2008, S. 10). Wie Cass Sunstein (2007, S. 15) beobachtet hat, spielt vor allem im Alltagsgebrauch eine „Verfügbarkeitsheuristik“ (Tversky & Kahneman 1974) in der Wahrnehmung von Gefahren und Bedrohungen eine zentrale Rolle: „Wenn Menschen keine statistischen Informationen vorliegen, schreiben sie Risiken eine große Bedeutung zu, falls ihnen leicht Beispiele einfallen, in denen diese Risiken tatsächlich eingetreten sind.“ Nicht allein das wissenschaftlich untermauerte Wissen prägt diese Verfügbarkeitsheuristik, entscheidend sind vielmehr die Vertrautheit der Informationen

---

*pre-emption* nicht mehr zögerlich ist, sich also auch nicht mehr mit Kosten-Nutzen-Abwägungen aufhält, und die Intervention bereits in dem Moment angezeigt sieht, in dem die Art der Bedrohung überhaupt noch nicht ausgemacht ist (vgl. Anderson 2010, S. 14; Massumi 2007).

<sup>12</sup> Verfügbar unter [www.nato.int/docu/speech/2002/s020606g.htm](http://www.nato.int/docu/speech/2002/s020606g.htm) [22. August 2013].



(z.B. über das Rauchen) und die Signifikanz eines Ereignisses, das in Erinnerung bleibt (vgl. ebd., S. 58). Wahrnehmung ist vor allem sinnlich: „Wir verlassen uns in unserem Alltag weniger auf unseren Intellekt als auf unsere Sinne. Wir glauben, was wir sehen, und wir sehen, was wir glauben.“ (Kreissl 2008, S. 322)

Wenn das Potenzial, immer weitere, mögliche Gefahren zu erkennen, also schon im Risikodenken präsent ist, so unterscheidet sich das Risikomanagement von der Ratio des Vorgriffs darin, dass es sich noch leisten kann, die Verteilung von Risiken zu organisieren und (kosten-)optimale Mittelwerte der Intervention sowie Grenzwerte des Akzeptablen festzulegen. Unter dem Vorzeichen unvorhersehbarer Katastrophen hingegen werden die Antizipation möglicher Gefahren sowie die Suche nach geeigneten Maßnahmen zu deren Abwehr eher zu einem permanenten Gebot, und Abwarten oder Unterlassen diskreditiert. In der Anforderung, sich auf das Mögliche einzustellen und vorzubereiten, werden Sicherheitsambitionen dabei tendenziell unabschließbar, gerade weil das Mögliche nicht auszuschließen ist. Bezeichnend ist jedoch für Risiko- und Szenariodenken gleichermaßen, dass die Imagination den Ausschlag gibt: Nicht nur, was wir wissen, sondern vor allem, was wir uns vorstellen können, bestimmt unsere Realitätswahrnehmung. Was uns affiziert, ist das, was erfahrbar ist und wir schließlich als real *empfinden* können (vgl. Massumi 2010, S. 53).

#### 1.4 Ethik der Sicherheit

In der Zusammenschau kristallisieren sich demnach zwei bezeichnende Momente eines modernen Sicherheitsdenkens heraus – und weisen die Krise der Sicherheit eher als eine Fortschreibung dessen denn als etwas Neues aus. Erst wenn man diese Logik der Sicherheit begreift, so der Ansatzpunkt hier, lassen sich auch die paradoxen Effekte historisch und kulturell je spezifischer Bedingungen der Regierung von Sicherheit erfassen: Auf der einen Seite stellt das Problem der Sicherheit sich notwendig an der Grenze des Wissens. Denn die Frage der Sicherheit bezieht sich auf Gefahren und Bedrohungen, die sich per definitionem noch nicht materialisiert haben. Sie sind unbekannt, weil sie noch nicht eingetreten sind. Andernfalls würde es sich um bereits eingetretene Schadensfälle handeln (vgl. Massumi 2005, S. 35). Das Unbekannte ist das Metier der Regierung der Sicherheit, die deshalb auch stets von ihrem Gegenteil, der Unsicherheit und Ungewissheit, handelt. Auf der anderen Seite, und auch das ist ihr Metier, überschreitet die Regierung der Sicherheit permanent eben diese Grenze des Wissens, indem sie nämlich eine unbekannte, gefährvolle oder bedrohliche Zukunft erkennbar, handhabbar oder auch beherrschbar zu machen sucht. Gefahrenprognosen, Risikokalküle, Szenariotechniken dienen hier als Wissenstechniken, die genau dies leisten sollen – und zugleich niemals können, weil die Grenze des Wissens



unüberschreitbar bleibt. Die Zukunft bleibt kontingent. Sie lässt sich nur in Kategorien des Wahrscheinlichen und Möglichen begreifen.

Eine der wichtigsten Fragen, die sich hieran für die sozialwissenschaftliche Analyse anschließen, lautet daher, wie dieses unhintergehbare Nicht-Wissen mit Hilfe von Wissenstechniken der Antizipation in ein Wissen überführt wird. Oder anders gesagt, wie es von einem anderen Wissen (etwa von Risikogrößen oder auch Szenariovorstellungen) eingenommen wird, das den Hiatus zwischen Zukunft und Gegenwart gleichsam überbrückt oder auch überspielt. Was also genau bildet die Grundlage unserer Entscheidungen bei Sicherheitsmaßnahmen oder auch in der Sicherheitsgesetzgebung, die notwendig mit dem Möglichen und nicht nur dem Tatsächlichen umgehen müssen?

Die Regierung der Sicherheit ist unauflöslich mit Wertfragen verknüpft. Dies nicht etwa nur weil Sicherheit ein knappes und nur begrenzt zu verteilendes Gut ist, das die Abwägung und Entscheidung über diese Verteilung verlangt. Die Frage der Ethik wird vielmehr bereits in dem Moment konstitutiv, in dem Handlungsentscheidungen unter den Bedingungen des Nicht-Wissens bzw. eines unzureichenden Wissens zu treffen sind. Epistemologie und Ethik – die Frage nach dem, was wir wissen und *was ist*, und die normativ die Frage nach dem, was wir wollen und *was sein soll* – überlagern sich hier, obgleich sie, wie der Sicherheitsforscher Peter Burgess (2011, S. 4f.) herausgearbeitet hat, im philosophischen Denken zu Recht zwei deutlich voneinander abgegrenzte Bereiche markieren. Wir entscheiden über Sicherheitsmaßnahmen, obwohl wir die Gefahr notwendig nur unzureichend kennen. Erkennen und Entscheidung verfehlen – und damit wiederholt und potenziert sich in der Regierung der Sicherheit ein generelles erkenntnistheoretisches Problem – gewissermaßen stets ihr Objekt (vgl. ebd., S. 7). Dies umso mehr, wie wir von abstrakten Bedrohungen ausgehen, die unbestimmt und per definitionem unvorhersehbar sind. In der Entscheidung auf der Basis von Ungewissheit bestimmen wir mithin, was sein soll, obwohl wir nur unzulänglich wissen, was ist. Die Norm als Grundlage der Entscheidung tritt gewissermaßen an die Stelle des Wissens.

Zugleich ist das Wissen, das die Techniken der Antizipation von Gefahren und Bedrohungen hervorbringen, seinerseits wirklichkeitskonstitutiv oder, wie die Soziologin Elena Esposito (2007, S. 31) mit Luhmann feststellt: Realitätsverdopplung. Realitätsverdopplungen wie etwa Risikokategorien und -schemata konkurrieren nicht mit der „realen Realität“ (ebd.), vielmehr fügen sie dieser eine weitere Ebene hinzu und machen die Realität, als Schema der Interpretation und Raster der Wahrnehmung, erst in bestimmter Weise erfahrbar und begreifbar. Sie nähern sich in diesem Sinne also nicht einfach nur einer Wahrheit an, die sie möglichst exakt beschreiben können, vielmehr bilden sie eine eigene Realität aus. Darin unterscheiden Risiko- und Szenariotechniken sich gerade nicht, dass sie insofern *fiktive Realitäten* (Esposito 1998) sind.



Sie sind deshalb keineswegs illusionär oder trügerisch. Vielmehr stellen sie als Verfahrenstechniken und Deutungsschema bestimmte Formen der Sichtbarkeit und Sagbarkeit erst her – und strukturieren auf diese Weise unsere Wahrnehmung wie unsere Vorstellungsweisen. So ist es für uns inzwischen Alltag geworden, unser Handeln und unsere Lebensweise in Kategorien von Risiken zu denken und auch danach auszurichten („Rauchen erzeugt Krebs“, „Tomaten oder Brokkoli essen bekämpft Krebs“). Und obgleich die Risikoprognose den Anspruch erhebt, möglichst präzise und zuverlässige Vorhersagen zu machen, ist sie doch immer auch imaginativ und in gewisser Weise sogar spekulativ, eben weil auch sie die Grenze des Wissens über das Zukünftige nicht überschreitet, sondern immer nur ihr eigenes Wissen oder genauer: ihre eigenen Wissensformen anbieten kann. Doch während die Szenariotechnik bewusst mit unseren Imaginationen spielt, gesteht die Risikotechnik zumeist nur widerwillig ein, dass ihre Treffsicherheit eine relative ist.<sup>13</sup> Sie handelt eben nicht von Tatsachen, sondern von Wahrscheinlichkeiten, in deren Kalkül überdies Werturteile und -entscheidungen eingeschmolzen sind.

Zusammenfassend lassen sich demnach folgende Ansatzpunkte festhalten:

Zunächst einmal haben wir argumentiert, dass die gegenwärtige Krise der Sicherheit ihrerseits im modernen Denken verankert ist und insofern gerade nicht von neuen Dimensionen der Bedrohung oder einer Ausweitung von Sicherheitsproblemen zeugt. Sie weist vielmehr auf eine spezifische Logik des Sicherheitsdenkens hin, die ihren Nährstoff in der Antizipation (immer weiterer) möglicher Gefahren und Bedrohungen findet. Risiko- und Szenariotechniken unterscheiden sich darin nicht, dass sie unsere Imaginationen evozieren.

Wenn eine Regierung der Sicherheit von der Einsicht in die stets unvollständige Sicherheit geprägt sein will, und das heißt, ohne damit zu hadern, dann bestünde ein erstes epistemisch-ethisches Prinzip darin, aus jener Logik der Vervielfältigung möglicher – antizipierter, imaginerter – Bedrohungen auszusteigen. Diese Option liegt in einer Praxis, welche das Abstrakte der Bedrohung zwangsläufig konkretisiert, nämlich auf einen konkreten Kontext der Anwendung bzw. Umsetzung herunterbuchstabiert. Ansätze, die eine Kultur des öffentlichen Streits zu implementieren suchen, sind insofern verdienstvoll. So kann es etwa gelingen, Bedrohungsszenarien im Augenschein ihrer Wahrscheinlichkeit oder Plausibilität zu dekonstruieren oder Sicherheitsfragen als Wertfragen offenzulegen. Abgesehen von dem Umstand jedoch, dass eine solche diskursive Praxis zumeist unausgesprochen ihre eigenen Rationalitätsansprüche voraussetzt, läuft sie auch Gefahr, letztlich auf einer rhetorischen Ebene zu verharren. Werte wie Sicherheit und Freiheit werden einander gegenübergestellt und zu einer

---

<sup>13</sup> Die verbreitete und durchaus beschönigende Rede vom Restrisiko gibt Zeugnis hiervon. Jasanoff (1991, S. 31) spricht in diesem Zusammenhang von „falscher Präzision“.



Frage der bloßen Abwägung oder „Balancierung“, die je nach normativer Ausgangsposition in die eine oder andere Richtung ausfällt.<sup>14</sup>

Eine andere Form der Praxis, um eine sich selbst reproduzierende und verstärkende Sicherheitslogik auszuhebeln, ist die *Ausübung* abstrakter Bedrohungsszenarien. Konzepte wie die LÜKEX, die sich an professionelle Akteure richten und gerade nicht nur nach Plan agieren, das Unvorhersehbare vielmehr gezielt zum Bestandteil der Übung machen, leisten genau dies: Szenarien in handlungspraktische und logistische Anforderungen zu übersetzen und die Dringlichkeit nicht nur simulierter Notfallsituationen reflexiv zurückzusetzen. „Thinking in an emergency“ (Scarry 2011) bedeutet dann gleichermaßen die epistemisch-empirische wie die ethische Dimension zu reflektieren und damit die Frage des *Was ist?*, bzw. was wir auf der Grundlage welcher Annahmen als ein Problem der Sicherheit wahrnehmen, und die Frage des *Was soll sein?*, bzw. auf welcher Grundlage wir entscheiden und handeln wollen (vgl. ebd., S. 8). Eine Katastrophenübung kann solchermaßen zu einer *Erfahrung* (Dewey 1993) werden, die dem Unbekannten und Unvorhergesehenen, das jede neue Notsituation mit sich bringt, die eingeübten und buchstäblich begriffenen Abläufe und Zusammenhänge, und damit Handlungsfähigkeit, entgegensetzen kann.

Eine Kultur der Resilienz, welche die „Selbstschutzzfähigkeit der Bevölkerung“ zu erhöhen sucht (Goersch & Werner 2011), verfolgt eine ähnliche Zielsetzung: Sie will vermitteln und einüben, was im Katastrophenfall nicht erst hergestellt werden kann (Gusy 2013). Während der Anspruch, Handlungsfähigkeit und sogar die zivilgesellschaftlichen Kräfte zu stärken (Mayer 2013), für sich genommen zu begrüßen ist, stellt sich gleichwohl die Frage, auf welche Weise dies geschieht – „top down“ oder unter Einbeziehung der Vor- und Problemstellungen der Bürger? – und in welcher Rolle staatliche Akteure sich dabei sehen: Nehmen sie das Programm als Ausstieg aus der Verantwortung oder verstehen sie sich selbst als Provider von Infrastrukturen und Koordinatoren von Kommunikationsstrukturen?

Wenn man auch von einer aktuellen *politischen* Krise der Sicherheit sprechen will, so besteht diese darin, dass der Staat sich einerseits aus der Verantwortung für die Sicherheit zurückziehen sucht, indem er die Bürger in die Regierung der Sicherheit mit einbezieht, andererseits aber auf einem Versprechen absoluter Sicherheit oder der Sicherheit als einem Grundrecht beharrt. Solche Versprechen täuschen indes vor, dass der Staat seinen Bürgern Sicherheit garantieren kann – und sie täuschen zugleich darüber hinweg, dass wir auf diese Weise selbst eine Gesellschaft der Kontrolle und der Kultur des Verdachts kreieren.

---

<sup>14</sup> Ausführlicher dazu im Kontext von Sicherheitsgesetzgebungen und m.w.V.: Krasmann (2012b).



Freilich beginnt der Ausstieg aus der Sicherheitslogik, und die ist wohl primär der Aufgabenbereich der Sozialwissenschaften, bereits mit der Reflexion ihrer epistemischen und ontologischen Voraussetzungen. Zu diesen Voraussetzungen gehören also nicht nur Wertentscheidungen, die Sicherheitsfragen stets zugrunde liegen, sondern vor allem auch die Frage, wie (Kontroll- und Sicherheits-)Diskurse und Technologien zuallererst unsere Wahrnehmung und unsere Handlungsmöglichkeiten, eben auch nicht-diskursiv, strukturieren; wie sie, mit anderen Worten, uns als Subjekte, aber auch als Objekte der Kontrolle konstituieren und das Feld politischer Artikulation, als Formen der Sichtbarkeit und der Sagbarkeit, gleichsam vorkonfigurieren.

Wenn es in diesem Sinne im Folgenden die Konstruktionen von Sicherheit eingehender zu inspizieren gilt und wir uns dabei auf die *Medien* der Herstellung von Sicherheit (oder Unsicherheit) konzentrieren, heißt das, diese umfassen nicht nur die Massenmedien, sondern auch Bevölkerungsumfragen, Sicherheitsgesetzgebung sowie entsprechende Kontrolltechnologien, die je eigene Realitäten und Formen der Sichtbarkeit hervorbringen.<sup>15</sup>

---

<sup>15</sup> Mit seinem „praxistheoretischen Ansatz“ verfolgt Christopher Daase (2012) ein ähnliches Anliegen der Analyse und gesellschaftspolitischen Implementierung einer Sicherheitskultur. Gleichwohl bleibt der Begriff der Praxis hier am Handeln von Akteuren und deren Sinn- und Bedeutungsgebungen orientiert und schließt die Frage der *Realitätsmächtigkeit* von Kontrolltechnologien aus.



## 2. Bedrohungs- und Risikowahrnehmungen in der Bevölkerung

Die öffentliche Wahrnehmung im Sinne von empirisch erhobenen Einstellungen und Wissensbeständen über Kriminalität und Strafverfolgung in der Bevölkerung einerseits und die tatsächliche Praxis der Instanzen bzw. das tatsächliche d.h. registrierte Ausmaß entsprechender Phänomene andererseits klaffen auseinander. Es ist empirisch mehrfach erwiesen, dass die allgemein verbreiteten Vermutungen über die Funktionsweise des Kriminaljustizsystems dessen Praxis – etwa in Bezug auf die Härte und Höhe der verhängten Strafen – nicht treffen (etwa Hough & Roberts 1999). Auch wird das Ausmaß von als problematisch geltenden sozialen Phänomenen, von Teenagerschwangerschaft über Sozialmissbrauch bis hin zum Ausländeranteil an der Bevölkerung regelmäßig überschätzt (exemplarisch für die diversen Probleme, die mit Ausländern assoziiert werden: Smith & Edmonston 1998).

Wie Ivan S. Sheehan (2012) zeigt, ist auch der Versuch, ein quantitatives Bild der Entwicklung von Terrorismus zu zeichnen, mit einer Reihe methodischer, theoretischer und praktischer Probleme konfrontiert. Allerdings sind derartige Versuche, über den Aufbau von globalen Datenbasen zu einer besseren Einschätzung von Bedrohungen zu kommen, für die öffentliche Diskussion nur von nachgeordneter Bedeutung. Entsprechende singuläre Ereignisse – seien es nun reale Anschläge nach terroristischer Manier oder folgenreiche Fehlalarme – halten die Vorstellung einer Bedrohung der Inneren Sicherheit präsenter als eine nach den Regeln der wissenschaftlichen Methodik entwickelte Datenbasis.

Ein weiteres Problem ist die kategoriale Differenzierung von Bedrohungen. Die diversen Erhebungen über die in der Bevölkerung als mehr oder weniger bedrohlich wahrgenommenen gesellschaftlichen Entwicklungen oder Ereignisse geben eine Ordnung vor, die nicht deckungsgleich sein muss mit der Wahrnehmung im Alltag. Diffuse Ängste und Bedrohungsgefühle erschließen sich in solchen Untersuchungen nur bedingt. Das Dilemma jeder Erhebung von Sicherheitsempfinden ist der eigentümlich paradoxe Status von Sicherheit als subjektiv empfundenem Zustand. Es handelt sich hier um eines jener Phänomene, die wie Jon Elster (1985) es nannte, „essentially by-products“ sind, d.h. sie stellen sich nur ein oder existieren nur, wenn sie nicht direkt gewollt werden. Mit der expliziten Thematisierung von Sicherheit eröffnet sich ein kognitiver Bezugsrahmen, der entlang der Differenz sicher/unsicher unterscheidet und damit ist der subjektiv zu erhebende Status von Sicherheit bereits durch die Thematisierung beeinflusst.

Methodisch stehen also entsprechende Untersuchungen vor der Schwierigkeit, indirekt einen Zustand zu messen oder zu erheben, der direkt nicht thematisiert werden sollte.





Leider ist, wie sich auch im Weiteren zeigen wird, bei der Mehrzahl der Studien zum subjektiven Sicherheitsempfinden das methodisch-theoretische Problematisierungsniveau nicht ausreichend, um dieses Problem überhaupt als solches zu identifizieren.

## 2.1 Methodische Herangehensweisen

Die Bedrohungs- und Risikowahrnehmung terroristischer Anschläge in der Bevölkerung ist seit 9/11 fester Bestandteil sozialwissenschaftlicher Sicherheitsforschung. Analog zu der Systematisierung der klassischen Kriminalitätsfurchtforschung lassen sich eine affektive (Bedrohungswahrnehmung) und eine kognitive Dimension (Risikowahrnehmung) unterscheiden, welche jeweils weiter in eine allgemeine und eine persönliche Komponente differenziert werden können (vgl. Tab. 1). Hierbei handelt es sich um rein theoretische Differenzierungen, die auf Seiten der Befragten nicht in gleicher Weise vorgenommen werden müssen. Die *Bedrohungswahrnehmung* bezieht sich auf die Angst, selbst Opfer eines terroristischen Anschlags zu werden (persönliche Dimension), bzw. die Angst, dass terroristische Anschläge verübt werden (allgemeine Dimension). Statt nach Angst wird in einigen Studien nach Sorgen (z.B. Haverkamp et al. 2013; Müller 2008), dem Bedrohungsgefühl (z.B. Bulmahn et al. 2011), der Beunruhigung (z.B. Bott & Koch-Arzberger 2012) oder der Verunsicherung (z.B. Gerhold 2009) gefragt. Die *Risikowahrnehmung*<sup>16</sup> zielt auf die Einschätzung des Risikos, der Gefahr oder der Wahrscheinlichkeit, Opfer eines terroristischen Anschlags zu werden (persönliche Dimension) bzw. dass terroristische Anschläge verübt werden (allgemeine Dimension). Ob in letzterem Fall auch eine eigene Opferwerdung impliziert wird oder nicht, ist keineswegs eindeutig.

Zuweilen erfolgt eine Kontextualisierung, indem ein bestimmter geographischer Raum (z.B. Deutschland, der eigene Wohnort), ein Zeitfenster (z.B. innerhalb der nächsten zwölf Monate) oder ein Transportbereich (z.B. Flugverkehr) als Bezugsrahmen angegeben wird. Ebenso hat es sich etabliert, die Bedrohungswahrnehmung terroristischer Anschläge nicht isoliert, sondern neben kriminalitätsbezogenen, existenziellen, gesundheitlichen und sozialen Bedrohungsfaktoren abzufragen, um auf diese Weise eine Rangfolge der größten Ängste bzw. Sorgen der Befragten erstellen zu können.

---

<sup>16</sup> Gefahr und Risiko werden hier synonym verwendet. Angesichts des Überflusses an Informationen werden Risiken zu Gefahren, wodurch sich die Unterscheidung beider Begriffe im Luhmann'schen Sinne als nicht mehr tragfähig erweist.



Tabelle 1: Beispielfragen zur Erhebung der Bedrohungs- und Risikowahrnehmung

	Bedrohungswahrnehmung	Risikowahrnehmung
allgemein	„Wie groß ist Ihre Angst, dass in Deutschland terroristische Anschläge verübt werden?“ (Lüdemann & Schlepper 2013)	„Wie groß schätzen Sie die Gefahr eines terroristischen Anschlages in Deutschland ein?“ (Lübcke & Irlenkaeuser 2006)
persönlich	„Und wie ist das rund ums Fliegen mit der Angst, Opfer eines terroristischen Anschlags zu werden?“ (Bug & Wagner 2013)	„Und für wie wahrscheinlich halten Sie es rund ums Fliegen, in den nächsten 12 Monaten Opfer eines terroristischen Anschlags zu werden?“ (Bug & Wagner 2013)

## 2.2 Zentrale Ergebnisse zur Bedrohungs- und Risikowahrnehmung

Im Folgenden werden die zentralen Ergebnisse zur Bedrohungs- und Risikowahrnehmung terroristischer Anschläge aus einschlägigen Studien dargestellt.<sup>17</sup> Es existieren überwiegend quantitative Untersuchungen, wobei die Bedrohungswahrnehmung häufiger Gegenstand der Forschung ist als die Risikowahrnehmung. Aufgrund des breiten Akteursspektrums – so ist die Sicherheitsforschung nicht alleinige Domäne wissenschaftlicher Disziplinen, sondern es beteiligen sich auch mediale und wirtschaftliche Akteure – und der damit verbundenen Vielzahl an vorliegenden Ergebnissen<sup>18</sup>, wird der Schwerpunkt auf sozialwissenschaftliche Untersuchungen gelegt und ein Überblick über aktuelle und häufig rezipierte Befunde gegeben<sup>19</sup>.

### 2.2.1 Allgemeine Bedrohungswahrnehmung terroristischer Anschläge

Es gibt verschiedene Indikatoren zur Erhebung der allgemeinen Bedrohungswahrnehmung, die teilweise zu erheblich divergierenden Befunden führen. Besonders gebräuchlich sind (1) Angst vor terroristischen Anschlägen, (2) Sorge vor terroristischen Anschlägen, (3) Bedrohungsgefühl durch terroristische Anschläge, (4) Beunruhigung durch Terrorismus oder (5) Verunsicherung durch Terrorismus. (1) Angst vor terroristischen Anschlägen.

<sup>17</sup> Sofern nicht anders angegeben, erstrecken sich die Untersuchungen auf das gesamte Bundesgebiet.

<sup>18</sup> Vor allem die Fülle an von Printmedien und Nachrichtensendern durchgeführten Umfragen ist kaum überschaubar.

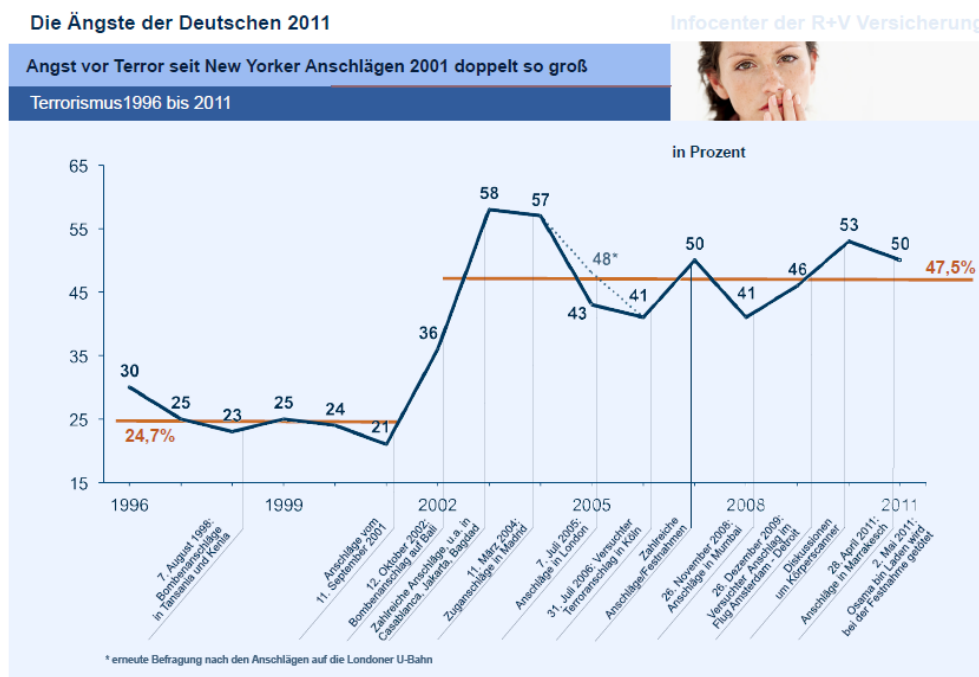
<sup>19</sup> Vernachlässigt wird die Darstellung von Befunden, deren Zustandekommen nicht detailliert nachvollziehbar ist, weil keine oder nur unzureichende Informationen über die Operationalisierung der Variablen vorliegen.



Die wohl bekannteste Untersuchung ist die seit 1991 jährlich durchgeführte Erhebung der „Ängste der Deutschen“ durch die R+V-Versicherung (face-to-face Befragung). Da sie eine der wenigen Langzeitstudien ist, die die Entwicklung der allgemeinen Bedrohungswahrnehmung terroristischer Anschläge in der Bevölkerung über einen längeren Zeitraum aufzeigen können, wird ihr sowohl in der Sicherheitsforschung als auch politisch und medial Beachtung geschenkt.

Die Befragten werden gebeten, für 17 verschiedene Ängste (Stand 2012; Infocenter der R+V Versicherung 2012a) auf einer Skala von 1 (*keine Angst*) bis 7 (*sehr große Angst*) jeweils anzugeben, wie groß ihre Angst davor ist. Die drei höchsten Ausprägungen werden als große Angst zusammengefasst und gehen in das Ranking der *größten Ängste* ein. In Bezug auf Terrorismus wird nach der Angst davor gefragt, dass *terroristische Vereinigungen Anschläge verüben* (ebd., S. 2; Herv. d. Verf.). Es findet keine räumliche Kontextualisierung statt, so dass man nicht weiß, ob sich die Befragten in ihrer Antwort überhaupt auf einen – und wenn ja, auf welchen – konkreten Ort beziehen.

Abbildung 1: Entwicklung der Angst vor terroristischen Anschlägen von 1996 bis 2011



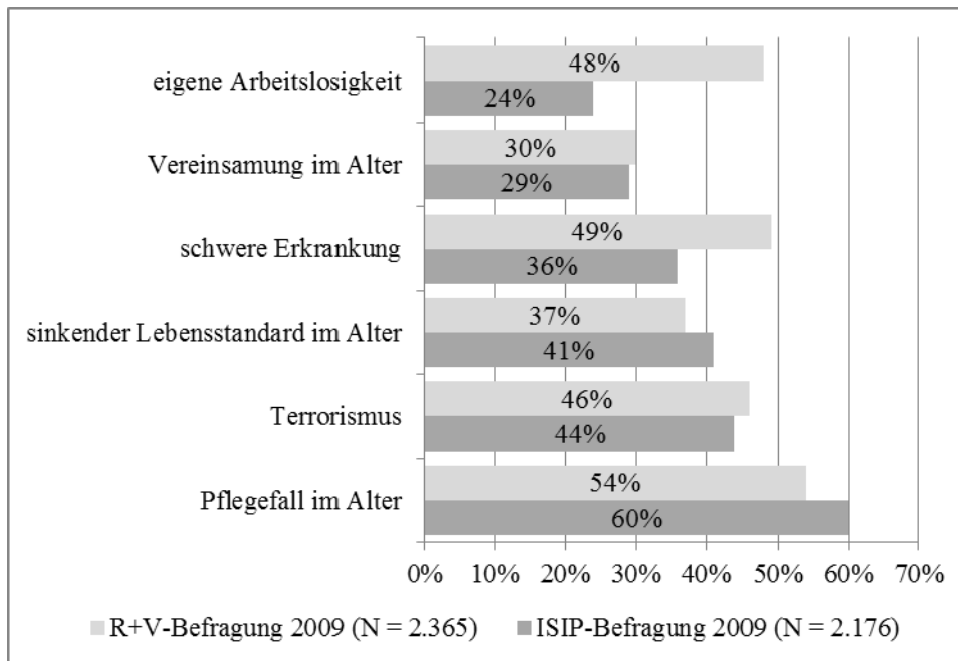
Quelle: Infocenter der R+V Versicherung 2011

Die Langzeitentwicklung zeigt, dass der Anteil der Personen, der große Angst vor terroristischen Anschlägen hat, durchaus Schwankungen unterliegt, aber sich seit 9/11 nahezu verdoppelt hat (vgl. Abb. 1). In den Jahren 2003, 2004, 2007 und 2011 äußerten jeweils mindestens die Hälfte der Befragten große Angst vor terroristischen



Anschlägen und sie rangierte unter den sieben größten Ängsten. Bei der diesjährigen Befragung nahm die Angst vor Terrorismus ebenfalls den siebten Platz ein und es gaben 43 Prozent der Befragten an, *große Angst* vor Terrorismus zu haben (Infocenter der R+V Versicherung 2013).

Abbildung 2: Vergleich R+V- und ISIP-Befragung 2009 – Häufigkeit der Antworten auf die Frage nach „großer Angst“



Quellen: R+V: Infocenter der R+V Versicherung 2009; ISIP-Projekt: eigene Berechnungen 2009

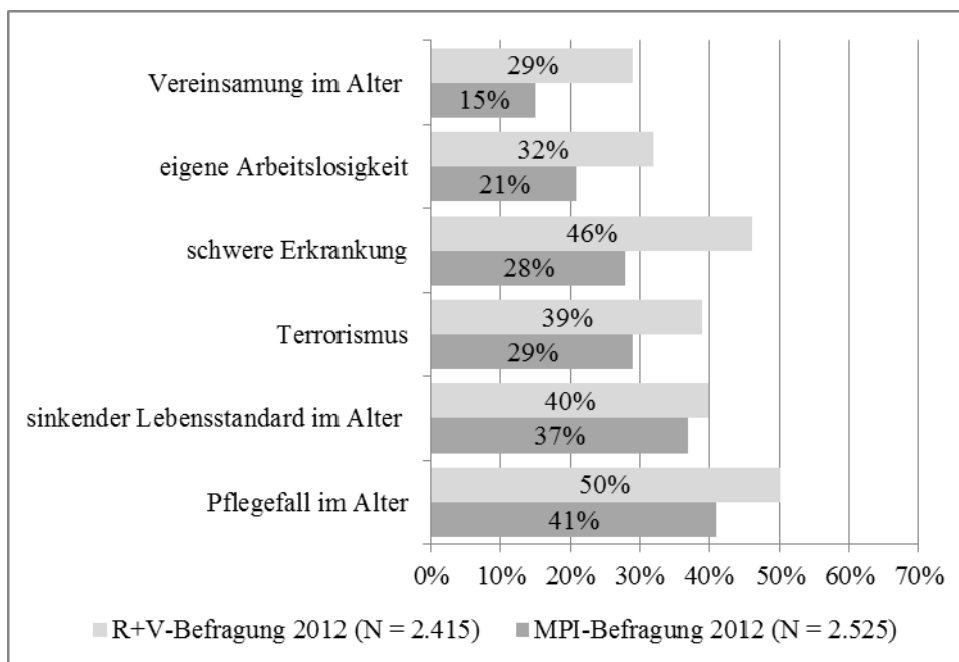
Vergleicht man die Ergebnisse der Studie der R+V Versicherung mit Befunden anderer Untersuchungen, die identische bzw. sehr ähnliche Fragen gestellt haben, so treten teilweise große Diskrepanzen auf. Die 2009 am Institut für Sicherheits- und Präventionsforschung (ISIP) durchgeführte telefonische Befragung im Rahmen des DFG-Projektes „Der überwachte Bürger zwischen Apathie und Protest“ zum Thema „Sicherheit der Bürger“ enthielt ebenfalls einen Fragenkomplex mit verschiedenen Ängsten. Die genaue Fragestellung zur Terrorismusfurcht lautete: *Wie groß ist Ihre Angst, dass in Deutschland terroristische Anschläge verübt werden.* Als Antwortmöglichkeiten wurde eine Skala von 1 (*gar keine Angst*) bis 4 (*sehr große Angst*) vorgegeben. Die in beiden Untersuchungen abgefragten Ängste sind in Abbildung 2 dargestellt. Die Prozentzahlen geben den Anteil der Befragten an, der *große Angst* vor den jeweiligen Ereignissen äußerte.<sup>20</sup> Zwar ähneln sich die Werte teilweise – z.B. hinsichtlich der

<sup>20</sup> Im ISIP-Projekt wurden die Antwortmöglichkeiten 3 und 4 zu *großer Angst* zusammengefasst, in der R+V-Studie die Antwortausprägungen 5 bis 7. Aufgrund dieser unterschiedlichen Skalierung ist die Vergleichbarkeit eingeschränkt.



Angst vor Vereinsamung im Alter sowie vor terroristischen Anschlägen und diese nimmt einen durchaus vorderen Platz ein. Erhebliche Unterschiede lassen sich jedoch z.B. in Bezug auf die Angst vor eigener Arbeitslosigkeit feststellen. Große Angst davor, arbeitslos zu werden, äußerten in der R+V-Studie doppelt so viele Personen wie in der Befragung im Rahmen des ISIP-Projektes. Auch große Angst vor einer schweren Erkrankung wurde in der R+V-Befragung deutlich häufiger berichtet. Je nach Studie variieren die Ergebnisse also mitunter stark.

Abbildung 3: Vergleich R+V- und MPI-Befragung 2012 – Häufigkeit der Antworten auf die Frage nach „großen Sorgen“



Quellen: R+V: Infocenter der R+V Versicherung 2012b; MPI: Haverkamp et al. 2013

## (2) Sorge vor terroristischen Anschlägen

Dass es einen deutlichen Unterschied ausmachen kann, wenn nicht nach Angst, sondern Sorge gefragt wird, zeigt sich, wenn man die Befunde der R+V-Befragung 2012 mit denen einer telefonischen Befragung des Max-Planck-Instituts (MPI) im Rahmen des BMBF-Projektes „Barometer Sicherheit in Deutschland“ (BaSiD) zum Thema „Sicherheitsempfinden und Lebensqualität in Deutschland“ aus demselben Jahr vergleicht (vgl. Abb. 3). In dieser Studie wurde in einer Itematterie unter anderem nach *Sorgen vor terroristischen Anschlägen* gefragt und es stand eine Antwortskala von 0 (*keine Sorgen*) bis 10 (*sehr besorgt*) zur Verfügung (Haverkamp et al. 2013).



Abbildung 3 zeigt den Anteil der Befragten, der sich *große Sorgen* vor den jeweiligen Ereignissen macht.<sup>21</sup>

Nicht nur lässt sich feststellen, dass in der R+V-Studie 2012 sieben Prozent weniger als noch 2009 *große Ängste* vor terroristischen Anschlägen äußerten, diese also rückläufig sind, sondern auch, dass der Anteil der Personen mit *großen Sorgen* vor terroristischen Anschlägen in der MPI-Befragung weitere zehn Prozentpunkte darunter liegt und weniger als ein Drittel umfasst. Noch stärker ist die Angst davor zurückgegangen, im Alter ein Pflegefall zu werden (von 2009 60 Prozent auf 2012 41 Prozent), wobei sich das Ergebnis der MPI-Befragung abermals weit darunter bewegt. Wird also die Sorge als Indikator eingesetzt, fällt die allgemeine Bedrohungswahrnehmung geringer aus als bei der Frage nach der Angst.

Im Rahmen des sozio-ökonomischen Panels (SOEP) wird ebenfalls ein „Sorgenkatalog“ (Müller 2008, S. 545) erhoben, in den 2007 erstmalig die *Sorge über den globalen Terrorismus* aufgenommen wurde (Online-Erhebung; N = 1.057). Für insgesamt zwölf „Gebiete“, die von der eigenen Gesundheit bis zu den Folgen der EU-Erweiterung reichen, wird gefragt *Wie ist es mit den folgenden Gebieten – machen Sie sich da Sorgen?* (ebd., S. 545; Herv. d. Verf.). 2007 und 2011 gab jeweils ca. ein Drittel der Befragten an, sich *große Sorgen* über den globalen Terrorismus zu machen, was dem Ergebnis der MPI-Befragung nahe kommt.

### (3) Bedrohungsgefühl durch terroristische Anschläge

In einer regelmäßig seit 1996 durchgeführten Bevölkerungsbefragung des Sozialwissenschaftlichen Instituts der Bundeswehr, die zum Thema „Sicherheits- und verteidigungspolitisches Meinungsklima in der Bundesrepublik Deutschland“ durchgeführt wird (2010: N = 3.026; computergestützte persönliche Interviews), wurde nicht die Angst oder Sorge, sondern das *Bedrohungsgefühl* erhoben (Bulmahn et al. 2011). Innerhalb einer Itematterie mit 19 weiteren potenziellen Bedrohungsfaktoren wurde danach gefragt, inwieweit sich die Befragten durch *Terroranschläge in Deutschland* bedroht fühlen. 2010 gaben zwölf Prozent an, dass sie sich dadurch stark bedroht<sup>22</sup> fühlen (Bulmahn 2011, S. 92), also weitaus weniger als in den bereits erwähnten Untersuchungen. In der im Jahr zuvor durchgeführten Befragung waren es 15 Prozent der Befragten (Bulmahn 2010, S. 9), so dass sich in dieser Untersuchung eine tendenziell rückläufige Entwicklung abzeichnet.

---

<sup>21</sup> In der MPI-Befragung wurden die Werte 7 bis 10 zu großen Sorgen zusammengefasst.

<sup>22</sup> Den Befragten stand zur Beantwortung eine fünfstufige Skala von *sehr stark bedroht* bis *gar nicht bedroht* zur Verfügung, wobei in der Ergebnisdarstellung die Kategorien *sehr stark bedroht* und *stark bedroht* zusammengefasst wurden.



#### (4) Beunruhigung durch Terrorismus

Auf deutlich höherem Niveau liegt die allgemeine Bedrohungswahrnehmung in einer 2008/2009 in Hessen durchgeführten telefonischen Befragung (N = 2.211) der Kriminalistisch-Kriminologischen Forschungsstelle der hessischen Polizei zur Kriminalitäts- und Terrorismusfurcht (Bott & Koch-Arzberger 2012). In dieser Untersuchung wurde nach der *Beunruhigung* durch acht verschiedene Themen gefragt und 47 Prozent äußerten, dass das Thema *Terrorismus* sie *sehr beunruhige* (vgl. ebd., S. 136). Die *allgemeine wirtschaftliche Situation* führte das Ranking der sehr beunruhigenden Themen an und lag nur einen Prozentpunkt über dem Terrorismus.

Im Eurobarometer Spezial 273, das 2006 durchgeführt wurde, wurde den Befragten (N = 1.504 im deutschen Survey; face-to-face Interviews) eine Liste mit 17 Themen vorgelegt und sie sollten angeben, welche *drei Themen sie im Moment im Hinblick auf Deutschland am meisten beunruhigen* (Europäische Kommission 2007a, S. 43). *Terrorismus* wurde von 27 Prozent der Befragten genannt und lag damit auf einem Platz im Mittelfeld (Europäische Kommission 2007b, S. 5).

Zwar sind die beiden Untersuchungen aus diversen Gründen (Erhebungszeitpunkt, Grundgesamtheit, Erhebungsmethode, genaue Frageformulierung) nur bedingt vergleichbar, dennoch klaffen die Ergebnisse sehr weit auseinander.

#### (5) Verunsicherung durch Terrorismus

Schließlich lässt sich auch die *Verunsicherung* durch Terrorismus als Indikator für die allgemeine Bedrohungswahrnehmung betrachten. In einer telefonischen Befragung (N = 998) im Rahmen des Projektes „Selbstverantwortliches Lernen in der Auseinandersetzung mit Unsicherheit und Risiko unter den Bedingungen des globalen Wandels“ zu den Bereichen „Arbeit, Gesundheit, Finanzen und Terrorismus“ sollten die Befragten auf einer fünfstufigen Skala von *trifft überhaupt nicht zu* bis *trifft voll und ganz zu* bewerten, inwiefern folgende Aussage auf sie zutrifft: *Ich fühle mich durch den Terrorismus in Europa verunsichert* (Gerhold 2009, S. 180; Herv. d. Verf.). Hohe Zustimmungswerte wurden von ca. einem Viertel der Befragten gegeben. Dabei weist Gerhold (ebd.) darauf hin, dass zum Befragungszeitpunkt die Anschläge auf den Bahnverkehr in Madrid 2004 und London 2005 aktuell waren, so dass davon auszugehen ist, dass sich deren Präsenz auf das Antwortverhalten auswirkte.

Insgesamt lassen diese Ergebnisse kaum verallgemeinerbare Aussagen über die allgemeine Bedrohungswahrnehmung zu, da diese zum einen je nach Befragungszeitpunkt unterschiedlich ausfällt. Zum anderen variiert sie aber auch mit den verwendeten Indikatoren. Je nachdem, ob nach Ängsten, Sorgen, Bedrohungsgefühl, Beunruhigung oder Verunsicherung gefragt wird, werden teilweise erheblich divergierende Befunde erzielt, und der Anteil der Befragten mit einer hohen allgemeinen Bedrohungswahr-



nehmung weist eine beachtliche Spannweite von zwölf Prozent bis fünfzig Prozent auf.

### 2.2.2 Persönliche Bedrohungswahrnehmung terroristischer Anschläge

Die persönliche Dimension der Bedrohungswahrnehmung ist bislang weitaus seltener Gegenstand der Forschung als die allgemeine und wird auch noch nicht systematisch erhoben, so dass über die zeitliche Entwicklung keine Erkenntnisse vorliegen. Dass sie noch keinen Eingang in eine Langzeitstudie gefunden hat, lässt sich indes schon als erstes Indiz für ihre marginale Bedeutung betrachten.

In einer forsa-Umfrage aus dem Jahr 2007 mit dem Titel „Öffentliche Sicherheit: Staatsmonopol oder marktfähiges Gut?“ (N = 1.505; computergestützte Telefoninterviews), die von der Alfred-Herrhausen Gesellschaft (2007) in Auftrag gegeben wurde, gab knapp ein Viertel der Befragten an, *große Angst* davor zu haben, *Opfer eines Terroranschlags* zu werden.

In einer telefonischen Befragung der Universität der Bundeswehr München im Rahmen des BMBF-Projektes „Sicherheit im öffentlichen Raum“ (SIRA)<sup>23</sup> wurde nicht generell, sondern spezifisch für den Kontext des Flugverkehrs („rund ums Fliegen“) nach der *Angst* gefragt, *Opfer eines terroristischen Anschlags* zu werden (Bug & Wagner 2013). In dieser Untersuchung wurde nicht die Intensität der Angst, sondern nur deren Vorhandensein mittels der Antwortmöglichkeiten *ja*, *nein* und *weiß nicht* erhoben. Zwölf Prozent der Befragten gaben an, Angst vor der eigenen Opferwerdung zu haben.<sup>24</sup> Im BaSiD-Projekt ergab sich ein ähnlicher Befund. Zehn Prozent der Befragten äußerten große *Sorgen*, *Opfer eines terroristischen Anschlags* zu werden (Haverkamp et al. 2013).

In einer Studie der Uni Kiel zur „Bedrohungsperezeption durch das Phänomen des Terrorismus und Bewertung der Gegenmaßnahmen der BR Deutschland“ (Lübcke & Irlenkaeuser 2006), die 2006 anhand einer telefonischen Befragung von 817 Personen durchgeführt wurde, fällt die persönliche Bedrohungswahrnehmung noch geringer aus. Es wurde danach gefragt, wie *sicher sie sich in ihrem Wohnort vor einem terroristischen Anschlag fühlen*. Lediglich fünf Prozent der Befragten gaben an, sich unsicher zu fühlen (vgl. ebd., S. 3). Dass die in dieser Studie selten berichtete Unsicherheit darauf zurückzuführen ist, dass nach dem Sicherheitsgefühl und nicht nach der Angst oder Sorge gefragt und der eigene Wohnort als Referenzpunkt angegeben wurde,

---

<sup>23</sup> Bei der von Mitte November bis Mitte Dezember 2011 durchgeführten telefonischen Befragung handelt es sich um eine repräsentative Stichprobe von 1.257 in Deutschland lebenden Personen (vgl. Bug & Münch 2012, S. 151)

<sup>24</sup> Die Berechnung bezieht sich nur auf Flugpassagiere (N = 799).





erscheint äußerst plausibel. So liegen Erkenntnisse vor, dass das Sicherheitsgefühl am eigenen Wohnort hoch ist. In der oben genannten forsa-Umfrage gaben fast neunzig Prozent der Befragten an, dass sie glauben, in ihrem Wohnort sicher leben zu können. (Alfred-Herrhausen-Gesellschaft 2007). In diese Richtung deuten auch die Ergebnisse der Untersuchung der Kriminalistisch-Kriminologischen Forschungsstelle der hessischen Polizei. 82 Prozent der Befragten schätzten die Wahrscheinlichkeit eines terroristischen Anschlags im eigenen Wohngebiet auf höchstens zehn Prozent (vgl. Bott & Koch-Arzberger 2012, S. 138).

Auch hinsichtlich der persönlichen Bedrohungswahrnehmung ergeben sich also, je nachdem ob nach Ängsten, Sorgen oder dem Sicherheitsgefühl am eigenen Wohnort gefragt wird, unterschiedliche Ergebnisse. Insgesamt bewegen sie sich auf einem eher geringen Niveau und es deutet sich damit als Grundtendenz an, dass sich eine hohe *persönliche* Bedrohungswahrnehmung als weniger verbreitet erweist als eine hohe *allgemeine* Bedrohungswahrnehmung. Nur ein eher kleiner Teil der Bevölkerung hat große Angst oder Sorge, selbst Opfer eines terroristischen Anschlags zu werden.

### 2.2.3 Risikowahrnehmung terroristischer Anschläge

Zur Risikowahrnehmung liegen bislang weniger Erkenntnisse vor. Daher erübrigt sich eine getrennte Betrachtung der allgemeinen und persönlichen Dimension, zumal letztere kaum erhoben wird. Ebenso ergeben sich nur in geringem Umfang und bedingt Vergleichsmöglichkeiten zwischen verschiedenen Untersuchungen. Diese begrenzen sich auf (1) die Risikowahrnehmung in verschiedenen Transportbereichen sowie (2) die Risikowahrnehmung in diachroner Perspektive.

Einen allgemeinen Anhaltspunkt über das in der Bevölkerung angenommene Risiko terroristischer Anschläge lässt sich der Studie der Uni Kiel (Lübcke & Irlenkaeuser 2006, S. 3) entnehmen, in der nicht der Begriff des Risikos, sondern der der Gefahr verwendet wurde. Es wurde danach gefragt, wie groß die Befragten die *Gefahr eines terroristischen Anschlags in Deutschland* (auf einer vierstufigen Skala von *gar keine* bis *sehr hoch*) einschätzen. Ein Drittel schätzte die Gefahr *hoch* und acht Prozent sogar als *sehr hoch* ein. Eine *geringe* Gefahr wurde von über der Hälfte der Befragten perzipiert und ca. drei Prozent vermuteten *gar keine* Gefahr.

#### (1) Risikowahrnehmung in verschiedenen Transportbereichen

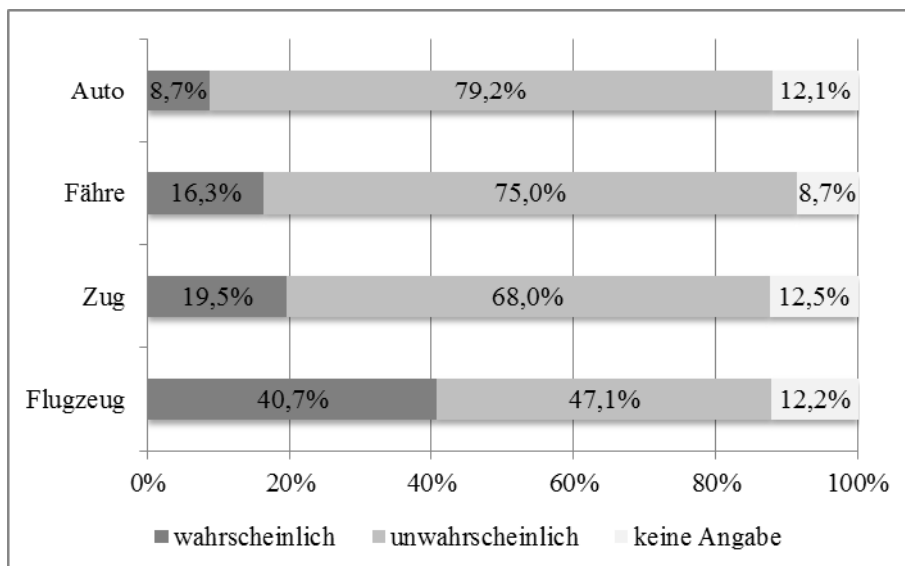
Daneben existieren Forschungsergebnisse zur Risikowahrnehmung terroristischer Anschläge im Kontext bestimmter Transportbereiche. Eine Beurteilung der Anschlagswahrscheinlichkeit auf verschiedene Verkehrsmittel wurde in einer Befragung von 766 Fährpassagieren im Ostsee-Verkehr zwischen Deutschland und Skandinavien erhoben. Diese wurde im Sommer 2012 im Rahmen des BMBF-Projektes „Verbesserung der



Sicherheit von Personen in der Fährschifffahrt“ (VESPER+) durchgeführt.<sup>25</sup> Die Passagiere wurden danach gefragt, für wie wahrscheinlich sie das *Eintreten einer Gefahrensituation verursacht durch einen Anschlag auf dem Weg von Deutschland nach Skandinavien* für verschiedene Verkehrsmittel halten (vgl. Abb. 4).<sup>26</sup> Den Befragten stand für die Beantwortung eine vierstufige Skala von *sehr wahrscheinlich* bis *sehr unwahrscheinlich* zur Verfügung.

Auf dem ersten Platz rangiert das Flugzeug – mit deutlichem Abstand. Etwa vierzig Prozent der Befragten hielt einen Anschlag auf ein Flugzeug für wahrscheinlich, auf einen Zug hingegen lediglich ein Fünftel und auf eine Fähre sogar nur ein Sechstel. An letzter Stelle steht das Auto, auf das knapp neun Prozent einen Anschlag für wahrscheinlich einschätzten.

Abbildung 4: Perzipierte Anschlagswahrscheinlichkeit auf verschiedene Verkehrsmittel



Quelle: VESPER+-Projekt, eigene Berechnungen 2012<sup>27</sup>, N = 766

Geht man davon aus, dass tatsächlich stattgefundenere Ereignisse die Risikowahrnehmung beeinflussen, überrascht der Befund, dass die Unterschiede zwischen Bahn- und Fährverkehr so gering sowie zwischen Bahn- und Flugverkehr so hoch ausfallen.

<sup>25</sup> Die Befragung erfolgte im Rahmen des Teilprojektes „Gesellschaftliche und wirtschaftliche Auswirkungen neuer Sicherheitsmaßnahmen im Fährverkehr“. Im Mittelpunkt steht die Untersuchung der Akzeptanz von Sicherheitsmaßnahmen im Fährverkehr, die im Zuge der Terroranschläge von 9/11 durch den ISPS-Code sowie die EU-Gesamthafenrichtlinie erhöht wurden.

<sup>26</sup> Diese Frage wurde nicht nur für die mögliche Ursache *Anschlag* gestellt, sondern auch für *menschliches Versagen*, *widrige Wetterbedingungen* sowie *technische Probleme*.

<sup>27</sup> Die Anteile *sehr* und *eher wahrscheinlich* sowie *eher* und *sehr unwahrscheinlich* wurden zusammengefasst.



Die Terroranschläge auf den Bahnverkehr in Madrid 2004 und London 2005 scheinen (im Unterschied zu 9/11) keinen entsprechenden Effekt gehabt zu haben. Welche Abwägungen die Befragten treffen, lässt sich anhand der Ergebnisse dieser Befragung nicht ergründen. Eine Erklärung liefert jedoch die Studie von Bonß und Wagner (vgl. 2012, S. 46), die im Rahmen des SIRA-Projektes qualitative Interviews mit Flugpassagieren geführt haben. Demnach herrscht die Auffassung vor, dass im Bahnverkehr weniger passiert, wobei aber auch die Folgen eines terroristischen Anschlags oder Unfalls als weniger gravierend eingeschätzt werden. Als eigentlichen Ursprung dieser rein rational nicht nachvollziehbaren Beurteilung betrachten Bonß und Wagner, dass das Fliegen letztlich für den Menschen fremd und unheimlich sei (vgl. ebd., S. 46), es also zu einer Konfundierung der Risikowahrnehmung mit der menschlichen Urangst vor dem Fliegen komme.

In der telefonischen Befragung des SIRA-Projektes wurde die Frage gestellt, für wie wahrscheinlich es die Befragten halten, *in den nächsten zwölf Monaten Opfer eines terroristischen Anschlags* im Kontext des zivilen Luftverkehrs zu werden (vgl. Bug & Wagner 2013). Lediglich 4,2 Prozent hielten dies für sehr oder eher wahrscheinlich. Das Anschlagrisiko wurde in dieser Untersuchung also von einer sehr großen Mehrheit als überaus gering eingeschätzt. Dies könnte zum einen mit dem vergleichsweise schmalen Zeitfenster von zwölf Monaten sowie zusätzlich der eigenen Betroffenheit zusammenhängen, zum anderen aber auch damit, dass Flugreisen für die meisten Menschen ein ziemlich seltenes Ereignis darstellen.

## (2) Risikowahrnehmung in diachroner Perspektive

Auch im Rahmen des BMBF-Projektes „Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme“ (APFeL) wurde 2010 eine Befragung durchgeführt, in der die Risikowahrnehmung erhoben wurde (Feldes et al. 2013). Die im Warte- und Boardingbereich des Flughafens Hannover schriftlich befragten Flugpassagiere (N = 1.400) sollten eine Einschätzung der *allgemeinen Sicherheitslage in Deutschland* abgeben und wurden danach gefragt, ob sie der Meinung sind, dass die *Gefahr, Opfer eines terroristischen Anschlags zu werden, heute größer als vor dem 11. September 2001* sei. Zur Beantwortung wurde eine fünfstufige Skala von *trifft gar nicht zu* bis *trifft voll und ganz zu* vorgegeben, welche anschließend in die Kategorien *zustimmend*, *ablehnend* und *unentschlossen* zusammengefasst wurden (ebd., S. 18). Knapp ein Drittel (30,9 Prozent) stimmte dieser Aussage zu, während ihr jeweils etwas mehr als ein Drittel unentschlossen (34 Prozent) oder ablehnend (34,9 Prozent) gegenüberstanden. Dieselbe Frage wurde nochmals für einen kürzeren Referenzzeitraum gestellt. Dass die *Gefahr, Opfer eines terroristischen Anschlags zu werden, heute größer als vor zwei Jahren* sei, entsprach nur mehr der Ansicht von knapp einem Viertel (24,1 Prozent) der Befragten, während jeweils fast vierzig Prozent unentschlossen (37 Prozent) oder gegenteiliger Meinung



(38,6 Prozent) waren. Die Mehrheit ist also nicht davon überzeugt, dass die Gefahr terroristischer Anschläge seit 9/11 oder in den vergangenen zwei Jahren zugenommen hat. Vergleicht man die beiden Ergebnisse, so ist die Risikowahrnehmung der Befragten in jüngster Zeit tendenziell rückläufig. Unklar bleibt allerdings, ob die Befragten die Gefahr der eigenen Opferwerdung oder einer beliebigen Person beurteilten.

Eine gegenteilige Entwicklungsrichtung legen die Ergebnisse des Sicherheitsreports 2011 nahe, welcher von T-Systems in Auftrag gegeben und vom Centrum für Strategie und Höhere Führung sowie dem Institut für Demoskopie Allensbach durchgeführt wurde (Deutsche Telekom & T-Systems 2011). Darin wurden sowohl 1.715 Bundesbürger als auch 330 Entscheidungsträger aus Wirtschaft und Politik zum Thema „Sicherheit in Deutschland“ in persönlichen mündlichen Interviews befragt und die Ergebnisse einander gegenüber gestellt. Über zwei Drittel (36 Prozent) der befragten Bürger, aber lediglich 14 Prozent der Entscheidungsträger gaben an, dass sie der Meinung sind, dass *Terroranschläge ein großes Risiko für die Menschen in Deutschland* darstellen. Während 44 Prozent der befragten Bürger der Meinung waren, dass das Risiko terroristischer Anschläge in Deutschland in Zukunft zunehmen wird,<sup>28</sup> waren nur acht Prozent der Entscheidungsträger dieser Ansicht. Allerdings wurden die Entscheidungsträger danach gefragt, welche *Risiken in Zukunft besonders stark zunehmen* werden. Zudem wurden ihnen keine Risiken vorgegeben, sondern sie konnten offen antworten. Den Bürgern hingegen wurden Karten und Bildblätter vorgelegt und sie sollten 18 Gefahren bzw. Risiken den Kategorien *wird zunehmen, geringer werden* und *da wird sich nicht viel ändern* zuordnen (vgl. Deutsche Telekom & T-Systems 2011, S. 16). Dass der Anteil der befragten Bürger, der eine Zunahme des Risikos terroristischer Anschläge perzipierte, derart höher ausfällt als der Entscheidungsträger, wird in erheblichem Maße auf die Unterschiede in der Frageformulierung und -technik zurückzuführen sein.<sup>29</sup> Der Schritt, aus diesem Befund ein steigendes Schutzinteresse der Bürger vor Terrorismus abzuleiten, auf welches die Politik reagieren muss, ist nicht weit. In der oben erwähnten forsa-Umfrage wurden die befragten Bürger offen nach den wichtigsten Problemen in Deutschland gefragt. Lediglich von sieben Prozent wurde die *Terrorismusbekämpfung* genannt (Alfred-Herrhausen-Gesellschaft 2007). Wird Terrorismus also nicht als Antwortkategorie vorgegeben, wird er auch nur von einer kleinen Gruppe der Befragten als Problem thematisiert.

---

<sup>28</sup> In der Befragung der Kriminalistisch-Kriminologischen Forschungsstelle der hessischen Polizei waren sogar 67 Prozent der Befragten der Meinung, dass die terroristische Bedrohung zukünftig weiter zunehmen wird (Bott & Koch-Arzberger 2012, S. 140).

<sup>29</sup> Auf die nicht direkte Vergleichbarkeit wird in dem Report hingewiesen (vgl. Deutsche Telekom & T-Systems 2011, S. 15).



Dass die in politischen Diskursen vorgenommene Reihung von Gefahren nach Graden der Bedrohlichkeit nicht immer in Übereinstimmung mit der Wahrnehmung der Bevölkerung oder des Laienpublikums ist, zeigt sich ebenfalls in repräsentativen Studien der EU wie dem „Special Eurobarometer 371“ zur Sicherheitslage (2011). So wird beispielsweise die Wirtschafts- und Finanzkrise als ein viel größeres Problem wahrgenommen als die Bedrohung durch Terrorismus oder Kriminalität. Zudem ergeben sich länderspezifische Differenzen, wie aus Tabelle 2 hervorgeht.

Tabelle 2: Eurobarometer Survey 2011 zur Sicherheitslage

QC 1 What do you think are the most important challenges to the security of (NATIONALITY) citizens at the moment?

	Economic and financial crises	Terrorism	Poverty	Organised Crime	Corruption	Illegal immigration	Petty crime	Natural disasters	Environmental issues / Climate change	Cybercrime	Nuclear disasters	Insecurity of EU borders	Religious extremism	Civil wars and wars	Other (SPONTANEOUS)	Don't know
EU27	33%	26%	24%	22%	18%	13%	13%	11%	11%	10%	8%	6%	6%	4%	0%	8%
BE	32%	20%	27%	15%	8%	23%	31%	11%	16%	10%	9%	7%	11%	3%	12%	2%
BG	48%	4%	60%	23%	24%	1%	26%	10%	4%	0%	2%	1%	2%	1%	19%	2%
CZ	38%	14%	16%	39%	38%	10%	8%	22%	12%	16%	8%	6%	4%	5%	3%	4%
DK	30%	55%	5%	19%	2%	9%	6%	5%	19%	4%	4%	5%	11%	5%	21%	4%
DE	28%	34%	10%	32%	14%	8%	0%	12%	20%	27%	10%	7%	10%	5%	6%	4%
EE	22%	9%	17%	9%	11%	3%	12%	5%	6%	9%	3%	12%	1%	4%	19%	14%
IE	10%	10%	30%	45%	25%	8%	17%	5%	9%	6%	4%	2%	1%	2%	5%	3%
EL	56%	7%	50%	13%	39%	28%	15%	6%	7%	2%	4%	10%	1%	3%	4%	0%
ES	57%	38%	35%	11%	37%	16%	7%	10%	7%	4%	5%	3%	4%	4%	2%	2%
FR	15%	16%	20%	7%	7%	10%	31%	7%	8%	4%	7%	3%	7%	3%	26%	19%
IT	44%	26%	18%	31%	19%	24%	7%	13%	13%	8%	10%	8%	5%	9%	2%	2%
CY	54%	6%	15%	20%	21%	55%	15%	5%	7%	7%	1%	0%	1%	1%	26%	
LV	27%	2%	41%	13%	28%	2%	23%	3%	4%	2%	1%	2%	0%	2%	5%	16%
LT	41%	5%	41%	25%	42%	4%	17%	9%	6%	7%	6%	2%	0%	2%	8%	6%
HU	16%	4%	10%	13%	5%	11%	37%	6%	9%	4%	7%	6%	1%	1%	21%	11%
HU	52%	5%	51%	20%	27%	4%	9%	20%	16%	3%	4%	3%	1%	1%	8%	2%
MT	27%	6%	15%	20%	27%	38%	12%	5%	12%	9%	1%	5%	3%	5%	9%	10%
NL	22%	26%	14%	23%	7%	7%	31%	8%	20%	22%	6%	6%	15%	3%	26%	4%
AT	40%	11%	20%	39%	9%	23%	15%	20%	21%	16%	14%	19%	6%	3%	3%	4%
PL	22%	9%	21%	13%	11%	1%	7%	16%	4%	3%	2%	1%	1%	4%	6%	27%
PT	41%	9%	42%	24%	30%	6%	11%	7%	6%	3%	4%	7%	2%	4%	2%	7%
RO	41%	14%	55%	14%	56%	2%	4%	19%	9%	4%	6%	3%	1%	5%	2%	4%
SI	46%	3%	30%	31%	47%	2%	6%	17%	15%	4%	3%	1%	2%	1%	9%	3%
SK	40%	11%	36%	24%	31%	3%	20%	46%	14%	5%	9%	3%	1%	3%	2%	1%
FI	27%	16%	11%	22%	2%	12%	10%	11%	14%	0%	15%	6%	2%	4%	27%	0%
SE	17%	30%	4%	23%	3%	3%	5%	7%	21%	6%	9%	1%	6%	3%	27%	9%
UK	24%	47%	14%	25%	6%	23%	9%	3%	7%	11%	2%	8%	10%	3%	6%	9%

Legend: Open/Umprompted question

Highest percentage per country      Lowest percentage per country  
Highest percentage per item      Lowest percentage per item

Quelle: Europäische Kommission 2011, S. 21

In den Dokumenten des Rats der Europäischen Union zur Strategie der inneren Sicherheit der Europäischen Union: „Hin zu einem europäischen Sicherheitsmodell“ kommen wirtschaftliche Krisen und Stabilität des Finanzsektors als Bedrohung gar nicht vor. Hier zeigt sich, dass politische und gesellschaftliche Wahrnehmungen in Bezug auf Sicherheitsprobleme nicht immer deckungsgleich sein müssen.

Überdies hängen entsprechende Bedrohungswahrnehmungen stark von tagespolitischen Konjunktoren ab. So ist etwa der höchste Wert für Terrorismus für Dänemark erhoben worden, ein Land, das mit terroristischen Anschlägen bisher nicht konfrontiert war. Allerdings dürfte hier der sogenannte „Karikaturenstreit“ im Jahr 2005 noch eine



Rolle spielen, in dem dänische Zeitungen wegen eines Verstoßes gegen das im Islam herrschende Bilderverbot mit Drohungen aus der arabischen Welt konfrontiert waren.

Welche Tendenzen zeichnen sich nun in der Zusammenschau der Ergebnisse ab? Hinsichtlich des Ausmaßes der in der Bevölkerung vorhandenen Bedrohungs- und Risikowahrnehmungen liegen keineswegs einheitliche Befunde vor, sondern diese divergieren teilweise erheblich. Daher lassen sich nur vage Aussagen treffen. Bezüglich der allgemeinen Bedrohungswahrnehmung hat sich gezeigt, dass sich die wahrgenommene allgemeine Bedrohung durch terroristische Anschläge durchaus auf einem ähnlichen Niveau mit existenziellen, gesundheitlichen und sozialen Bedrohungsfaktoren bewegt, also in den meisten Studien, in denen Rankings vorgenommen werden, einen prominenten Platz einnimmt.

Im Vergleich scheint eine hohe *allgemeine* Bedrohungs- und Risikowahrnehmung jeweils weiter verbreitet zu sein, während sich der Anteil der Befragten mit einer hohen *persönlichen* Bedrohungs- und Risikowahrnehmung jeweils als gering erweist. In Bezug auf verschiedene Transportbereiche lässt sich auf Basis der vorliegenden Ergebnisse eine Ausnahmestellung des Flugverkehrs feststellen, für den die allgemeine Risikowahrnehmung deutlich höher ausfällt als für Bahn-, Fähr- und Straßenverkehr.

In diachroner Perspektive deuten die Ergebnisse darauf hin, dass die allgemeine Bedrohungswahrnehmung in jüngster Zeit zurückgeht. Für die Risikowahrnehmung existieren widersprüchliche Befunde, so dass keine eindeutigen Aussagen über die Entwicklungsrichtung möglich sind.

### 2.3 Kritik und methodische Probleme

Vor dem Hintergrund, dass die Sicherheitsforschung seit geraumer Zeit expandiert und sich die Gefahren und Risiken, mit denen sie sich beschäftigt, multiplizieren, ist zunächst Kritik an der gängigen Forschungspraxis zu üben, Bedrohungs- und Risikowahrnehmungen terroristischer Anschläge in Itembatterien mit einer Vielzahl weiterer potenzieller Bedrohungs- und Risikofaktoren zu erheben. Auf diese Weise werden Risikokategorien festgeschrieben und Risikobewusstsein und Risikodenken angeleitet. Dies trifft gleichermaßen auf die „Angst- und Sorgenbatterien“ zu, deren feingliedrige Kategorisierung diese womöglich erst ins Bewusstsein zu rufen und zu wecken vermag. Ein Indiz dafür ist, dass Terrorismus weitaus seltener genannt wird, wenn offene Fragen gestellt werden.<sup>30</sup> Dass die Ängste nicht so klar trennbar im Bewusstsein der

---

<sup>30</sup> So haben beispielsweise in der Untersuchung von Gerhold (2009, S. 99) insgesamt nur sechs der 820 Befragten das Thema Terrorismus als Antwort auf die offen gestellte Frage *Was beschäftigt Sie zurzeit in Ihrem Leben?* genannt.



Bürger existieren, wie sie erhoben werden, haben Studien ergeben, die multivariate Analyseverfahren verwenden. Für die Kriminalitätsfurchtforschung liegen zahlreiche Befunde vor, die eine generelle Verunsicherung nahelegen, in welcher sich Ängste wechselseitig durchdringen und miteinander verschmolzen sind (Hirtenlehner & Farrall 2012). Aus Analysen anhand von Strukturgleichungsmodellen wird gefolgert, dass die Kriminalitätsfurcht „eine mit anderen Ängsten verwobene Komponente einer umfassenderen Verunsicherung darstellt“ (ebd., S. 108). Es lässt sich vermuten, dass auch die Angst vor terroristischen Anschlägen nicht eindeutig von anderen Ängsten abgrenzbar ist und sich in dieses Konglomerat bzw. diesen „Unsicherheitskomplex“ einfügt. In dem Projekt „Der überwachte Bürger zwischen Apathie und Protest“ hat sich gezeigt, dass Kriminalitäts- und Terrorismusfurcht hoch miteinander korrelieren (Schlepper & Lüdemann 2010; vgl. auch hochsignifikanter starker Zusammenhang bei Leese 2013). Gleiches gilt für Existenzängste und Terrorismusfurcht (Lüdemann & Schlepper 2013).

Zudem ist Skepsis angebracht, dass sich subjektive Empfindungen wie Angst, Sorge, Verunsicherung, Bedrohungs- oder Sicherheitsgefühl so direkt abfragen lassen, wie es in den Untersuchungen üblich ist, aber auch daran, dass die Befragten zu derartigen Differenzierungsleistungen imstande sind.

Damit stellt sich die Frage, wie aussagekräftig diese Messergebnisse sind und wie treffend sie die Wahrnehmungen der Bürger tatsächlich abbilden können oder ob vielmehr methodische Artefakte geschaffen werden: Inwieweit spiegeln die dargestellten Untersuchungsergebnisse die Bedrohungs- und Risikowahrnehmung terroristischer Anschläge in der Bevölkerung wider bzw. werden diese erst im Moment der Befragung generiert und inwieweit konstituiert Sicherheitsforschung ihren Gegenstand durch ihre eigene Praxis?<sup>31</sup>

Verstärkend kommt hinzu, dass in diesen Untersuchungen impliziert wird, dass persönliche und allgemeine Bedrohungs- und Risikowahrnehmungen weitgehend kontextunabhängig als statische Größe fassbar sind, was erheblich in Zweifel zu ziehen ist, da sie in alltägliche Handlungszusammenhänge eingebettet und damit situativ variabel sind. So werden sowohl die Bedrohungs- also auch die Risikowahrnehmung unterschiedlich ausfallen, je nachdem, ob man als Referenzpunkt ein Großereignis (z.B. Fußballspiel), einen Hauptverkehrsknotenpunkt (z.B. Hauptbahnhof) oder die eigenen vier Wände annimmt. Mit der vagen Eingrenzung auf *terroristische Anschläge in Deutschland* lassen sich diese Differenzen und deren Bedeutung für den Bürger nicht erfassen.

---

<sup>31</sup> Siehe exemplarisch für dieses Argument die Analyse einer Eurobarometer-Studie zu Einstellungen der europäischen Bürger beim Kauf von tierischen Lebensmitteln bei Law (2009).



Wenn, in Anlehnung an die Äußerung des ehemaligen Vizepräsidenten des Bundesverfassungsgerichts Winfried Hassemer (2006, S. 140), die „gefühlte“ Bedrohung“ der Bürger als Richtschnur politischen Handelns gelten sollte, dann bieten die bislang vorliegenden Erkenntnisse dafür keine geeignete Grundlage, da sie jene nur unzureichend abbilden können. Der derzeitige Forschungsstand lässt kaum Aussagen darüber zu, wie präsent die perzipierte Bedrohung durch terroristische Anschläge im täglichen Leben der Befragten ist und inwieweit und in welcher Form sie sich beeinträchtigend auf deren Lebensqualität auswirkt.<sup>32</sup> Zu denken wäre etwa an Verhaltensänderungen, wie z.B. sozialer Rückzug oder Vermeiden bestimmter öffentlicher Räume und Plätze.<sup>33</sup> In diesem Sinne sollte die Sicherheitsforschung bei der Analyse der lebensweltlichen Relevanz der terroristischen Bedrohungswahrnehmung ansetzen, welche die abstrakten Angst-, Sorgen- und Bedrohungswerte deutlich relativiert und damit eine validere empirische Basis darstellt, aus der sich politische Handlungsbedarfe ableiten ließen.

Es gibt aber auch gute Gründe dagegen, das subjektive Sicherheitsempfinden überhaupt zur Richtschnur politischen Handelns zu machen. So führt Christoph Gusy (2010, S. 116) aus: „Die ‚objektive‘ Sicherheitslage ändert sich mit Veränderungen von Bedrohungs-, Gefahren- oder Risikolagen: Verschlechtert sich die Lage, verschlechtert sich die Sicherheit; verbessert sich jene, verbessert sich auch diese. Dies ist beim subjektiven Sicherheitsgefühl nicht notwendig der Fall; im Gegenteil: Es kann sogar zu gegenläufigen Entwicklungen kommen. Das Sicherheitsgefühl ist überaus komplex und insbesondere keine bloße Resultante der Sicherheitslage.“ Vielmehr wird den sogenannten Massenmedien, die ihre eigenen Bilder von Bedrohungen produzieren, hier für gewöhnlich eine nicht unerhebliche Rolle zugeschrieben.

---

<sup>32</sup> So liefert etwa Gerhold (vgl. 2009, S. 181) erste Hinweise aus der bereits weiter oben erwähnten Untersuchung, dass die *Verunsicherung durch Terrorismus in Europa* geringe Auswirkungen auf die Lebensqualität der Befragten hatte. Im BaSiD-Projekt zeigte sich, dass die Sorge vor terroristischen Anschlägen die Lebenszufriedenheit der Befragten kaum beeinträchtigt (Hummelsheim 2013).

<sup>33</sup> Dass die Auswirkungen auf das Alltagshandeln indes als gering zu veranschlagen sind, legen die Ergebnisse der Untersuchung der Kriminalistisch-Kriminologischen Forschungsstelle der hessischen Polizei nahe, in der sich gezeigt hat, dass nur ein geringer Teil der befragten hessischen Bürger aufgrund der terroristischen Bedrohung „immer“ oder „oft“ Großveranstaltungen (11%), Flugreisen (8%), öffentliche Räume (6%) oder öffentliche Verkehrsmittel (5%)“ (Bott & Koch-Arzberger 2012, S. 138) meidet. Etwas höher fallen die Ergebnisse der Studie der Uni Kiel (Lübcke & Irlenkaeuser 2006) aus. Die Frage, ob *aufgrund der Terroranschläge der letzten Jahre die Nutzung öffentlicher Verkehrsmittel vermieden wird*, verneinten ca. 93 Prozent der Befragten (vgl. ebd., S. 19). Großveranstaltungen werden von fast jedem Fünften gemieden und Flugreisen von ca. zwölf Prozent.







### 3. Die mediale Vermittlung von Unsicherheit

Terroristische Bedrohungen sind wesentlich politisch und medial vermittelte Themen, nicht nur weil sie sich, hierzulande, meist der unmittelbaren Alltagserfahrung entziehen: Die Bevölkerung erfährt aus den Medien – im klassischen Sinne der Massenmedien – über Geschehnisse, die als terroristische Akte bzw. Bedrohungen bezeichnet und gedeutet werden. In der spätestens seit 9/11 dominierenden Lesart von Terrorismus als „kommunikativer Gewaltstrategie“ (Neidhardt 2006, S.11) gelten die Massenmedien überdies auch als unverzichtbare Mitspieler. Terrorismus, so die Beobachtung, funktioniert erst über die symbolische Botschaft (Juergensmeyer 2004) und in der symbiotischen Beziehung zwischen Medien und Terrorismus (vgl. Hoffman 2006, S. 183).<sup>34</sup> Die „medial vermittelte Interaktion“ zwischen den Terroristen auf der einen Seite und ihren Adressaten (Opfer, breite Öffentlichkeit, politische Entscheidungsträger) auf der anderen (vgl. Gerhards et al. 2011, S. 217) ist Voraussetzung für eine „Angst erzeugende Wirkung“ in der Bevölkerung und die *Erfahrung* einer Bedrohung (Kersten 2009, S. 300). Um diese Theorie vom „mass mediated terrorism“ (Nacos 2002) herum gruppiert sich eine Diskussion um die mögliche Instrumentalisierung, aber auch die Verantwortung der Medien (Hoffman et al. 2010) sowie eine wechselseitige Verstärkung der Akteure (Hoffman 2006). Den Medien als Sprachrohr des Terrorismus, aber auch der Politik, kommt eine besondere Rolle in der Vermittlung von Sicherheit bzw. Unsicherheit zu.

Dabei ist die Terrorismusforschung sich weitgehend einig, dass ihr Gegenstand selbst politisch und moralisch besonders heikel und umstritten ist. Es ist eine Binsenweisheit, dass die Unterscheidung zwischen Terrorismus und Freiheitskampf notorisch schwierig ist. Die öffentliche Diskussion, so die Medienwissenschaftler Stefan Bronner und Hans-Joachim Schott (2012, S. 7), sei deshalb von einer „moralischen Metaphysik“ geprägt, die eine unabhängige wissenschaftliche Einschätzung ihrerseits erschwere. Dieser Umstand hebt die Frage der Deutung von Gewaltereignissen bzw. Anschlägen zu einer der Deutungshoheit und unterstreicht die Bedeutung des medialen Zuschnitts. Eine durchgängige Kritik nimmt „[d]ie enorme Präsenz des Terrorismus in den Massenmedien“ ins Visier, welche „die entsetzliche Gewalt des Terrorismus zu bagatellisieren [droht ... und] weder der politischen Dimension noch den Opfern des Terrorismus gerecht wird.“ (Ebd., S. 9)

Freilich sind „die Medien“ kein singulärer Akteur, auch „inszenieren“ sie nicht einfach Bedrohungen durch den Terrorismus. Vielmehr treten sie buchstäblich „dazwischen“ (Mersch 2006, S. 9). Sie sind Medium, das „Botschaften“ nicht nur „überträgt“, sondern dabei eigene Formen der Darstellung und Rezeption und mithin eigene Gehalte

---

<sup>34</sup> Juergensmeyer (2004) verwendet das Vokabular des „Theaters“; dazu auch Bronner & Schott (2012).



prägt (Krämer 2011). Medien erzeugen eigene Bilder, auf die sie sich wiederum beziehen können.<sup>35</sup> Diese produktive Mittlerfunktion gilt es im Folgenden in den Blick zu nehmen.

### 3.1 Konstruktionen der Bedrohung und die Rolle der Medien

Klassisch ist der medientheoretische Ansatz des Soziologen Stuart Hall. Hall und Kollegen (1978, S. 53) betonen, was uns heute schon selbstverständlich erscheint: „The media do not simply and transparently report events which are ‚naturally‘ newsworthy in themselves“. Der Wert einer Nachricht liegt nicht in einem Geschehnis selbst verankert. Nachrichten sind vielmehr immer schon selektierte Begebenheiten, vor allem aber sind sie Zuschnitt eines Themas. Das bedeutet freilich keineswegs, dass terroristische Anschläge nicht „Ereignisse“ jenseits medialer Vermittlung sind, die als solche Mitgefühl mit den Opfern und Empörung hervorrufen. Insbesondere für die Anschläge vom 11. September 2001 gilt jedoch, dass diese erst *durch* die Medien zu einem *major event* werden konnten (Derrida 2006, S. 122). 9/11 ist wie kein Ereignis zuvor, wie der Medienwissenschaftler Richard Grusin (2004) herausgearbeitet hat, selbst zu einem (globalen) medialen Ereignis geworden. So wurden die Bilder vom Einschlag der Flugzeuge in die New Yorker Zwillingstürme gleichsam auf Dauer gestellt: Sie waren nicht nur am Tag des Anschlags unablässig medial präsent – das reale Ereignis wiederholte sich gewissermaßen unendlich in Echtzeit. Sie wurden vielmehr auch selbst zu einem Symbol, das immer wieder abrufbar ist, und das immer wieder abgerufen wird, nicht nur medial, sondern auch in unserer Vorstellung.

Vor diesem Hintergrund lässt sich nunmehr die Rolle der Massenmedien als – aktiv bestimmende – Akteure im Diskurs um Sicherheit und Bedrohung ausloten. So zeigen Oliver Bidlo, Carina Jasmin Englert und Jo Reichertz (2011) hauptsächlich mit Blick auf das mediale Format des Fernsehens und Internets, dass die Medien nicht nur als Überbringer von Nachrichten oder Multiplikatoren verstanden werden können. Sie seien heute vielmehr selbst zum (politischen) Akteur „im Diskurs über die richtige Form und gültige Legitimierung innerer Sicherheit“ geworden (Reichertz 2011, S. 34). Dabei führe die Ausrichtung auf die Kundenbindung dazu, dass das Thema der Inneren Sicherheit zur Unterhaltung mutiert: Aus Sicherheit und *Securitization* wird *Securitainment* (Bidlo et al. 2011). Wenn Medien, wie das Fernsehen, vor allem kommerziell orientiert sind, bedeutet das, vereinfacht gesagt, dass sie dem Publikum

---

<sup>35</sup> Wie diskurs- und systemtheoretische Perspektiven gezeigt haben, sind gesellschaftliche Kommunikationsprozesse und mediale Realitätskonstruktionen eben nicht auf Akteure und Interaktion oder gar ein einfaches Sender-Empfänger-Modell zu reduzieren. Die Möglichkeit der Artikulation ist selbst immer schon an die Modalitäten der Artikulation und Sinnherstellung gebunden.



geben, was es hören, lesen und sehen will. Die Nachfrage bestimmt das Angebot, kommerzielle Notwendigkeiten und Interessen bilden die Basis der Nachrichtenproduktion. Gesagt ist damit freilich nicht, dass die Nachfrage nicht ihrerseits durch das Angebot produziert und geformt wird – Sicherheit wird zu *Securitarianment*, weil das Fernsehen hier Unterhaltung bietet. Auch ist die Vorstellung, dass die Gesetze des Marktes die Mediendarstellungen bestimmen, recht pauschal. So werden jene schon von publizistischen Routinen und Normen unter dem Einfluss einer weitgehend regulativen Medienpolitik hierzulande durchbrochen (vgl. Vowe 2012, S. 443f.). Die populäre Gleichsetzung von Marktmechanismen und schlechtem Journalismus verkennt überdies, dass Massenmedien sich auch mit Qualitätsjournalismus profilieren können.

Wenn die Medien im Prozess der Nachrichtenproduktion selbst aktive Gestalter sind, so sind sie doch auf bestimmte Quellen angewiesen. So entscheiden beim Thema Kriminalität und Sicherheit die Behörden selbst, welche Informationen sie überhaupt nach außen geben (dazu Jenkins 2003). Gestalter sind die Medien dann vor allem durch die spezifische Rahmung und Fokussierung (grundsätzlich Scheufele 2003), gebunden zugleich aber auch an ihre eigenen Routinen und Produktionsmechanismen (Hall 1989). Dabei gilt für die Medienlandschaft der Gegenwart, dass die Angebote einerseits nicht zuletzt durch den Einzug der „Neuen Medien“ in den Alltag der Bevölkerung vielfältiger geworden sind, andererseits aber vielfach standardisierte und sich wechselseitig standardisierende mediale Inhalte und Formate anzutreffen sind. Mit Blick auf die zunehmend visuell geprägten Berichte ist dies u.a. auf den Zugriff auf gemeinsame Bilddatenbanken zurückzuführen (Drechsel 2005). Einmal eingeführte Deutungsrahmen und Bilder, die überdies zunehmend unkommentiert lanciert werden können (Chèroux 2011), sehen sich reproduziert und bekräftigt.

Bilder scheinen für sich zu stehen – das Vertrauen ins Augenscheinliche und die Zuverlässigkeit des Visuellen geht aus der Unmittelbarkeit der Wahrnehmung hervor (Schmied-Knittel 2010, S. 9). Im Artefakt der Fotografie verobjektiviert sich die Bedeutung der Bilder bis hin zu einem Beweischarakter (Burri 2008, S. 252f.).<sup>36</sup> Doch ihre Bedeutung erhalten Bilder, wenn nicht durch das bereits vorhandene kulturelle Wissen, erst durch den sie rahmenden Text und ihre Platzierung (Blair 2004). Und dabei ist die Entscheidung über die Auswahl und ihre Platzierung (ebenso wie die Wahl des Ausschnitts, die Weitergabe an Datenbanken und Nachrichtenagenturen usw.), auch jenseits der Marktmechanismen und Produktionsbedingungen, ihrerseits stets kulturell vorgeprägt, d.h. in gesellschaftlichen Deutungen und Rahmungen, Bildern und Imaginationen verhaftet.

---

<sup>36</sup> Für eine ausgezeichnete Analyse der Inszenierung der „Beweisbilder“ für die Irak-Intervention beim Auftritt von Colin Powell vor der UNO siehe Holert (2006).



### 3.2 Mediale Darstellungen von terroristischen Bedrohungen

Für die Analyse der Aushandlung medialer Inhalte und Kommunikationsprozesse greift die Kriminologie traditionell auf das Konzept der „Moralpanik“ von Stanley Cohen (1972/2002) zurück. Gefahrendiskurse werden hier mit Blick auf die Rolle der Medien im Wechselspiel mit Politik und anderen Interessenvertretern sowie der Frage der Initiierung, der beförderten Interessen, der Art und Weise der Darstellung usw. untersucht. Dabei geht das Konzept der Moralpanik im Kern davon aus, dass das jeweilige Thema, wie das delinquente Verhalten von Jugendlichen, in der Öffentlichkeit nicht angemessen, sondern verzerrt verhandelt wird. Eine überzogene Berichterstattung entwickelt sich über eine negative Stereotypenbildung zur Feindbildkonstruktion. Als Folge wird der Anstieg der Besorgnis über diese Themen in der Bevölkerung gesehen und angenommen, dass auf diese Weise eine – nicht weiter kritisierte – „Kriminalitätsfurcht“ erzeugt wird und damit zugleich die normativen Grenzen der Gesellschaft bekräftigt werden. Die Analyse des Themas des Terrorismus mit dem Konzept einer Moralpanik wurde bislang nicht vorgenommen bzw. setzt gegenwärtig erst zögerlich ein (z.B. Welch 2006).

Genau hierin sieht der Soziologe David Garland (2008b) eine der Schwachstellen des Konzeptes, dass nämlich die Identifizierung einer Thematisierung als Moralpanik nicht unabhängig vom Standpunkt der jeweiligen Autoren erfolgt. Diese moralische Befangenheit trägt, Garland zufolge, im Umkehrschluss dazu bei, dass sich die aktuellen Vertreter des Konzepts seit den Anschlägen von 9/11 mit der Schwierigkeit konfrontiert sehen, eine moralisch integre Analyseform zu finden. Dabei weist der (US-amerikanische) Anti-Terror-Kampf in der Art und Weise seiner Selbstpräsentation durchaus Züge einer Moralpanik (öffentliche Sensibilisierung, Feindseligkeit, Verzerrung bis hin zur Falschdarstellung etc.) auf, die aber in der Kriminologie nicht analysiert und problematisiert werde (vgl. ebd., S. 24). Für David Altheide (2009, S. 93) ist einer der möglichen Gründe hierfür darin zu sehen, dass die Terrorismus-Bedrohung von der Bevölkerung selbst als real erlebt und Terrorismusbekämpfung entsprechend als notwendig bzw. legitim erachtet wird:

„Terrorism and the terrorist threat are still regarded as legitimate and objectively real by many people in the United States and the UK; it is not viewed as a social construction and the government actions are not treated in the mass media as arbitrary overreaction. Indeed, opposition parties in the USA insist that terrorism is a pressing issue, and offer slight differences in how to combat it.“

Die wenigen Studien, die sich aus dem Bereich der Kriminologie mit dem „sakrosankten“ Thema des Terrorismus befassen (vgl. ebd.), widmen sich vor allem der medialen Feindbildkonstruktion. So identifizieren Dawn Rothe und Stephen L. Muzatti (2004,



S. 333) in ihrer Analyse dreier US-Tageszeitungen nach 9/11 die Kreation medialer „Folk Devils“ von Bin Laden und Al Quaeda bis zur „Achse des Bösen“. Auch der Politikwissenschaftler Hans J. Kleinsteuber (2003) zeigt, wie sich die Feindbildkonstruktion in der US-amerikanischen Außenpolitik von Bin Laden, als „Urheber des Terrors“ auf Saddam Hussein verlagerte – und zeichnet dafür vor allem einen Mangel an verwendbarem Bildmaterial als verantwortlich.<sup>37</sup>

Die meisten – und dominierenden (Ross 2007, S. 218ff.) – inhaltsanalytischen Studien beziehen sich auf das Konzept der „Frames“, das heißt auf Deutungsrahmen, die den Zuschnitt eines Themas in „bedeutungsvolle Einheiten des Medieninhalts“ strukturieren (Scheufele 2001, S. 145). Dabei unterscheiden Norris et al. (2003) zwischen konventionellen und abweichenden („dissident“) Media-Frames. Während konventionelle Frames weit verbreitete Normen und Werte reflektieren, fordern letztere diese heraus. Media-Frames helfen, neue komplexe Probleme, Ereignisse und Handlungen in bekannte Kategorien einzuordnen (ebd., S. 4f.). Sie produzieren einfache und überzeugende Narrative und konturieren zum Beispiel Freund/Feind-Gegenüberstellungen. Sie ermöglichen der Politikvermittlung auf diese Weise, auf weitere Argumentation oder Begründungen zu verzichten (vgl. ebd., S. 15). Warum sich aber ein bestimmter Frame in Konkurrenz zu anderen durchsetzt und hegemonial werden kann, ist im Kontext von Medienanalysen bislang jedoch noch unbeantwortet geblieben (ebd., S. 11).<sup>38</sup> Auszugehen ist mit Albert Scherr (2010, S. 32) jedenfalls, dass „Bedrohungsszenarien und Feindbildkonstruktionen [...] potentiell umstritten und nicht beliebig durchsetzungsfähig“ sind.

Als exemplarisch für die Ergebnisse einer aktuellen inhaltsanalytischen Frame-Analyse zum Thema kann die von Wolfgang Frindte und Nicole Haußecker (2010) herausgegebene Studie *Inszenierter Terrorismus. Mediale Konstruktionen und individuelle Interpretationen* gelten.<sup>39</sup> In ihrer Untersuchung von knapp 2000 Nachrichtenbeiträgen zwischen 2007 und 2009 kommen sie zu dem Schluss, dass „Beiträge über den Kampf gegen den Terrorismus sowie Berichte über geplante bzw. stattgefundenen terroristische Ereignisse“ die Fernsehnachrichten dominieren (ebd., S. 317).<sup>40</sup>

---

<sup>37</sup> Ähnlich untersucht Maren Kuntze (2003) die Kriegsvorbereitungsphase und die Phase kurz nach dem Angriff auf Afghanistan. Am Beispiel der FAZ und NZZ zeigt sie, dass sich das Feindbild in diesen Phasen nicht nur auf Bin Laden richtete, sondern eher diffus auch auf „die Taliban und das Terroristen-Netzwerk“ (ebd., S. 243).

<sup>38</sup> Hegemonietheoretische Ansätze böten hier das geeignete Instrumentarium, siehe etwa Dzudzek et al. (2012).

<sup>39</sup> Exemplarisch für eine soziologische Fragestellung steht die Studie von Matthias Junge (2003), der die „Politisierung kultureller Differenz“ (ebd., S. 134) als Kerninterpretation der Anschläge von 9/11 in seinem Datensample von Tageszeitungen bestätigt fand.

<sup>40</sup> Auch Hoffman et al. (2010) kommen zu diesem Ergebnis in ihrer Analyse von *Washington Post* und *USA Today*.



Dabei gehe die „ereignisorientierte Berichterstattung“ (Haußecker 2012, S. 36), so die Kritik, auf die politischen, sozialen und historischen Hintergründe selten ein, und das gelte für die öffentlich-rechtlichen Sender gleichermaßen wie für die privaten (die indessen grundsätzlich weniger darüber berichten). Demgegenüber werde vor allem die „mediale Botschaft: Staat und Bürger müssen geschützt werden“, vermittelt und „die wichtigsten Mittel dafür sind die Verschärfung von Gesetzen und militärische Gewalt“ (Frindte & Haußecker 2010, S. 318). Eine zentrale Rahmung bildet die Bedrohung durch den Terrorismus, die sich nicht nur auf die USA, sondern auch auf Deutschland beziehe und einerseits eher unspezifisch gezeichnet, andererseits aber vor allem als gegen Individuen (weniger gegen Werte, Infrastrukturen oder Gruppen) gerichtet präsentiert werde (vgl. ebd., S. 91f.).

Auch Jürgen Gerhards und Kollegen (2011, S. 218) haben auf der Grundlage einer Frame-Analyse im internationalen Vergleich von Fernsehnachrichtensendungen die „Besonderheiten massenmedialer Terrorismuskonstruktionen“ zu ermitteln versucht und dabei die These einer weltweiten Standardisierung der Formate und Kriterien der Nachrichtenselektion bestätigt (vgl. ebd., S. 221ff.). Während bei *CNN* und *Al Jazeera* gleichermaßen die Deutung von Terroranschlägen als Ausdruck eines weltweiten Konfliktes dominiert, neigten sowohl die *ARD* als auch die *BBC* zu der Lesart, es handle sich um kriminelle, weniger um politische Akte (vgl. ebd., S. 224ff.). Und während *CNN* und *Al Jazeera* eher diffuse „Angst vor einem allgegenwärtigen Terrorismus, der überall und jederzeit zuschlagen kann“ (in Verstärkung des weltpolitischen Deutungsrahmens) vermittelten, würden *ARD* und *BBC* eher konkrete Bedrohungsszenarien und mithin eine ereignis- und lebensweltbezogene Darstellung entwerfen (ebd., S. 236).

Emotionalisierende Formen der Visualisierung, wie eine schnelle Schnitffrequenz, Nahaufnahmen etc., die eine Dramatik herstellen, sind Frindte und Haußecker (2010, S. 95f.) zufolge nicht spezifisch für das Thema des Terrorismus, kommen hier aber besonders zum Einsatz. So berichteten private TV-Nachrichtensender weniger über die politischen Hintergründe des Terrorismus selbst, setzten aber deutlichere Stilmittel wie etwa „bildliche Darstellungen von Opfern, Verletzten/Toten“ ein (ebd., S. 10, grundsätzlich S. 75), die einer Emotionalisierung (im Sinne „physiologischer Erregung“) Vorschub leisteten (ebd., S. 96).

Im Kontrast zu den Studien über die deutsche Medienberichterstattung kommen Brigitte L. Nacos und Oscar Torres-Reyna (2003) mit der Inhaltsanalyse verschiedener (vier) US-Zeitungen und (zwei) US-Fernsehsendungen zu dem Schluss, dass nach 9/11 (medienübergreifend) eine wesentlich differenziertere Darstellung von Muslimen und Amerikanern mit arabischer Herkunft zu verzeichnen war als vor 9/11. Auffallend war z.B., dass diese Bevölkerungsgruppen häufiger selbst zu Wort kamen.



Allerdings waren Stereotypisierungen bei ausgewählten Themen, wie etwa der häufig vorkommenden Rahmung einer Verletzung der Bürgerrechte sowie politischer Aktivitäten von Muslimen bzw. „Arab-Americans“, zu verzeichnen (ebd., S. 151).

Zusammenfassend lässt sich sagen, dass die hier exemplarisch referierten Studien über mediale Botschaften und Bilder der Terrorismusbedrohung eine eigenständige mediale Realität zeichnen (vgl. Kirchhoff 2010, S. 281). Ausgesagt ist damit noch nichts über die Art und Weise der Rezeption. Medienanalysen können über einen langen Zeitraum den Wandel und die Durchsetzung von Deutungsmustern und insofern die „Karriere sozialer Probleme“ nachzeichnen (Schetsche 2008), aber sie können selbst nicht belegen, welchen Einfluss die verschiedenen Akteure tatsächlich auf die Formung der medialen Bilder und Botschaften oder gar deren Wirkungen haben. Ein gutes Beispiel dafür ist die Inszenierung des ehemaligen Präsidenten Bush, der sich im Mai 2003 demonstrativ in Pilotenuniform auf dem Flugzeugträger Abraham Lincoln ablichten ließ (zur Analyse vgl. Hentschel 2008). Obgleich die mediale Inszenierung vielfach als missglückt wahrgenommen wurde, gelang es Bush trotz aller Häme, das „kollektive Bildgedächtnis der großen Gefühle“, wie es aus Hollywood-Filmen gleichsam zeitlos präsent ist, zu evozieren und damit einen „heroisierten Rahmen“ für seine Botschaft im „Krieg gegen den Terror“ und die Operation *Enduring Freedom* zu schaffen (ebd., S. 191).<sup>41</sup>

Auch die Frage, die der Moralpanik-Ansatz aufwirft, welche Akteure in welcher Weise ihre Interessen – oder Botschaften – durchsetzen, lässt sich so nicht beantworten, schon weil sie homogene und eindeutig identifizierbare Interessen voraussetzt, die sich im politischen Spiel und der sozialen Praxis indes vielfach brechen.<sup>42</sup> Möglich ist jedoch nachzuzeichnen, welche kollektiven und kulturellen Bilder in welcher Weise etwa in Prozesse der Legitimitätsherstellung von Sicherheitsmaßnahmen und -gesetzen einziehen.<sup>43</sup> So haben Gabe Mythen und Sandra Walklate (2006) herausgearbeitet, wie die mediale Anti-Terror-Metaphorik mit der Diskussion um nationale Regelungen und Maßnahmen in gänzlich anderen politischen Feldern, wie etwa der Migration,

---

<sup>41</sup> Ähnlich hat auch der Kulturwissenschaftler Tom Holert (2008, S. 176f.) herausgearbeitet, wie das US-Militär Ende 2005 die Gelegenheit ergriff, „das Militär als Institution der Trauer- und Affektarbeit zu präsentieren, als Modell von praktiziertem Mitleid“.

<sup>42</sup> Dieser Umstand lässt sich theoretisch mit einem „praxeologischen Zugriff“ (etwa Reckwitz 2003) begründen und empirisch auch nachweisen, siehe für eine entsprechende Analyse Garland (2010) am Beispiel der Kontinuität der Todesstrafe in den USA.

<sup>43</sup> Zur Analyse entsprechender Diskurse zur Legitimitätsherstellung zur Terrorismusbekämpfung und dem „War on Terror“ im Anschluss an 9/11 eingehend Kirchhoff (2010). Ein weiteres Feld, das hier ausgespart wurde, jedoch auch zu den klassischen Feldern der Medienanalyse zählt, ist die filmische Bearbeitung im Kino oder Fernsehen. So arbeitet etwa Campbell (2010) in seiner Filmanalyse heraus, wie Deutungen zum Terrorismus auch die Legitimation einer Verweigerung von Grundrechten gegenüber muslimischen Gefangenen in Guantanamo erzeugen.





verschmelzen und aus der Erzeugung von Furcht („fear“) gleichsam politisches Kapital geschlagen wird. Solche Analysen können mit empirischen Beobachtungen aus anderen Politikfeldern verknüpft werden, in denen sich die Hochzeiten medialer Risikokonjunkturen als ein „policy window“ (Kingdon 1995) der Legitimation und Durchsetzung neuer Gesetze darstellen (für die Umweltpolitik etwa Ernst 2008).

### 3.3 Mediale Rezeption von terroristischen Bedrohungen

Abseits der *ill effects*-Debatten der klassischen Medienwirkungsforschung haben Frindte und Haußecker (2010) im qualitativen Teil ihrer Studie die Einstellungen zu Anti-Terrorismus-Maßnahmen und das persönliche Bedrohungserleben erhoben. Sie konnten dabei keine direkten Zusammenhänge zwischen der Einstellung zu den Maßnahmen und einem persönlichen Bedrohungserleben feststellen, wie internationale Studien behaupten. Allerdings legen die Ergebnisse ihrer Interviews nahe, dass Vorurteile gegenüber „Fremden“ und die Befürwortung einer Verschärfung von Anti-Terror-Maßnahmen sich gegenseitig bestärken, was sie – klassisch – mit einem „hohe[n] Maß an Autoritarismus“ in Verbindung bringen (ebd., S. 317). „Es ist also nicht primär die Angst vor Terrorismus an sich, die Menschen veranlasst, militärischen und verschärften Sicherheits- und Überwachungsmaßnahmen zuzustimmen. Wenn sie dies tun, so offenbar vor dem Hintergrund manifester autoritärer Einstellungen und negativer Vorurteile gegenüber Muslimen.“ (Ebd., S. 316) Diese „Vorurteile“ führen die Autoren auch auf „medial vermittelte Stereotype“ zurück, auf die die Mediennutzer vor allem zurückgreifen, wenn sie selbst keine Berührungspunkte zu den Personengruppen hätten. Wenn „Terrorismus aus Sicht des Fernsehens [...] von fundamentalistischen Islamisten aus[geht]“ (ebd., S. 318), so zeige sich bei den Mediennutzern selbst indes ein differenzierteres Bild. Danach gefragt äußern sich die Mediennutzer etwa gegenüber „entwicklungspolitischen Maßnahmen zur Eindämmung des Terrorismus“ (ebd., S. 314) durchaus positiv, obschon diese in den Medieninhalten selbst kaum eine Rolle spielten.

Heute kann man jedoch immer weniger von der klassischen Kategorie der „Massenmedien“ ausgehen (Sturken & Carthwright 2005) – denn mit der Vervielfältigung „der Medien“ hat sich spätestens seit den 1990er Jahren unser mediales Verständnis grundlegend verändert. Das Publikum ist zugleich auch Nischenpublikum, dem individualisierte Angebote gemacht werden. Damit ist zugleich eine Abkehr von dem Verständnis verbunden, dass „die Bevölkerung“ einheitlich mediale Inhalte aufnehmen und passiv rezipieren würde. Mediale Inhalte werden vielmehr aktiv und durchaus auch kreativ angeeignet.

Mit den sogenannten Neuen Medien eröffnen sich zum einen neue Wege der Partizipation der Mediennutzer, und dabei verschmelzen die klassischen Rollen von Publikum



und Nachrichtenproduzenten (Bidlo et al. 2012; Kirchhoff 2010). „Prosumenten“ sind aktive Produzenten und Konsumenten gleichermaßen (Bidlo 2011, S. 129). Zum anderen verstärkt sich, auch im Fernsehen, die Tendenz zu einer All-Gegenwart von Nachrichten und „News“, die praktisch ständig live abrufbar sind oder zu sein scheinen (im TV z.B. als „Rolling News“). Mit dem ständig möglichen Internetzugang, auch via Mobiltelefon, können nicht nur Nachrichten und Reportagen in einem bis dato ungekannten Ausmaß rezipiert, sondern, in sozialen Netzwerken, auch kommentiert, verlinkt und vervielfältigt werden. Diese Entwicklung führt auch dazu, dass Laien gleichsam selbst zu Reportern werden und etwa mit Videoaufnahmen zum Teil eher vor Ort sind als Journalisten. Dieses auf eine spezifische Art gemeinsame Erleben kreiert nicht nur eine spezifische Wahrnehmung und Deutung von Ereignissen, sondern auch die Illusion, man würde verstehen, was vor sich geht (so Bourke 2006).

Ferner eröffnen die Neuen Medien die Möglichkeit, dass Laien selbst Bilder der Überwachung erzeugen und die Überwachungspraktiken ihrerseits beobachten und verbreiten. Mit diesen Möglichkeiten der aktiven Beteiligung ist, Oliver Bidlo (2011) zufolge, auch der Wunsch entstanden, sich nicht mehr mit den überlieferten Bildern und Berichten zufrieden zu geben. Überdies lädt eine kontinuierliche Aufrechterhaltung der Bedrohung die Bevölkerung dazu ein, selbst an der Herstellung ihrer Sicherheit mitzuwirken. Der Aktivierungsaufruf, z.B. mittels Wachsamkeitsappellen – ob medial kommuniziert (wie bei Bidlo et al. 2012) und/oder behördlich initiiert (für UK: Mythen & Walklate 2006; für die USA: Reeves 2012) – erzeugt ein Klima, das suggeriert, jeder Bürger sei persönlich bedroht, müsse Maßnahmen ergreifen (Verdächtiges melden) oder erdulden, um dem Kollektiv, der staatlichen Ordnung beizustehen gegen die Bedrohungen von außen. Während neue Medien eine selbständige Plattform der Vervielfältigung, des Austausches, der Übermittlung solcher Verdachtsmomente durch den Laien bieten, versuchen die klassischen Medien dieser Konkurrenz zu begegnen, indem sie die Bürger zum Mit-mach-Journalismus mobilisieren und ihnen ebenfalls Raum und Verbreitungsmedien zur Verfügung stellen (Bidlo 2011, S. 129ff.).

### 3.4 Perspektiven der Medienanalyse

Die Rolle der Medien in der Konstruktion von Sicherheit bzw. einer Bedrohung durch den Terrorismus erschließt sich, so lässt sich nunmehr schlussfolgern, wenn man einen erweiterten Medienbegriff in Anschlag bringt und Medien nicht nur im traditionellen Sinne als Informationsübertragungs- und Kommunikationsmedien begreift. Massenmedien berichten nicht nur über Ereignisse in der Welt, vielmehr bringen sie Phänomene wie Terrorismus in Erscheinung, machen sie sichtbar. Auch Sicherheitstechnologien wirken als Medien. Sie produzieren Wirklichkeiten, Objekte, Klassen von Individuen. Richard Ericson und Kevin Haggerty (1997) haben bereits vor Jahren für die



Polizeiarbeit den Slogan geprägt, „community policing“ sei „communications policing“, d.h. die Hauptaufgabe der Sicherheitsbehörden ist aus ihrer Sicht in erster Linie Risikokommunikation. Die Art, wie sie das tun, mit Hilfe welcher Methoden und Mittel, bestimmt nicht nur das Bild der Kriminalität, sondern erzeugt eine bestimmte Art von nicht mehr hintergebarter Realität.

Diesen Sachverhalt gilt es bei der Analyse von Wahrnehmung, Medien und gesellschaftlicher Konstruktion von Sicherheit zu berücksichtigen. Die Suche nach einer wahren, objektiven, nicht verzerrten oder von Störeinflüssen freien Wirklichkeit des Verbrechens im Allgemeinen und des Terrorismus im Besonderen endet spätestens an der Grenze der körperlichen Verletzung und jenseits der – tödlichen – Schmerzen der Opfer gibt es nur mehr medial Vermitteltes.<sup>44</sup> Natürlich lässt sich unterscheiden zwischen dominanten, akzeptierten, abgesicherten, hegemonialen Wirklichkeiten und Wahrheiten auf der einen Seite und nicht akzeptierten, marginalen, und wenig abgesicherten auf der anderen. Allerdings gilt es dabei zu berücksichtigen, dass sich die Differenz zwischen diesen unterschiedlichen Konstrukten nicht durch ihre mehr oder weniger große Übereinstimmung mit einer vorgängigen Wirklichkeit bestimmen lässt. Die Verhältnisse zwischen Wahrheiten sind Machtverhältnisse und die Differenz zwischen heterodoxen und orthodoxen Deutungen verweist auf Machtdifferenzen und differentielle Chancen der Durchsetzung.

Betrachtet man die Rolle der Medien im Prozess der Wahrnehmung und der Konstruktion von Wirklichkeiten, so zeigt sich eine interessante Paradoxie. Medien machen Phänomene wie Terrorismus im visuellen und sozialen Sinne sichtbar – man denke an die emblematischen Bilder der Flugzeuge, die in die Twin Towers in New York stürzen, oder auch an Fahndungsfotos im Fernsehen und auf Plakaten. Medien können Objekte aber auch gleichsam verschwinden lassen. Im Kontext des Einsatzes von Sicherheitstechnologien sprechen Bellanova und Fuster (2013) hier von den „politics of disappearance“.

Die gesellschaftliche Konstruktion von Sicherheit entfaltet sich in diesem Wechselspiel von Sichtbarmachung und Unsichtbarmachung. Dies gilt in dem trivialen Sinne, dass ein terroristischer Anschlag, über den nicht berichtet wird, außer für die unmittelbar Betroffenen, gleichsam nicht stattfindet. Es entspricht der Dramaturgie terroristischer Anschläge, Wirksamkeit über die mediale Vermittlung zu entfalten. Die lokale

---

<sup>44</sup> Jenseits der Evidenz der eigenen Körperlichkeit (bei den sogenannten „Qualia“) endet die unhintergehbare Evidenz der Wahrnehmung. Die hier wichtigen Unterscheidungen zwischen der Evidenz der körperlichen Empfindung und der sozialen Deutung spielen nicht nur für die Kriminologie, sondern auch für die (Neuro-)Biologie und die Philosophie eine zentrale Rolle (Grahek 2001; Scarry 1992).



Aktion soll politische Botschaften an ein globales Publikum senden. Vereinzelte, unberechenbare Operationen sollen ein allgemeines Klima der Angst erzeugen.

Das Wechselspiel von Sichtbarkeit und Unsichtbarkeit vollzieht sich aber auch in einem weniger trivialen Sinne. Die Durchdringung des Alltags und des öffentlichen Raums mit mehr oder weniger bewusst wahrnehmbaren Sicherheitstechnologien und -praktiken (von den Videokameras im öffentlichen Raum über routinemäßige Kontrollen an Flughäfen bis hin zur kontinuierlich wiederholten Aufforderung über Lautsprecher, sein Gepäck an Bahnhöfen nicht unbeaufsichtigt stehen zu lassen), erinnert auf banale Weise an die niedrighschwellige, allgegenwärtige Gefährdung. Dieser Mechanismus ist von Michael Billig (1995) für das politisch-kulturelle Objekt des Nationalstaats beschrieben worden: Ohne explizit auf die Nation Bezug zu nehmen, verweisen eine Vielzahl von kulturellen Praktiken und linguistischen Varianten unterschwellig und kontinuierlich auf dieses Objekt. Billig bezeichnet dies als „Flagging the Homeland Daily“. Sicherheitstechnologien und dazu gehörige Praktiken erfüllen eine ähnliche Funktion. Ihre Wirkung ließe sich als „Flagging security threats daily“ bezeichnen. Ganz offensichtlich ist im Hinblick auf die vermeintlichen Gefahren des Terrorismus die Überschneidung zwischen Sicherheit und Nationalstaat, da es die derzeit als besonders bedrohlich eingestuften terroristischen Akteure gemäß der herrschenden Deutung auf „unseren“ Staat, „unsere“ Kultur abgesehen haben. Ihre Angriffe zielen auf „uns im Westen“. Die verzweigten und teils kruden, teils differenzierten Diskurse, die diese Deutung umgeben, bilden das Grundrauschen einer hegemonialen Selbstvergewisserung im Angesicht brüchig werdender kollektiver Identitäten (Barber 1995; Said 1978).

Betrachtet man die Dynamik der medial vermittelten Kommunikation über Sicherheit, so zeigt sich, dass einfache Ursache-Wirkungsschemata nicht hinreichend sind, um die Zusammenhänge zwischen Medien in diesem erweiterten Verständnis und den verschiedenen Dimensionen oder Facetten von Sicherheit zu erfassen. Vorherrschend sind hier Rückkopplungen und Kreisläufe der Verstärkung oder Dämpfung von Vorstellungen, Politiken und Praktiken, die verschiedene öffentliche Sicherheitsdiskurse prägen.

Einer der bekanntesten dieser Kreisläufe ist in der *News Making Criminology* (Barak 1994) beschrieben worden. Vereinfacht besagt dieser Kreislauf, dass ein Großteil der Kriminalität, die der Polizei zur Kenntnis kommt, auf Anzeigen aus der Bevölkerung basiert. Das Wissen der Bevölkerung über verschiedene Formen der Kriminalität und ihre Bedrohlichkeit und Verbreitung wiederum basiert auf der Rezeption von Medien (im traditionellen Sinne von Zeitungen und TV). Der Großteil der medialen Kriminalitätsberichterstattung speist sich seinerseits aus Informationen, die aus Polizeiquellen kommen. Selten recherchieren Redakteure oder Journalisten eigenständig in diesem Bereich. Sie verlassen sich auf die Informationen aus den polizeilichen Pressestellen. Hier schließt sich dann der Kreis zwischen Medien, Strafverfolgung und Bevölkerung.



In ähnlicher Richtung argumentiert Katherine Beckett (1997) in ihren Untersuchungen. Sie konzentriert sich auf das Zusammenspiel von Politik und Medien. Entgegen der These, dass punitive und repressive politische Maßnahmen als Folge einer steigenden Kriminalität oder sonstigen Problemdrucks interpretiert werden können, sind es vielmehr die öffentlichen und veröffentlichten Aussagen einschlägig motivierter Kriminalpolitiker, die einhergehen mit einer entsprechenden Medienberichterstattung über die Bedrohlichkeit der jeweiligen Probleme, die diese Entwicklung vorantreiben. Beckett nennt die gängige Interpretation die „democracy at work“ These, die besagt, Politik reagiere auf reale Probleme und den Druck der Bevölkerung. Beckett kann anhand ihrer Daten aus den Vereinigten Staaten nachweisen, dass politisch-mediale Initiativen die über Meinungsumfragen erhobene Besorgnis in der Bevölkerung erst auslösen. Zudem zeigt sie am Beispiel von Drogenmissbrauch, dass die öffentliche Erregung über dieses soziale Problem mit seiner realen Verbreitung nicht korreliert. In Zeiten steigender Zahlen registrierter Drogenprobleme hält sich die öffentliche Erregung über dieses soziale Übel in Grenzen. Sie steigt jedoch an, nachdem sich politische Akteure zu Wort gemeldet haben und offiziell ein „Drogenproblem“ ausgerufen haben.

Im Hinblick auf politische Initiativen im Politikfeld Terrorismusbekämpfung wirkt ein weiterer Verstärkerkreislauf. Die Bedrohungsanalysen, die der Politik zur Verfügung stehen, stammen von nationalen oder transnationalen Lagezentren.<sup>45</sup> Diese Expertengremien sind mit Fachleuten aus dem Bereich der Sicherheitsbehörden besetzt. Die dort entwickelten Bedrohungsszenarien basieren i.d.R. auf nicht öffentlich zugänglichen Daten („Intelligence“). In ihrer Bewertung dieser Daten neigen diese Gremien eher zu *worst-case*-Annahmen als zur Verharmlosung. Die politisch Verantwortlichen sind dann in der Situation, auf der Grundlage solcher Gefährungsdiagnosen Entscheidungen zu treffen – etwa Gesetzesinitiativen einzubringen, die zu einem Ausbau von Überwachungsmaßnahmen führen. Die Politik ist in diesem Bereich auf die Diagnosen der Sicherheitsbehörden angewiesen. Es gibt keine unabhängige Evidenz, die im Sinne eines „Gegengutachtens“ oder „Sondervotums“ wie es in anderen expertenabhängigen Politikbereichen existiert, alternative Standpunkte in die Diskussion einbringen könnte.

Im rationalen Kalkül der politisch Verantwortlichen ist im Angesicht von vermeintlichen Bedrohungen eine prä-emptive Reaktion die bessere Lösung, da im Fall eines

---

<sup>45</sup> In Deutschland ist hierfür das GLMZ, das gemeinsame Lage- und Meldezentrum des BMI zuständig. Ferner wird eine Anti-Terror Datei unterhalten (ATD), in der wichtige Informationen gespeichert werden (vgl. 4.1.3.4). Auf europäischer Ebene existiert ein EU Counterterrorism Coordinator, der ebenfalls für die Koordination und Aufbereitung entsprechender Informationen zuständig ist.



Nicht-Reagierens der Eintritt des Schadens ihrem Nicht-Handeln zugeschrieben werden kann (Kreissl 2008).





## 4. Sicherheit im Fluchtpunkt von 9/11

Kontroll- und Überwachungstechnologien kommt eine besondere Vermittlerfunktion im Prozess der Konstruktion von Sicherheit zu. Die vom Staat ergriffenen Terrorismusbekämpfungsmaßnahmen erfüllen nicht lediglich einen instrumentellen Zweck und sind nicht nur gegen „die Terroristen“ gerichtet, sondern transportieren gleichzeitig eine „symbolische Botschaft“ an die Bevölkerung. Hiervon ausgehend gibt dieses Kapitel zunächst einen Überblick über die sicherheitspolitischen Initiativen, die sich zumeist als Antworten auf 9/11 präsentierten, im Wesentlichen jedoch schon vorher anvisiert waren und eine eher kontinuierliche Entwicklung in der Regierung von Sicherheit anzeigen. Der Schwerpunkt liegt auf dem erfolgten Ausbau der Kontroll- und Überwachungstechnologien und zeigt, wie diese von der Bevölkerung wahrgenommen werden und das Verhältnis von Bürger und Staat modulieren.

### 4.1 Sicherheitspolitik und Terrorismus

Die Terroranschläge vom 11. September 2001 haben national wie international zu tiefgreifenden sicherheitspolitischen Umbaumaßnahmen geführt. Die Rede ist von einer *Neuen Sicherheitsarchitektur* (Lange 2008; Pütter 2008; Glaeßner 2010; Gusy 2012), deren Notwendigkeit kaum in Frage gestellt wurde, sondern vielmehr als einzig richtige Antwort auf die „qualitativ neue Bedrohung“ (Lepsius 2004, S. 64) erschien. Das „qualitativ Neue“ bestand darin, dass die Bedrohung als global wahrgenommen wurde und sich nicht mehr einzelnen Akteuren zurechnen ließ (vgl. ebd., S. 67). So beginnt der Entwurf des Gesetzes zur Bekämpfung des internationalen Terrorismus (BGBl. I, S. 361) („zweites Sicherheitspaket“), welches zusammen mit dem nur kurz zuvor verabschiedeten „ersten Sicherheitspaket“ den Auftakt einer „Flut von Rechtsakten“ (Koep-Kerstin & Will 2009, S. 5) bildete, mit den folgenden Worten: „Der internationale Terrorismus hat sich zu einer weltweiten Bedrohung entwickelt. Das Ausmaß der Gewalt, die logistische Vernetzung der Täter und ihre langfristig angelegte, grenzüberschreitende Strategie erfordert die Fortentwicklung der gesetzlichen Instrumente“ (BT-Drs. 14/7386 (neu), S. 1). Politisch wurden die Terroranschläge nicht nur als „Angriff auf die Menschen in New York“, sondern auch als „Angriff auf die offene Gesellschaft“ und „unsere Demokratie“ gedeutet (BT-Protokoll 14/192, S. 18693).

Die neue Sicherheitsarchitektur folgt einer Präventionslogik – oder, wie Glaeßner (2010, S. 181) es ausdrückt, dem Leitmotiv der „Prävention durch Information“ – und ist damit auf die Akkumulation von Wissen angelegt (vgl. Huster & Rudolph 2008, S. 18). Daher setzt sie zum einen auf neue und erweiterte Befugnisse, um an Daten und Informationen zu gelangen, was nicht zuletzt durch die Einführung einer Vielzahl





neuer Kontroll- und Überwachungstechnologien möglich gemacht wird, die weitgehend im Verborgenen ablaufen. Zum anderen wurden neue nationale und internationale Allianzen geschlossen und Organisationen eingerichtet, um die gesammelten Daten und Informationen verarbeiten und austauschen zu können. Nach dem Bundesdatenschutzbeauftragten (2013, S. 105) folgen die neuen Befugnisse dem Grundsatz „Need to Share“: „Ohne konkrete Anfrage werden Informationen mit allen anderen Stellen geteilt, die vielleicht etwas damit anfangen können – Datenübermittlung auf Vorrat.“ Darüber hinaus wurden der Präventionslogik entsprechend auch Strafbarkeiten im Vorfeld weiter ausgedehnt, um im Vorbereitungsstadium eines terroristischen Anschlages noch mehr Eingriffsmöglichkeiten zu schaffen.

Somit lassen sich folgende zentrale, ineinander greifende Prinzipien der neuen Sicherheitsarchitektur bestimmen: erstens die Ausdehnung der Vorfeldkriminalisierung, zweitens die institutionelle Aufrüstung und Vernetzung der Sicherheitsbehörden sowie drittens die Einführung von neuen und die Erweiterung von bestehenden Befugnissen.

#### 4.1.1 Ausdehnung der Vorfeldkriminalisierung

Als eine der ersten Maßnahmen im sog. ersten Sicherheitspaket wurde § 129b eingeführt, welcher es erlaubte, nunmehr auch die Bildung einer kriminellen oder terroristischen Vereinigung im Ausland strafrechtlich zu verfolgen, was bislang nur im Inland möglich war. Damit fand eine räumliche Ausdehnung der zuvor schon im Vorfeld einer Rechtsgutsverletzung bestehenden Strafbarkeit statt. Zugleich wurde das Religionsprivileg im Vereinsrecht abgeschafft, wodurch die Möglichkeit geschaffen wurde, extremistische religiöse Vereinigungen zu verbieten.

Mit dem Gesetz zur Verfolgung der Vorbereitung schwerer staatsgefährdender Gewalttaten (GVVG) vom 30. Juli 2009 (BGBl. I, S. 2437) wurde das Spektrum an kriminalisierten Vorbereitungshandlungen noch deutlich erweitert. Es stellt unter anderem die Ausbildung in sogenannten Terrorcamps, das Verbreiten von Anleitungen zum Bombenbau sowie vielfältige Umgangsformen mit Gegenständen oder Stoffen, die sich zur Vorbereitung schwerer staatsgefährdender Gewalttaten eignen, unter Strafe (ausführlich dazu Puschke 2010; Radtke & Steinsiek 2010; zur Evaluation des Gesetzes Oehmichen & Klukkert 2012).

Daneben war der Tatbestand der Geldwäsche wiederholte Male Gegenstand gesetzlicher Novellierungen, um insbesondere die Bekämpfung der *Terrorismusfinanzierung* zu effektivieren (z.B. Gesetz zur Optimierung der Geldwäscheprävention vom 22. Dezember 2011, BGBl. I, S. 2959).



#### 4.1.2 Institutionelle Aufrüstung und Vernetzung der Sicherheitsbehörden

In institutioneller Hinsicht lautet die Maxime der neuen Sicherheitsarchitektur *Vernetzung*. Statt Trennungsgebot wird eine enge Kooperation zwischen Polizei und Nachrichtendiensten groß geschrieben. Wie der ehemalige Bundesinnenminister Schäuble (2008) in einer Rede auf dem 7. Symposium des Bundesamtes für Verfassungsschutz in Berlin äußerte, gründen die „Erfolge unserer Sicherheitsbehörden“ auf einem „tragfähige[n] Konzept der vernetzten Sicherheit“. Den „Netzwerken der Terroristen“ werde ein „Netzwerk unserer Sicherheitsbehörden“ entgegengesetzt (ebd.). Zu diesem Zweck wurde nicht nur die Zusammenarbeit der 38 schon existierenden Sicherheitsbehörden – 16 Landeskriminalämter, Bundeskriminalamt (BKA), Bundespolizei, Zollkriminalamt (ZKA), 16 Landesämter für Verfassungsschutz, Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND) – gestärkt, sondern es wurden auch eine Reihe neuer Organisationen geschaffen. Als Einrichtungen, die sich explizit der Bekämpfung des islamistischen Terrorismus verschrieben haben, sind das Gemeinsame Terrorismus-Abwehrzentrum (GTAZ) und das Gemeinsame Internetzentrum (GIZ) zu nennen.

Das GTAZ wurde Ende 2004 in Berlin ins Leben gerufen. Neben den 38 Sicherheitsbehörden sind auch das Bundesamt für Migration und Flüchtlinge sowie die Generalbundesanwaltschaft darin vertreten. Erklärtes Ziel des GTAZ ist die „Zusammenarbeit der Sicherheitsbehörden zur Bekämpfung des islamistischen Terrorismus“ (BMI 2011b), wofür durch die Vernetzung der beteiligten Partner optimale Voraussetzungen geschaffen worden seien. Hierdurch soll vor allem der Informationsaustausch zwischen den verschiedenen Behörden sowie die Abstimmung operativer Maßnahmen verbessert werden.

Das GIZ existiert seit Anfang 2007 – ebenfalls in Berlin – und dient der Zusammenarbeit des BfV, BKA, BND, MAD und der Generalbundesanwaltschaft im Hinblick auf die „Bekämpfung des islamistischen Terrorismus im Internet“ (BMI 2011a): Extremistische und terroristische Aktivitäten im Internet sollen dadurch frühzeitig erkannt, Anschlagsvorbereitungen aufgedeckt und internetgestützte Rekrutierungs- und Radikalisierungsbemühungen radikaler Islamisten nachvollzogen werden.

Auch die Einführung der Bundespolizei lässt sich auf 9/11 zurückführen (vgl. Ströbele & Erlenmeyer 2006, S. 137), welche aus dem Bundesgrenzschutz hervorging und dessen Befugnisse übernahm. Es kamen allerdings auch neue Aufgaben hinzu, wie z.B. als Flugsicherheitsbegleiter (sogenannte „Sky-Marshalls“) an Bord deutscher Flugzeuge für die Aufrechterhaltung von Sicherheit und Ordnung zu sorgen.

Auch auf internationaler Ebene wurde die Zusammenarbeit intensiviert. Zwar findet schon seit Mitte der 1970er Jahre eine zwischenstaatliche Kooperation der Innen- und



Justizminister der EG-Mitgliedstaaten statt – so wurde 1975 unter der Abkürzung TREVI (Terrorism, Radicalism, Extremism, Violence International) eine Arbeitsgruppe zur Terrorismusbekämpfung und polizeilichen Zusammenarbeit gegründet –, aber durch die Terroranschläge von 9/11 sowie in Madrid 2004 und London 2005 wurde die Zusammenarbeit deutlich ausgeweitet. Durch den Rat der Europäischen Union wurde am 30. November 2005 eine gemeinsame „Strategie der Europäischen Union zur Terrorismusbekämpfung“ beschlossen, welche auf den vier Säulen „Prävention“, „Verfolgung“, „Schutz“ und „Reaktion“ beruht (Europäische Kommission 2010). Unter diesem Dach finden sich u.a. weitere Strategien und Aktionspläne, Informationssysteme (VIS; SIS II), gemeinsame Standards für die Sicherheit des zivilen Luftverkehrs, der Häfen und des Seeverkehrs, der „europäische Haftbefehl“, die „europäische Beweisverordnung“ sowie zahlreiche bi- und multilaterale Abkommen, die den Informationsaustausch und -zugang zwischen den Mitgliedstaaten erleichtern.

#### 4.1.3 Einführung von neuen und Erweiterung von bestehenden Befugnissen

Die Zahl der Befugnisse der Sicherheitsbehörden, die im Dienste der Terrorismusbekämpfung eingeführt wurden, ist kaum überschaubar. So hat es eine Reihe an Verschärfungen im Ausländer- und Asylrecht gegeben, welche verstärkte Kontrollen der Betroffenen zur Folge hat.<sup>46</sup> Ebenso erfährt der Personenkreis, der Sicherheitsüberprüfungen unterworfen wird, eine stetige Ausweitung. Der Schwerpunkt der legislativen Aktivitäten liegt indes auf der Einführung und Ausweitung von Kontroll- und Überwachungstechnologien, mit denen bislang nicht bzw. nicht auf diese Weise erhobene Daten erfasst und zusammengeführt werden. Diese stehen im Mittelpunkt dieses Abschnittes und lassen sich in vier Kategorien einteilen: (1) Um Finanzströmen von Terroristen auf die Spur zu kommen, erfolgt der Zugriff und Austausch von Bankdaten; (2) durch eine stärkere Kontrolle des Reiseverhaltens sollen Terroristen an der Einreise ge- und Anschläge verhindert werden; (3) zur Aufdeckung von Anschlagplanungen wurden vielfältige Möglichkeiten zur Registrierung des Kommunikationsverhaltens sowie deren Inhalte geschaffen; (4) darüber hinaus werden Datenbanken und Listen mit „Terrorverdächtigen“ geführt, in denen teilweise Reise-, Bank- und Kommunikationsdaten zusammenlaufen sowie weitere Daten registriert und ausgetauscht werden.

---

<sup>46</sup> So ist z.B. der komplette Datenbestand des Ausländerzentralregisters von Polizei und Sicherheitsbehörden online abrufbar. Auch findet ein automatisierter Abgleich zwischen der jüngst in Betrieb genommenen Visa-Warndatei und der Antiterrordatei statt.



#### 4.1.3.1 Erfassung von Bankdaten

Im Rahmen des zweiten Sicherheitspaketes wurde das *Kontenabrufverfahren* eingeführt. Kreditinstitute wurden dazu verpflichtet, eine besondere Datei zu führen, aus der die Kontostammdaten der Bankkunden durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) online abrufbar sind (vgl. Schaar 2009, S. 166f.). Das Verfahren war ursprünglich lediglich zur Bekämpfung des internationalen Terrorismus und der Geldwäsche bestimmt. 2003 wurde die Befugnis durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I, S. 2928) jedoch auf Finanzämter und weitere Behörden ausgedehnt. Welche weiteren Behörden das sind, ist im Gesetz nicht eindeutig festgelegt. Die Zugriffsschwellen wurden mit der Zeit immer weiter gesenkt. Seit Januar 2013 gehören auch Gerichtsvollzieher zum Kreis der Berechtigten, die eine Abfrage vornehmen können (vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2013, S. 127ff.). Die Nutzung dieser Maßnahme steht also in keinem Zusammenhang mehr mit der ursprünglichen Zielsetzung dieser Befugnis zur „Austrocknung der Finanzströme des Terrorismus“ (ebd., S. 129).

Tabelle 3: Abrufe von Bankkontodaten durch verschiedene Behörden 2004 bis 2012

Behörde	2004	2005	2006	2007	2008	2009	2010	2011	2012
BaFin	1.380	632	972	472	277	547	1.371	757	992
Polizei-behörden	26.212	38.675	47.805	54.111	46.132	52.367	58.477	69.330	68.066
Finanz-behörden	6.057	10.008	11.838	13.061	10.936	11.691	13.673	13.122	13.286
Staats-anwalt-schaften	3.038	7.494	12.861	18.002	18.520	20.915	23.765	25.997	24.629
Zollbe-hörden	2.251	5.160	7.202	7.167	7.604	6.198	8.054	7.316	7.207
Sonstige	479	441	478	747	469	158	275	386	184
gesamt	39.417	62.410	81.156	93.560	83.938	91.876	105.615	116.908	114.364

Quelle: Jahresberichte 2004 – 2012 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)



Die BaFin hat die Pflicht, die Zahl der Abrufe zu registrieren. Tabelle 3 stellt die Zahl der Abfragen aufgeschlüsselt nach Jahren und Auskunft ersuchender Behörde dar und zeigt, wie stark die Nutzung dieser Befugnis zugenommen hat.<sup>47</sup>

Auf internationaler Ebene existiert seit 2010 ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des Programms der USA zum Aufspüren der Finanzierung des Terrorismus („SWIFT-Abkommen“). Damit hat die USA Zugriff auf Informationen über fast den gesamten grenzüberschreitenden Zahlungsverkehr in Europa, der über den Finanzdienstleister SWIFT (Society for Worldwide Interbank Financial Telecommunication) abgewickelt wird. Darüber, wie oft von dieser Befugnis Gebrauch gemacht wird, existieren keine Informationen. In der Kritik steht dieses Abkommen vor allem deshalb, weil SWIFT nicht in der Lage ist, auf spezifische Daten aus einzelnen Transaktionen zuzugreifen und daher ganze Datenpakete übermittelt, die in den USA fünf Jahre lang gespeichert und verwendet werden dürfen (vgl. Leopold 2011, S. 42f.).

#### 4.1.3.2 Erfassung des Reiseverhaltens

Im November 2005 wurde der *elektronische Reisepass* (ePass) in Deutschland eingeführt, der als erstes biometrisches Merkmal ein auf einem Mikrochip gespeichertes digitales Lichtbild enthält. Seit November 2007 werden zusätzlich zwei Fingerabdrücke im Chip gespeichert. Politisch durchgesetzt wurde der biometrische Reisepass durch eine EG-Verordnung, an der der ehemalige Bundesinnenminister Otto Schily maßgeblich beteiligt war (vgl. Selbmann 2008, S. 13). Auf nationaler Ebene ließ sich die biometrische Erfassung von Reisenden zuvor nicht durchsetzen (vgl. Busch 2006, S. 29f.; Kurz 2008, S. 102). 2015 verlieren die letzten alten Reisepässe ihre Gültigkeit, so dass in naher Zukunft eine vollständige Umstellung stattgefunden haben wird und nur noch biometrische Pässe im Umlauf sein werden.

Seit 2007 gilt das sogenannte „PNR-Abkommen“ zwischen der EU und den USA, welches Fluggesellschaften dazu verpflichtet, die *Fluggastdaten* von USA-Reisenden an das Department of Homeland Security (DHS) zu übermitteln, welche dort 15 Jahre lang gespeichert werden. Diese enthalten persönliche Daten wie Name, Geburtsdatum, Geschlecht, Staatsangehörigkeit, Adresse, Telefonnummer sowie sämtliche Angaben zum genauen Reiseverlauf sowie der Buchung (u.a. auch spezielle Essenswünsche).

---

<sup>47</sup> Der vermeintlich starke Rückgang, den der Vergleich der Abfragen des Jahres 2008 mit dem Vorjahr indiziert, ist auf eine technische Umstellung in der ersten Jahreshälfte zurückzuführen, aufgrund dessen das Verfahren temporär nicht richtig funktionierte (vgl. Bundesanstalt für Finanzdienstleistungsaufsicht 2009, S. 209).



Ein ähnliches Abkommen besteht seit 2011 zwischen der EU und Australien. Weitere PNR-Abkommen mit anderen Ländern sind in Planung (derzeit Kanada) ebenso wie ein eigenes EU-PNR-System für innereuropäische Flüge.<sup>48</sup> Im Zuge des Dritten Gesetzes zur Änderung des Bundespolizeigesetzes vom 22. Dezember 2007 (BGBl. I, S. 3214) werden zudem seit 2008 die Fluggastdaten von den Fluggesellschaften an die Bundespolizei übermittelt und unterliegen einer Speicher- und Löschfrist von 24 Stunden. Ebenso werden seit 2010 *Schiffspassagierdaten* erhoben, für die allerdings keine festen Speicher- und Löschfristen existieren.

#### 4.1.3.3 Erfassung des Kommunikationsverhaltens und deren Inhalte

Im Rahmen des zweiten Sicherheitspaketes wurde dem Bundesamt für Verfassungsschutz und dem Militärischen Abschirmdienst die Befugnis zum Einsatz des *IMSI-Catchers* erteilt, welcher 2002 in die Strafprozessordnung aufgenommen wurde und von Strafverfolgungsbehörden generell zu Fahndungszwecken verwendet wird. Mit diesem Gerät lässt sich sowohl die Kartenummer (IMSI) als auch der aktuelle Standort eines eingeschalteten Mobiltelefons feststellen.<sup>49</sup> Dabei senden alle eingeschalteten Mobiltelefone im Einzugsbereich des IMSI-Catchers ihre Daten an diesen (Will 2006). Bei hoch frequentierten Veranstaltungen wie z.B. einer Demonstration können davon sehr viele Personen betroffen sein. Eine Klage der Humanistischen Union gegen den Einsatz des IMSI-Catchers, weil er die Grundrechte aller, die sich in seinem Einzugsbereich befinden, sowie das Fernmeldegeheimnis verletze (vgl. ebd.), wurde vom Bundesverfassungsgericht zurückgewiesen.

Das Parlamentarische Kontrollgremium muss den Bundestag jährlich über den Einsatz der Maßnahmen nach dem Terrorismusbekämpfungsgesetz unterrichten. Danach erfolgte im Bereich des Bundesamtes für Verfassungsschutz eine Anwendung des IMSI-Catchers zur Abwehr terroristischer Gefahren 2002 dreimal, 2003 und 2007 jeweils neunmal, 2004, 2005 und 2006 jeweils zehnmal, 2008 und 2011 in 14 sowie 2009 und 2010 in 16 Fällen (vgl. BT-Drs. 17/12774, S. 7).<sup>50</sup> 2012 wurde der IMSI-Catcher vom

---

<sup>48</sup> Nach dem Bundesdatenschutzbeauftragten (2013, S. 40) ist sogar ein Abgleich der Daten aller Passagiere mit vordefinierten Risikoprofilen vorgesehen, worin er eine verfassungsrechtlich höchst bedenkliche „Nähe zur Rasterfahndung“ sieht.

<sup>49</sup> Analog wird ein sogenannter *WLAN-Catcher* genutzt, mit dem Netzwerkanschlüsse von Computern ermittelt werden können, ohne dass eine separat geschaffene Befugnis hierfür existiert (Apell & Lüders 2011).

<sup>50</sup> In der Unterrichtung durch das Parlamentarische Kontrollgremium heißt es: „Grund für den IMSI-Catcher-Einsatz waren terroristische Aktivitäten der Betroffenen und Gefahren für die auswärtigen Belange der Bundesrepublik Deutschland durch Gewaltanwendung bzw. darauf gerichtete Vorbereitungshandlungen sowie Bestrebungen, die gegen den Gedanken der Völkerverständigung, insbesondere das friedliche Zusammenleben der Völker, gerichtet waren.“ (BT-Drs. 17/12774, S. 7)



BfV ebenfalls 16-mal sowie in der ersten Hälfte 2013 18 mal eingesetzt (vgl. BT-Drs. 17/14714, S. 5).

Ähnlich werden auch sogenannte *stille SMS* dazu genutzt, Mobiltelefone zu orten, ohne dass deren Besitzer davon etwas bemerken. Eine Kleine Anfrage der Linken (BT-Drs. 17/14515) ergab, dass diese weitaus häufiger angewendet werden als der IMSI-Catcher. So versendete das BfV 2012 28.843 stille SMS und beinahe ebenso viele (28.472) in der ersten Hälfte 2013 (vgl. BT-Drs. 17/14714, S. 3). Die Nutzungshäufigkeiten stiller SMS durch BKA (2012: 37.352; bis 6/2013: 31.948) und Bundespolizei (2012: 63.354; bis 6/2013: 65.449) liegen noch weit darüber. Eine weitaus intensivere Nutzung erfolgt durch die Zollbehörden (2012: 199.023; bis 6/2013: 138.779). Wie oft der BND davon Gebrauch gemacht hat, erfährt man indessen nicht, da dies als geheim eingestuft und daher unter Verschluss gehalten wurde. Ebenso bleibt unbekannt, in welchem Kontext – Prävention von Terrorismus oder anderer Kriminalitätsformen – die durchgeführten Ortungen mittels stiller SMS standen, und zu welchen Ermittlungserfolgen diese führten. Blickt man auf die Länderebene, zeigt sich ein noch größeres Ausmaß dieser Praxis. So wurden 2011 allein in Nordrhein-Westfalen über 250.000 stille SMS von Strafverfolgungsbehörden verschickt.<sup>51</sup>

2005 wurde die *akustische Wohnraumüberwachung* in modifizierter Form<sup>52</sup> wieder eingeführt, nachdem sie 2004 vom Bundesverfassungsgericht für verfassungswidrig erklärt worden war. Das heimliche Abhören von Wohnungen ist auch unter dem Begriff „großer Lauschangriff“ bekannt. „Die akustische Wohnraumüberwachung hat sich als unverzichtbar erwiesen, um die strafrechtliche Bekämpfung der organisierten Kriminalität, des Terrorismus und anderer schwerer Formen von Kriminalität zu verbessern“, heißt es in der Gesetzesbegründung (BR-Drs. 722/04, S. 1). Die Bundesregierung ist verpflichtet, den Deutschen Bundestag jährlich über den Einsatz technischer Mittel zur Überwachung von Wohnungen zu unterrichten (vgl. z.B. für 2011 BT-Drs. 17/10601). Seit der Neuregelung wird die akustische Wohnraumüberwachung in nicht mehr als zehn Verfahren pro Jahr eingesetzt. Zuvor lagen die Nutzungshäufigkeiten weitaus höher (z.B. 2003 in 37 Verfahren; vgl. BT-Drs. 15/3699).

Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I, S. 3198) wurde die *Vorratsdatenspeicherung* von Telefon- und Internetverbindungsdaten eingeführt. In Deutschland wurde die Vorratsdatenspeicherung durch das Urteil des Bundesverfassungsgerichts vom 2. März 2010

---

<sup>51</sup> Matthias Monroy: Jährlich eine Viertelmillion ‚Stille SMS‘, in: *Telepolis*, 22.11.2011. Verfügbar unter <http://www.heise.de/tp/artikel/35/35905/1.html> [24. September 2013]

<sup>52</sup> Wesentliche Neuregelungen bestehen darin, dass der Anlasstatenkatalog reduziert wurde und gewährleistet sein muss, dass der Kernbereich privater Lebensgestaltung gewahrt bleibt.



für verfassungswidrig erklärt. Das Gesetz erlaubte den Zugriff auf Vorratsdaten nicht nur zur Verfolgung von Straftaten mit erheblicher Bedeutung, sondern auch mittels Telekommunikation begangener Straftaten. Der Anwendungsbereich ging also deutlich über die Terrorismusbekämpfung hinaus.

Die EU-Richtlinie verlangt von den Mitgliedstaaten die Speicherung von Daten, „die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden“ (Amtsblatt der Europäischen Union 2006, S. L 105/54). Anhand dieser Daten lässt sich feststellen, wer mit wem wann und wie lange telefoniert hat und wer mit wem wann in E-mail- oder SMS-Kontakt stand. Bei der Handynutzung wird zudem der Standort registriert.

Die Zugriffe auf Verkehrsdaten werden vom Bundesamt für Justiz statistisch erfasst, wobei allerdings nicht zwischen anlasslos und aus anderen Gründen gespeicherten Verkehrsdaten unterschieden wird. 2008 wurde in 13.904 Fällen nach § 100g StPO darauf zugegriffen, 2009 stiegen die Fallzahlen auf 16.226 und sanken 2010 auf 12.576, woraufhin 2011 wieder ein Anstieg auf 14.153 zu verzeichnen war (vgl. Bundesamt für Justiz 2009-2012). Es zeigt sich also, dass mit der 2010 erfolgten Stoppung der anlasslosen Speicherung die Zugriffe zunächst zurückgingen, aber schon im Folgejahr wieder anstiegen, so dass trotz des BVerfG-Urteils kein drastischer Rückgang der Nutzung von Verkehrsdaten stattgefunden hat und diese auch ohne Vorratsdatenspeicherung reichlich vorhanden zu sein scheinen.

Mit dem Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKA-Gesetz) vom 25. Dezember 2008 (BGBl. I, S. 3083) wurde dem BKA die Befugnis zur *Online-Durchsuchung* – dem verdeckten Zugriff auf private Computer – eingeräumt. Mit diesem Instrument lassen sich nicht nur Inhalte der Internet-Kommunikation, sondern sämtliche Daten, die sich auf der Festplatte befinden, einsehen. Gegen die Online-Durchsuchung wurde wiederholt Klage eingereicht, sie ist gegenwärtig allerdings noch zulässig. Durch das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 wurde die Eingriffsschwelle erhöht. Die Online-Durchsuchung wurde unter Richtervorbehalt gestellt, der „Kernbereich privater Lebensgestaltung“ muss geschützt bleiben und es müssen „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen“ (Britz 2008, S. 411). Zudem wurde das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme neu geschaffen. Wie einst das Recht auf informationelle Selbstbestimmung im Zuge des Volkszählungsurteils wurde auch dieses Grundrecht aus dem allgemeinen Persönlichkeitsrecht abgeleitet. Mit Erhard Denninger (2009, S. 23; Herv. i. O.) ist darin insofern eine positive Entwicklung zu sehen, als dass das neue Grundrecht „den Einzelnen [...] vor Persönlichkeitsgefährdungen, die durch den heimlichen Zugriff auf sein IT-System *als Ganzes* verursacht





werden“, schützt. Kritische Stimmen bezweifeln jedoch, dass es den Grundrechtsschutz tatsächlich stärkt, da, so etwa Kutscha (vgl. 2008, S. 1044), die Aussagen des Bundesverfassungsgerichts zur Reichweite des neuen Grundrechts angesichts einer immer mehr personenbezogene Daten generierenden Kommunikationsinfrastruktur wenig eindeutig seien.

Darüber, wie häufig diese Maßnahme praktiziert wird, wird keine (öffentlich zugängliche) Statistik geführt. Lediglich der Antwort der Bundesregierung auf eine Kleine Anfrage der Linken (BT-Drs. 17/7104) aus dem Jahr 2011 ist zu entnehmen, dass eine Online-Durchsuchung durch das BKA bis zu diesem Zeitpunkt in sieben Fällen angeordnet worden war (BT-Drs. 17/7760, S. 10). Im 24. Tätigkeitsbericht des Bundesdatenschutzbeauftragten (2013, S. 95) ist von sechs Online-Durchsuchungen die Rede.

Darüber hinaus wurde dem BKA auch die Befugnis zur Quellen-Telekommunikationsüberwachung erteilt, welche allerdings nur zur Terrorismusbekämpfung und nicht zur Strafverfolgung eingesetzt werden darf. Mit dieser Maßnahme ist es möglich, über IP-Telefonie (z.B. Skype) geführte Gespräche abzuhören, indem heimlich eine Software auf dem Computer installiert wird. Bei der Kontrolle der bislang durchgeführten vierzig Quellen-Telekommunikationsüberwachungen hat der Bundesdatenschutzbeauftragte (ebd., S. 94) „Mängel bei der technischen Absicherung der Maßnahmen und den Lösungsmechanismen für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung festgestellt.“

#### *4.1.3.4 Erfassung von „Terrorverdächtigen“*

Die Antiterrordatei wurde im März 2007 im GTAZ in Betrieb genommen und ist eine gemeinsame Datenbank der 38 oben bereits erwähnten Sicherheitsbehörden, in der sämtliche Angaben über Personen gesammelt werden, über die sich durch Querverweise ein Verdacht auf geplante Attentate erhärten könnte. Dies sind unter anderem: Zugehörigkeit zu terroristischen Vereinigungen, Waffenbesitz, Telekommunikations- und Internetdaten, Bankverbindungen, Schul- und Berufsausbildung, Arbeitsstelle, Familienstand, Religionszugehörigkeit, Verlust von Ausweispapieren, Reisebewegungen und bekannte Aufenthalte an Orten mit terroristischem Hintergrund (z.B. Ausbildungslager). Darüber hinaus enthält diese Datei ein Freitextfeld, das im Umfang nicht begrenzt ist.

Seit ihrer Einführung hat der Bestand stetig zugenommen. Im März 2007 waren rund 13.000 Personensätze in der Datenbank erfasst, Ende Mai 2008 waren es bereits 17.745 (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2009, S. 51) und im Juni 2011 18.280 (BT-Drs. 17/6223, S. 7). Bei einer Kontrolle der Antiterrordatei hat der Bundesdatenschutzbeauftragte Mängel festgestellt.



So wurden Datensätze, die gelöscht werden sollten, weiterhin vorgehalten und Freitextfelder enthielten unzulässige Bearbeitervermerke (vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2011, S. 84). Im April 2013 wurde die Antiterrordatei teilweise für verfassungswidrig erklärt und muss bis Ende des Jahres 2014 novelliert werden.

Darüber hinaus gibt es sowohl auf EU- als auch auf UN-Ebene sogenannte „*Terrorlisten*“, in denen als terroristisch eingestufte Gruppen und Einzelpersonen erfasst sind (vgl. Gericke 2011, S. 160). Sie zielen darauf ab, die Finanzierung von Terrorismus zu verhindern (vgl. Aden 2013, S. 264). Die Kritik an den Listen bezieht sich in erster Linie auf deren intransparentes Zustandekommen (vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2013, S. 101). Diverse Klagen gegen diese Listen hatten bislang keine Auswirkungen auf deren grundsätzliches Fortbestehen.<sup>53</sup>

Ein multilaterales Abkommen – der Prümer Vertrag vom 5. Dezember 2006, der zwischen Deutschland, Frankreich, Spanien, Österreich und den Benelux-Ländern geschlossen wurde –, sieht die – so der Titel – „Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration“ vor und erlaubt unter anderem den Austausch von Daten über „terroristische Gefährder“. Diesem Abkommen treten sukzessive weitere EU-Mitgliedstaaten bei.

Seit 2009 erlaubt ein bilaterales Abkommen zwischen Deutschland und den USA zur Verhinderung terroristischer Straftaten die Übermittlung personenbezogener Informationen von „Terrorverdächtigen“. Sowohl der Prümer Vertrag als auch das Gesetz zu dem Abkommen vom 1. Oktober 2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität (BGBl. II, S. 1010) ermöglichen den beteiligten Ländern einen Online-Abruf von biometrischen Daten (DNA-Profile und Fingerabdrücke).

Diese Aufzählung an neuen und erweiterten Befugnissen, die im Kontext der Terrorismusbekämpfung stehen, ist keineswegs erschöpfend. Wechselt man auf die Ebene des Polizei- und Ordnungsrechts der Länder, auf der sich prinzipiell dieselben Entwicklungen abzeichnen, gerät noch eine Reihe weiterer Maßnahmen in den Blick. Zu nennen sind präventiv-polizeiliche Rasterfahndung, Schleierfahndung, (automatisierte) Videoüberwachung, Kfz-Kennzeichen-Screening (vgl. Saurer 2005, S. 278f.).

Darüber hinaus findet auch eine Art „Testbetrieb“ neuer Kontroll- und Überwachungstechnologien statt, die sich noch in der Entwicklung befinden. So erprobte das BMI ab September 2010 am Hamburger Flughafen Körperscanner, mit welchen das Ziel

---

<sup>53</sup> Dazu ausführlich: de Goede (2012).



verbunden wird, Anschlagversuche wie jenen von Detroit am 25. Dezember 2009 verhindern zu können. Nach zehn Monaten wurde der Versuch aufgrund hoher Fehlerquoten beendet. Seit März 2013 wird an den Flughäfen Hamburg und Frankfurt ein weiterentwickelter Körperscanner getestet.

Am Hauptbahnhof Mainz führte das BKA ab Oktober 2006 vier Monate lang ein Pilotprojekt mit einem Videoüberwachungssystem zur biometrische Gesichtserkennung durch, welches die Fahndung nach Terroristen und Straftätern erleichtern soll. Diese Technologie hat sich jedoch als nicht tauglich erwiesen.

Dieser Abriss über die gesetzgeberischen Maßnahmen nach 9/11 und insbesondere die neu eingeführten Kontroll- und Überwachungstechnologien hat gezeigt, dass diese rechtlich höchst umstritten sind. Im bürger- und datenschutzrechtlichen Diskurs herrscht weitgehend Einigkeit darüber, dass die legislativen Änderungen seit 9/11 nicht nur an die rechtsstaatlichen Grenzen gehen, sondern diese überschreiten. Inzwischen ist es keine Seltenheit mehr, dass das Bundesverfassungsgericht korrigierend eingreifen muss. Gegen eine beachtliche Zahl an Gesetzen wurde Klage eingereicht, etliche Befugnisse wurden eingeschränkt oder für verfassungswidrig erklärt, weil sie Grund- und Bürgerrechte verletzen.

Zwar wurden einige Gesetze mit einer Evaluierungs- und Befristungsklausel versehen. Diese sollten „als Korrektiv zum sehr beschleunigten Gesetzgebungsverfahren, gleichsam als Übereilungsschutz“ dienen, heißt es im 54-seitigen Evaluierungsbericht der Bundesregierung (2005, S. 53) des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002. Im Rahmen der Evaluation dieses Gesetzes, welche von der Bundesregierung selbst durchgeführt wurde, wurden alle Maßnahmen um weitere fünf Jahre verlängert. Die meisten Regelungen wurden mit der Begründung entfristet, dass sie aufgabendienliche Erkenntnisse erbracht hätten, ohne dass damit unangemessen breite Überwachungsfolgen verbunden gewesen seien (vgl. ebd., S. 10). Ebenso wurden Regelungen beibehalten, von denen noch gar kein Gebrauch gemacht wurde. Daher bleibt es den Nachweis seiner Effizienz schuldig.<sup>54</sup> Auch die 2010 erfolgte erneute Evaluation lässt adäquate Kriterien vermissen und wird selbst vom Bundesdatenschutzbeauftragten (2013, S. 91) als „unzureichend“ beurteilt. Zwar wurde diese extern in Auftrag gegeben, allerdings an eine Unternehmensberatung (Rambøll Management GmbH) und nicht einen wissenschaftlichen Sachverständigen, wie im Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I, S. 2) vorgesehen (vgl. Will 2011).

---

<sup>54</sup> Für eine ausführliche Kritik des Evaluationsverfahrens vgl. Gusy (2007, S. 283ff.).



Lediglich zwei Befugnisse, die noch nie zur Anwendung kamen, wurden gestrichen (Postfächer-Abfrage sowie Lauschangriff in einer Wohnung zum Schutz eines Spitzels), während alle übrigen im Rahmen des Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes vom 7. Dezember 2011 (BGBl. I, S. 2576) erneut verlängert und teilweise noch erweitert wurden (vgl. Busch 2012, S. 24).

Nun sagt die Gesetzgebung selbst noch wenig über die konkrete Praxis der Ermittlung und Strafverfolgung aus. Sie ist erst einmal eine Ermöglichung durch Befugnisse. Der tatsächliche Nachweis über den Einsatz und Nutzen der Befugnisse ist im doppelten Sinne nicht leicht zu erbringen: Nicht nur liegt die Kausalität zwischen einer Maßnahme und einer Überführung von mutmaßlichen Straftätern immer auf der Hand, vielmehr sind Zahlen hierzu auch kaum öffentlich zugänglich. So werden diesbezügliche Informationen, die etwa im Rahmen von Anfragen von der Bundesregierung erbeten werden, häufig mit dem Verweis auf das staatliche Geheimhaltungsinteresse unter Verschluss gehalten. Begründet wird dies damit, dass Informationen, die die „Arbeitsweise und Methodik der Sicherheitsbehörden“ und insbesondere „Aufklärungsaktivitäten und Analysemethoden“ tangieren, geheimhaltungsbedürftig seien, um die Effektivität der Maßnahmen aufrechtzuerhalten (BT-Drs. 17/14714, S. 1f.). In dieser Logik verbietet sich ein Nachweis der Wirksamkeit also, um eben diese in der Zukunft nicht zu gefährden. Mit Christoph Gusy (2004) kann man gegen dieses Argument indes auch einwenden, dass die Kontrolle der Geheimdienste deren Arbeit weniger beeinträchtigt, als sie vielmehr effektiver macht, nämlich „im Interesse eines wirksamen Schutzes von Freiheit und Demokratie“.

Man kann sich dieser Frage nach der Wirksamkeit von Sicherheitsgesetzen aber zum einen auch mit Plausibilitätsrekonstruktionen und zum anderen sozialwissenschaftlich mit der Analyse entsprechender Mechanismen annehmen. Nehmen wir das Beispiel der biometrischen Ausweisdokumente. Obwohl im Zuge der Sicherheitsgesetze zur Bekämpfung eines international operierenden Terrorismus eingeführt, erschließt sich der konkrete Bezug der Integration von biometrischen Daten im deutschen eReisepass und ePersonalausweis zunächst einmal kaum – „al-Quaida-Strukturen lassen sich mit der Einführung biometrischer Ausweise für deutsche Staatsbürger jedenfalls nicht aufdecken.“ (Büsching 2010, S. 130) Tatsächlich ist der Abgleich der verschlüsselten biometrischen Daten des Fingerabdrucks auf diesen Ausweispapieren bislang auch nur zur Überprüfung der Echtheit des Dokuments sowie zur Identitätsprüfung erlaubt.<sup>55</sup>

---

<sup>55</sup> Die Gesetze zur Änderung des Passgesetzes vom 20. Juli 2007 (BGBl. I, S. 1566) und des Personalausweisgesetzes vom 18. Juni 2009 (BGBl. I, S. 1346) verbieten ausdrücklich die Speicherung von Fingerabdrücken in zentralen Datenbanken. Und anders als der Bundesrat, der in seiner Stellungnahme zum Gesetzesentwurf zur Änderung des Passgesetzes (BT-Drs. 16/4138) die Notwendigkeit von Referenzdateien zur effektiven Identitätsüberprüfung betont (BT-Drs. 16/4456, S. 3), spezifiziert die Bundesregierung in ihrer Gegenäußerung den Fingerab-



Doch auch hier wurden zunächst Zweifel laut, nicht zuletzt weil der deutsche Pass schon vorher zu den (fälschungs-)sichersten Ausweisdokumenten zählte. Überdies argwöhnten Kritiker der Einführung des Fingerabdrucks, dass der besondere Nutzen biometrischer Daten auf lange Sicht kaum erkennbar sei, wenn diese nicht zumindest dezentral gespeichert und polizeilich zugänglich gemacht würden (z.B. Petra Pau, BT-Protokoll 14/195, S. 19020). Bis 2007 schien dies angesichts unbestimmter rechtlicher Regelungen auch prinzipiell möglich.<sup>56</sup> Im Rahmen der Strafverfolgung bzw. bei Verkehrsordnungswidrigkeiten ermöglicht wurde indes mittlerweile die (auch automatisierte) Übermittlung von Lichtbildern durch die Pass- an die Polizei- und Ordnungsbehörden.<sup>57</sup> In diesem Sinne wäre die weitere Entwicklung mit Blick auf das zu beobachten, was die wissenschaftliche Literatur als „function creep“ bezeichnet, also gewissermaßen als schleichende Funktionserweiterung entweder durch die nicht beabsichtigte oder autorisierte Nutzung gespeicherter Daten (Mordini 2009) oder im Zuge der retrospektiven Entdeckung und Legalisierung von Nutzungsmöglichkeiten.

In diese Reihe fügen sich noch weitere Maßnahmen ein, deren Einführung klar in den Kontext der Terrorismusbekämpfung gestellt, diese Zweckbindung mit der Zeit allerdings gelockert wurde. Ein besonders offensichtliches Beispiel ist das Kontenabrufverfahren, welches in vielen Fällen zur Adressfeststellung und damit als Ersatz für ein nicht existentes Bundesmelderegister genutzt wird (vgl. Lüdemann & Schlepper 2011, S. 120). Ein weiteres Beispiel ist die Vorratsdatenspeicherung, deren Nutzung auch für die Verfolgung von Straftaten, die mittels Telekommunikation begangen wurden, erlaubt wurde. Treffend bezeichnet Frankenberg (2010, S. 248) „Terrorismus als Türöffner“ und stellt fest: „Gesetze sollen den Kampf aufnehmen gegen alles, was immer auch bedrohlich erscheinen könnte: ‚Organisierte Kriminalität‘, Geldwäsche und Drogenhandel, Steuerhinterziehung, Asylmissbrauch und Schwarzarbeit sowie, nicht zu vergessen, den internationalen Terrorismus“ (Frankenberg 2006, S. 59).

Ferner lässt sich in der Tat eine generelle Verschiebung hin zu präventionsstaatlichen Prinzipien verzeichnen, indem der allgemeine „Verdacht zum Ermittlungsgrund“ wird (Büsching 2010, S. 168). Faktisch betroffen waren auch hier bestimmte Gruppierungen (Eckert 2007).

---

druckabgleich als eine 1:1-Verifikation und lehnt eine Identifizierung im Sinne eines 1:n-Abgleichs ab (ebd., S. 5).

<sup>56</sup> Siehe etwa den 19. Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz (2003, S. 22).

<sup>57</sup> § 22a des Passgesetzes („Datenübertragung und automatisierter Abruf von Lichtbildern“) und § 24 („Verwendung im Personalausweisregister gespeicherter Daten“) und § 25 („Datenübertragung und automatisierter Abruf von Lichtbildern“) des Personalausweisgesetzes.



Besonders deutlich ist dies bei der Rasterfahndung, die nach dem 11. September auf der Suche nach „Schläfern“ „gegen die pauschal verdächtige Gruppe junger Muslime durchgeführt wurde“, ohne dass eine konkrete Straftat vorlag (Büsching 2010, S. 136). Während diese Maßnahmen heftiger Kritik ausgesetzt waren und eine Ausnahme blieben,<sup>58</sup> ist das präventionsstaatliche Prinzip der Ermöglichung staatlicher Interventionen aufgrund eines verallgemeinerten Verdachts und abstrakter Bedrohungslagen mit den Sicherheitspaketen gesetzlich verankert worden. Erhard Denninger (2008, S. 95; Herv. i. O.) erkennt in dieser Entwicklung eine gewisse „Maß- und Grenzenlosigkeit“, die das „Sicherheitsideal“ selbst hervorbringt und in der sich das Verhältnis von Freiheit und Sicherheit tendenziell verkehrt: „Die Grundrechte des Bürgers werden nicht mehr in erster Linie als Grundfreiheiten und Abwehrrechte gegen staatliche Eingriffe wahrgenommen; sie verwandeln sich [...] in primäre *Schutzpflichten des Staates* und damit in Eingriffsermächtigungen.“

Zwei legislative Entwicklungen sind hier abschließend hervorzuheben, die ihrerseits vielleicht Extrempunkte, als solche indes keineswegs Marginalien markieren. Bezeichnend ist vielmehr, dass der politische Diskurs selbst maßgeblich zu elementaren Verschiebungen in der Auffassung des Grundgesetzes geführt hat. Das betrifft zum einen die sog. Folterdebatte,<sup>59</sup> die mittelfristig die Vorlage für eine Neukommentierung des Grundgesetzes im Jahr 2003 bildete, in der Matthias Herdegen (2003, Rdn. 17) Gehalt und Geltung der Menschenwürdegarantie zwar auf „die (unantastbare) Verankerung im Verfassungstext und die Exegese der Menschenwürde als Begriff des positiven Rechts“ festgelegt wissen wollte, sie im gleichen Zuge jedoch auf je „konkrete Umstände“ verwies (vgl. ebd., Rdn. 50; für eine ausführliche Kritik: Böckenförde 2006).

Zum anderen betrifft es die Diskussion um die Änderung des sog. Luftsicherheitsgesetzes im Sinne des Bundeswehreinsetzes im Inneren. Zweifelsohne schon lange ein Projekt der CDU/CSU, nahm der damalige Innenminister Otto Schily im Jahr 2003 den Vorfall eines verirrten Motorseglers, der über der Frankfurter Innenstadt schwebte, zum Anlass für eine entsprechende Gesetzesinitiative. Vorbild war zweifelsohne das Szenario von 9/11, das diese konkrete Konstellation zum Passepartout machte, um den Abschuss eines entführten Flugzeuges – und damit den Einsatz von Kampfjets und also der Streitkräfte im Inneren – rechtlich zu legitimieren.

Der Erste Senat des Bundesverfassungsgerichts annullierte im Jahr 2006 die Änderung des Luftsicherheitsgesetzes, zum einen formal mit Verweis auf die fehlende Zuständigkeit des Parlaments für eine solch weitreichende Entscheidung und zum anderen

---

<sup>58</sup> Rasterfahndung: Gigantischer Aufwand. *Spiegel Online*, 11. März 2002. Verfügbar unter <http://www.spiegel.de/unispiegel/studium/rasterfahndung-gigantischer-aufwand-a-186636.html> [12. September 2013].

<sup>59</sup> Stellvertretend etwa: Beestermöller & Brunkhorst (2006).



materiell, indem es den Abschuss eines Flugzeugs, der das Leben unbeteiligter Passagiere opfere, um eine größere Anzahl von Menschenleben zu retten, für verfassungswidrig erklärte.

Als die öffentliche Debatte über den Abschuss von Passagierflugzeugen eigentlich schon längst vom Tisch war und sich überdies die terroristische Bedrohung in Deutschland eher in verstreuten, regionalen Gruppierungen gezeigt hatte, entschied der Zweite Senat des Bundesverfassungsgerichts am 3. Juli 2012 (BVerfG, 2 PBvU 1/11) anlässlich eines von der CDU/CSU angestrebten Normenkontrollverfahrens, wenig beachtet von der Öffentlichkeit und gleichsam „ohne Not“ positiv über den Kampfeinsatz der Streitkräfte im Inneren<sup>60</sup> – und gab damit ein elementares Stück des politischen Selbstverständnisses der Bundesrepublik preis. Selbst wenn das Gericht strenge Auflagen gemacht hat – der Einsatz der Bundeswehr darf nur ein allerletztes Mittel sein, und zwar nur in „ungewöhnlichen Ausnahmesituationen katastrophischen Ausmaßes“, also nicht etwa bei Großdemonstrationen; ferner ist der Verteidigungsminister nicht allein entscheidungsbefugt, sondern nur das gesamte Bundeskabinett –, ist Terrorismusbekämpfung, und das heißt der Einsatz der Streitkräfte für militärische und letztlich politische Zwecke, nunmehr prinzipiell mit dem gesamten Arsenal von Luftwaffe, Marine und Heer erlaubt. Kritische Beobachter befürchten sogar, dass die Aufhebung des für das deutsche Verfassungsverständnis so elementaren Trennungsgabotes zwischen Polizei und Militär eine weitere Entgrenzung der Befugnisse nach sich ziehen wird.<sup>61</sup>

Bei der Sichtung der jüngeren Sicherheitsgesetzgebung wurde deutlich, dass der Schwerpunkt auf der Schaffung informationeller Eingriffsbefugnisse liegt, von deren überwiegender Mehrzahl nicht gezielt „Terrorverdächtige“, sondern breite Bevölkerungskreise betroffen sind, deren Daten erhoben und gespeichert werden. So muss jeder Bürger die Registrierung seiner Reise- und Bankdaten gewähren lassen. Ebenso entzieht sich seiner Kontrolle – und das ist seit Bekanntwerden des US-amerikanischen Überwachungsprogramms PRISM („Planning Tool for Resource Integration, Synchronization, and Management“) noch deutlicher geworden<sup>62</sup> –, ob und in welcher

---

<sup>60</sup> So urteilte Heribert Prantl in seinem Kommentar in der *Süddeutschen Zeitung* (Ein Katastrophen-Beschluss, 18./19. August 2012, S. 4), eben weil die Debatte längst vom Tisch war und weil das Bundesverfassungsgericht überdies gleichsam eigenmächtig eine Grundgesetzänderung vorgenommen hatte, für die eben eigentlich das Parlament zuständig (und eben eine Zweidrittelmehrheit erforderlich) ist.

<sup>61</sup> „Der Karlsruher Beschluss“, so prophezeit etwa Prantl, „ist ein Einstieg in eine Militarisierung der inneren Sicherheit, die nicht zur deutschen Geschichte und nicht zum Grundgesetz passt.“ (ebd.)

<sup>62</sup> Glenn Greenwald und Ewen MacAskill: NSA Prism program taps in to user data of Apple, Google and others, in: *The Guardian*, 7. Juni 2013. Verfügbar unter: <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data> [25.06.2013];



Weise seine Telefon- und Internetkommunikation überwacht wird. Er – oder sie – ist auch nicht davor gefeit, als unbescholtener Bürger in der Antiterrordatei geführt zu werden, da vor dem Urteil des Bundesverfassungsgerichts vom 24. April 2013 bereits der Kontakt zu einem „Terrorverdächtigen“ ausreichte, um in die Datenbank aufgenommen zu werden.

Dieser „Verlust an kognitiver Sicherheit durch hoheitliche Überwachung und Kontrolle“ wird nach Frankenberg (2010, S. 269) durch die politische Verheißung „eine[r] existenzielle[n], aufs Dasein verallgemeinerte[n] Sicherheit ausgeglichen.“ In diesem Sinne lassen sich Kontrolltechnologien als Sicherheitsversprechen betrachten, die dem verunsicherten Bürger „suggerieren sollen, alles Erforderliche zur Bannung des Bedrohlichen werde unverzüglich getan“ (ebd., S. 239).

## 4.2 Akzeptanz von Sicherheitsmaßnahmen

Politisch wurde die Einführung von Sicherheitsmaßnahmen und -gesetzen im Anschluss an die Ereignisse von 9/11 zumeist als konsequente oder sogar erforderliche Antwort auf eine neue Bedrohungslage dargestellt. Ob und inwiefern solche Diskurse zur Bedrohung unserer Sicherheit und zu Sinn und Zweck entsprechender Sicherheitstechnologien tatsächlich einen Widerhall in der Wahrnehmung der Bürger finden, hat die Akzeptanzforschung in den vergangenen Jahren vermehrt untersucht. Etymologisch auf das lateinische Verb *accipere*: *annehmen*, *empfangen* (in der Regel eines Vorschlags) zurückgehend, bezieht der Begriff der Akzeptanz sich auf die Frage nach den Gründen und Argumenten, die dieser zugrunde liegen und die als solche als rationalisierbar und also auch daraufhin befragbar gelten, ob sie „in sich stimmig, schlüssig, sachgemäß, vernünftig, zielführend und insoweit vertretbar, der Situation oder den Verhältnissen angemessen und damit als richtig und rechtens anzuerkennen“ sind (Lucke 2010, S. 13).

Die Methoden zur Erfassung der Akzeptanz variieren freilich. Während in diesem Feld quantitative Untersuchungen dominieren (vgl. ISIP-Projekt: z.B. Lüdemann & Schlepper 2013), werden standardisierte Erhebungen zunehmend auch durch qualitative Befragungen ergänzt (SIRA-Projekt: z.B. Bug & Wagner 2013; VESPER+-Projekt:

---

Barton Gellman und Laura Poitras: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, in: The Washington Post, 7. Juni 2013, Verfügbar unter [http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html?hpid=z1](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1) [25.06.2013].





z.B. Schlepper et al. 2013).<sup>63</sup> Vereinzelt nähern sich Studien dem Phänomen der Akzeptanz von Sicherheitstechnologien ausschließlich anhand qualitativer Methoden (Biometrie-Projekt: z.B. Krasmann & Kühne 2013) und untersuchen kontext- bzw. situationsabhängige Bedingungen der Akzeptanz.

Auch die thematische Ausrichtung ist unterschiedlich. So untersuchen Studien die „Bewertung“ einer Vielzahl verschiedener Maßnahmen kontextunabhängig (z.B. das ISIP-Projekt: vgl. Lüdemann & Schlepper 2013; Pietsch & Fiebig 2011), während andere ausgewählte Sozial- bzw. Kontrollräume, wie z.B. Flughäfen (z.B. das SIRA-Projekt: Bug & Wagner 2013 oder das APFEl-Projekt: Feltes et al. 2013), Informations- und Kommunikationstechnologien (insbesondere des Internets, z.B. das SIRA-Projekt: Bug & Münch 2013) oder den Fährverkehr (VESPER+-Projekt: Schlepper et al. 2013), oder kontextübergreifend nur eine spezifische Technologie in den Blick nehmen (z.B. den Fingerabdruck im Biometrie-Projekt: Krasmann & Kühne 2013). Die in diesem Kapitel vorgestellte Auswahl der Ergebnisse von Akzeptanzstudien repräsentiert diese unterschiedlichen Zugänge. Sie ermöglicht zunächst einen Vergleich der Ergebnisse von quantitativen Studien zu Bewertungen und Einschätzungen verschiedener Sicherheitsmaßnahmen und -technologien durch die Bürger. Anschließend werden die daraus abgeleiteten Schlussfolgerungen zu Bedingungen und Grenzen der Akzeptanz, auch unter Bezugnahme auf Ergebnisse qualitativ ausgerichteter Untersuchungen, erörtert.

#### 4.2.1 Zentrale Ergebnisse zu Bewertungen einzelner Sicherheitsmaßnahmen

Für einen ersten Vergleich der Studien orientiert sich die nachfolgende Darstellung an der im vorangegangenen Kapitel entwickelten Systematik über die „neuen und erweiterten Befugnisse der Sicherheitsbehörden“. Maßnahmen, die sich nicht ohne Weiteres einer Kategorie zuordnen lassen, gleichwohl aber unter die seit 2001 etablierten Sicherheitsmaßnahmen subsummiert werden können, werden im letzten Abschnitt dieses Kapitels vorgestellt. Dabei geht es einerseits um quantitative Studien, die Akzeptanz als eine Frage der „Einstellung“ konzipieren und entsprechende Faktoren (beispielsweise eine Maßnahme, die ein Sicherheitsgefühl bestimmt) inspizieren (Bug & Münch 2012; Pietsch & Fiebig 2012; Lüdemann & Schlepper 2013).

---

<sup>63</sup> Ein weiteres Forschungsprojekt, das sowohl quantitative als auch qualitative Methoden in das Forschungsdesign integriert, ist das Projekt SAFEST (Social-Area Framework for Early Security Triggers at Airports), welches sich der Herstellung von Akzeptanzbedingungen neuer elektronischer Sicherheitssysteme im Flughafenbereich widmet und zu diesem Zweck die Akzeptanz von Sicherheitsmaßnahmen am Flughafen erhebt (Baccelli et al. 2012).



Andererseits suchen Studien (die Grenze der) Akzeptanz nicht im Maß der Zustimmung zu einer konkreten Maßnahme, sondern über die Attribuierung von Sicherheit und Risiken zu ermitteln (Bug & Wagner 2013; Feltes et al. 2013; Schlepper et al. 2013).

#### 4.2.1.1 Akzeptanz des Zugriffs auf Bankdaten

Im Mittelpunkt des Projektes „Der ‚überwachte Bürger‘ zwischen Apathie und Protest“ standen die Einstellungen der Bürger zu folgenden sieben Kontroll- und Überwachungstechnologien: elektronische Ausweisdokumente, Online-Zugriff auf digitalisierte Lichtbilder, Kontenabrufverfahren, Vorratsdatenspeicherung von Telefon- und Internetverbindungsdaten, Online-Durchsuchung, Antiterrordatei und Passagierdatenspeicherung. In welchem Maß Bürger einzelne Maßnahmen akzeptieren, wurde durch die subjektive Bewertung der einzelnen Maßnahmen erhoben.<sup>64</sup> Gefragt wurde, wie gut oder wie schlecht sie diese einzelnen Maßnahmen finden, wobei als Antwortmöglichkeiten *sehr gut*, *eher gut*, *eher schlecht* oder *sehr schlecht* vorgegeben wurden (vgl. Tab. 4).

Tabelle 4: Wie bewerten die Bürger die folgenden Kontroll- und Überwachungstechnologien?

	<i>sehr gut</i>	<i>eher gut</i>	<i>eher schlecht</i>	<i>sehr schlecht</i>	<i>Mittelwert</i>
<i>Biometrische Ausweisdokumente</i>	691 32,2%	979 45,6%	323 15,0%	155 7,2%	3.03
<i>Antiterrordatei</i>	604 28,2%	1037 48,4%	364 17,0%	139 6,5%	2.98
<i>Online-Zugriff auf digitalisierte Lichtbilder</i>	598 27,9%	1044 48,6%	345 16,1%	160 7,5%	2.97
<i>Erfassung von Passagierdaten</i>	462 21,5%	971 45,1%	527 24,5%	192 8,9%	2.79
<i>Zugriff auf Bankdaten</i>	378 17,5%	808 37,5%	703 32,6%	265 12,3%	2.60
<i>Online-Durchsuchung</i>	330 15,3%	655 30,4%	632 29,4%	535 24,9%	2.36
<i>Vorratsdatenspeicherung</i>	188 8,7%	475 22,0%	776 36,0%	719 33,3%	2.06

Quelle: ISIP-Projekt, eigene Berechnungen 2009 (N = 2.176)

<sup>64</sup> Die im Oktober 2009 durchgeführte, standardisierte Telefonbefragung zu staatlichen Überwachungsmaßnahmen beruhte auf einer repräsentativen Stichprobe von 2.176 in Privathaushalten lebenden Personen ab 18 Jahren (Lüdemann & Schlepper 2013).



Die Ergebnisse zeigen, dass die Kontrolltechnologien von den Bürgern durchaus polarisierend wahrgenommen werden. Wenngleich das *Kontenabrufverfahren* im Vergleich mit anderen Maßnahmen die am dritt schlechtesten bewertete Maßnahme ist, beurteilen dennoch etwas mehr als die Hälfte der Befragten die Maßnahme mit *gut* bis *sehr gut*.

Auch die Untersuchung von Pietsch und Fiebig, die sich auf Daten der Bevölkerungsumfrage des Sozialwissenschaftlichen Instituts der Bundeswehr 2010 bezieht, integriert (12) unterschiedliche Maßnahmen zur Terrorismusbekämpfung in die Frage nach der Bewertung sicherheitspolitischer Maßnahmen (vgl. Tab. 5).

Tabelle 5: Zustimmung und Ablehnung der folgenden sicherheitspolitischen Maßnahmen durch den Bürger:

	<i>stimme zu</i>	<i>stimme eher zu</i>	<i>lehne eher ab</i>	<i>lehne ab</i>	<i>weiß nicht/k.A.</i>
<i>Überführte Terroristen härter bestrafen</i>	78%	13%	4%	3%	3%
<i>Verdächtige Ausländer aus Deutschland ausweisen</i>	65%	19%	9%	5%	2%
<i>Die militärischen Mittel und Möglichkeiten der Bundeswehr auch im Inland nutzen, z.B. zum Schutz von Atomkraftwerken</i>	60%	26%	7%	5%	2%
<i>Mehr Polizisten in der Öffentlichkeit einsetzen</i>	58%	24%	12%	4%	2%
<i>Öffentliche Plätze und Gebäude, z.B. Flughäfen und Bahnhöfe, verstärkt mit Videokameras überwachen</i>	56%	24%	9%	8%	2%
<i>Potentielle Terroristen vorbeugend in Gewahrsam nehmen</i>	56%	23%	10%	7%	4%
<i>Handy- und Internetverbot für Personen, die im Verdacht stehen, Terroranschläge vorzubereiten</i>	45%	23%	13%	12%	7%
<i>Den Verfassungsschutz auf die Bank-, Telefon- und Reisedaten (z.B. Flugverbindungen) von verdächtigen Personen zugreifen lassen</i>	44%	28%	12%	11%	4%
<i>Fingerabdrücke und andere Persönlichkeitsmerkmale von allen Bundesbürgern in einer zentralen Datei erfassen und zur Verbrechensbekämpfung nutzen</i>	40%	17%	15%	24%	4%
<i>Die Möglichkeiten zum Abhören von Telefonen und Privaträumen ausweiten</i>	23%	19%	24%	29%	5%
<i>Online-Durchsuchungen von privaten Computern aller Bundesbürger ermöglichen</i>	16%	12%	24%	43%	6%
<i>Von Terroristen gekaperte Flugzeuge im Notfall abschießen, auch wenn dabei unschuldige Passagiere getötet werden</i>	11%	11%	24%	44%	11%

Quelle: Pietsch & Fiebig 2011, S. 269 (N = 3.026)



Erfragt wird die jeweilige Zustimmung bzw. Ablehnung zu der Frage *Um die Menschen in Deutschland vor den Gefahren des Terrorismus zu schützen, werden verschiedene Maßnahmen erwogen. Sagen Sie mir bitte, ob Sie den folgenden Vorschlägen zur Terrorabwehr zustimmen oder ob Sie diese ablehnen.* (2011, S. 269)

Anders als bei Lüdemann und Schlepper (2013) wird hier auch die Zustimmung bzw. Ablehnung von Maßnahmen erfasst, die in der Form nicht Teil der Sicherheitsgesetzgebung nach 2001 waren, wie z.B. *Handy- und Internetverbot für Personen, die in Verdacht stehen, Terroranschläge vorzubereiten.* (Pietsch & Fiebig 2011, S. 269)

In dieser Untersuchung zeigt sich ebenfalls im Vergleich mit anderen Maßnahmen zunächst eine eher ablehnende Haltung gegenüber dem staatlichen Zugriff auf Bankdaten. Allerdings stimmen 72 Prozent der Befragten und damit deutlich mehr als in der Untersuchung von Lüdemann und Schlepper (2013) einem Zugriff auf diese Daten *zu* bzw. *eher zu* (vgl. Tab. 5).<sup>65</sup> Dabei muss allerdings berücksichtigt werden, dass in dem betreffenden Item verschiedene Maßnahmen, d.h. sowohl der Zugriff auf Bankdaten als auch auf Telefon- und Reisedaten, gemeinsam erfasst wurden. Zudem ist im Item selbst eine Einschränkung des Zugriffs auf *verdächtige Personen* angegeben. Im Vergleich erreicht die Maßnahme des Zugriffs auf Bankdaten bei den Befragten eine größere Zustimmung als eine zentrale Erfassung von Fingerabdrücken, das Abhören privater Kommunikation oder die Onlinedurchsuchung (vgl. Pietsch & Fiebig 2011, S. 269ff.).

#### 4.2.1.2 Akzeptanz der Kontrolle des Reiseverhaltens

Eine geringere Zustimmung erhält der Zugriff auf Reisedaten durch die Bundespolizei (in der hypothetischen Frage von Pietsch und Fiebig ist es dagegen der Verfassungsschutz, der auf die Daten zugreift, vgl. Tab. 5), wenn dieser Zugriff separat ohne Angabe eines konkreten Zwecks erfragt wird. Im Vergleich der sieben in Frage stehenden Maßnahmen in der Studie von Lüdemann und Schlepper (2013, S. 155) erreicht die Erfassung der Passagierdaten von Flug- und Schiffsreisenden durch die Bundespolizei einen mittleren Bewertungsplatz: 62,6 Prozent befinden das Verfahren für *gut* bis *sehr gut* (vgl. Tab. 4).

Das SIRA-Projekt untersucht unterschiedliche Sozialräume hinsichtlich der Bewertung und Akzeptanz von Sicherheitsmaßnahmen, zum einen das Internet – hier wurde die Wahrnehmung der Vorratsdatenspeicherung erfragt (Bug & Münch 2012, S. 150) – und zum anderen den Flugverkehr (Bug & Wagner 2013). Dabei richtete sich die Befragung zur Akzeptanz neben allgemeinen Sicherheitsmaßnahmen auch auf die im Flugverkehr relevante Passagierdatenspeicherung: *Wie finden Sie die Erfassung von*

---

<sup>65</sup> Die Bewertung *stimme zu* setzt sich dabei aus den Anteilen *stimme vollkommen zu* und *stimme überwiegend zu* zusammen.



*Passagierdaten von allen Flug- und Schiffsreisenden durch die Bundespolizei?* Die in dieser Studie befragten Flugpassagiere bewerten diese deutlich positiver als die Befragten in der Untersuchung von Lüdemann und Schlepper (2013). 19,4 Prozent der befragten Flugpassagiere bewerten die Maßnahmen als *sehr gut*, weitere 53,2 Prozent als *eher gut* (Bug & Wagner 2013).

Während die Einführung des ePasses, d.h. eines Reisepasses mit biometrischem Passbild und digitalisiertem Fingerabdruck, in der Studie von Lüdemann und Schlepper (2013, S. 155) die vergleichsweise größte Akzeptanz erreicht (77,8 Prozent der Befragten bewerten es mit *gut* bis *sehr gut*, vgl. Tab. 4), stößt eine vom Dokument abgekoppelte zentrale Speicherung von Fingerabdrücken aller Bundesbürger auf weniger Zustimmung. So *lehnen* 39 Prozent der Befragten in der Studie von Pietsch und Fiebig (2011, S. 269) eine zentrale Speicherung unter der Voraussetzung, dass diese *zur Verbrechensbekämpfung* genutzt wird, *ab* bzw. *eher ab* (vgl. Tab. 5).

#### 4.2.1.3 Akzeptanz der Registrierung des Kommunikationsverhaltens

Unter der Voraussetzung, dass sich die *Vorratsdatenspeicherung* unter dem *Zugriff auf Bank-, Telefon- und Reisedaten* in der Studie von Pietsch und Fiebig subsummieren lässt (die Zustimmung liegt bei 72 Prozent, vgl. Tab. 5), zeigt der Vergleich mit den Ergebnissen der Studie von Lüdemann und Schlepper, in der diese Maßnahme konkret benannt wird, eine deutlich andere Bewertung. Die *Vorratsdatenspeicherung* ist hier die am schlechtesten bewertete Maßnahme (Lüdemann & Schlepper 2013, S. 155). Lediglich 8,7 Prozent der Befragten bewerten diese mit *sehr gut* bzw. 22 Prozent mit *eher gut* (Schlepper & Leese 2011, S. 74, vgl. Tab. 4).

Anhand des gleichen Bewertungsschemas wie bei Lüdemann und Schlepper kommen Bug und Münch (2012, S. 166ff.) zu ähnlichen Ergebnissen in der Bewertung der *Vorratsdatenspeicherung*. Hier wurde zunächst gefragt: *Nun geht es um Vorratsdatenspeicherung: Dadurch sollen Telefon- und Internetverbindungsdaten durch Kommunikationsunternehmen für 6 Monate gespeichert werden. Haben Sie schon einmal von der Vorratsdatenspeicherung gehört?*<sup>66</sup> Während Befragte, denen die Maßnahme bekannt war, dies anhand folgender Frage bewerten sollten: *Wie gut oder schlecht finden Sie die Maßnahme, sehr gut, eher gut, eher schlecht, sehr schlecht?*, erhielten jene ohne Vorwissen eine kurze Information dazu: *Aus den Daten geht hervor, mit wem sie wann und wie lange telefoniert haben und mit wem Sie wann E-Mail- oder SMS-Kontakt hatten. Bei Handynutzung wird auch der Standort festgehalten. Halten Sie die Vorratsdatenspeicherung für sehr gut, eher gut, eher schlecht, sehr schlecht?*

---

<sup>66</sup> Auch in der Studie von Lüdemann und Schlepper (2013, S. 158) wurde das Vorwissen erfragt, das allerdings ohne Einfluss auf die Bewertung war. Alle Interviewten erhielten in der Studie die gleichen erläuternden Informationen zu den einzelnen Maßnahmen.



Im Vergleich zeigt sich, dass 9,8 Prozent der Befragten mit Vorwissen und ohne eine weitere Erläuterung der Maßnahme die Vorratsdatenspeicherung mit *sehr gut* bzw. ca. 31 Prozent mit *eher gut* bewerteten.<sup>67</sup> Diese „unterstützende“ Haltung verringerte sich allerdings bei den Befragten ohne Vorwissen und die eine Kurzinformation erhielten, hier beurteilten dann nur ca. 23 Prozent (statt ca. 31 Prozent) die Maßnahme als *eher gut*.

Die *Möglichkeiten zur Ausweitung des Abhörens von Telefonen und Privaträumen, um vor den Gefahren des Terrorismus zu schützen* – ein Item, das sich als Einführung der *Wohnraumüberwachung* lesen lässt –, wird in der Untersuchung von Pietsch und Fiebig (2011, S. 269) dagegen lediglich von 42 Prozent der Befragten als *eher gut* bis *sehr gut* bewertet (vgl. Tab. 5).

Ähnlich wie bei der Vorratsdatenspeicherung begegnen Befragte der *Online-Durchsuchung* offenbar mit größeren Vorbehalten. In der Untersuchung von Lüdemann und Schlepper (2013) bewerten weniger als die Hälfte der Befragten (45,7 Prozent) diese mit *gut* oder *sehr gut* (vgl. Tab. 4). Ein Viertel (24,9 Prozent) bewertet diese sogar mit *sehr schlecht* (Schlepper & Leese 2011, S. 74). Wenn sich bei Pietsch und Fiebig noch deutlichere Ablehnungswerte zeigen (vgl. Tab. 5) – so lehnen 43 Prozent die Maßnahme ab (24 Prozent *lehne eher ab*) – ist erneut die unterschiedliche Formulierung der Frage zu beachten. Lüdemann und Schlepper beschreiben die Maßnahme als einen behördlichen Zugriff auf Computerdaten *verdächtiger Personen [...] ohne dass die Betroffenen dies merken*, während der Verdachtsbezug im Item von Pietsch und Fiebig (2011, S. 269) fehlt. Hier lautet die Formulierung *Online-Durchsuchungen von privaten Computern aller Bundesbürger ermöglichen*. Zudem muss berücksichtigt werden, dass letztere in der konsequentesten Ablehnung *lehne ab* die Antwortkategorien *lehne überwiegend ab* und *lehne vollkommen ab* summiert haben.

#### 4.2.1.4 Akzeptanz von Datenbanken und Listen

Die Akzeptanz von Maßnahmen im Sinne neuer bzw. erweiterter Befugnisse der Sicherheitsbehörden, die ebenfalls im Mittelpunkt der Studien stehen – die Erfassung von Terrorverdächtigen sowie die zentrale Erfassung von Fingerabdrücken – lassen sich unter die Kategorie „Datenbanken und Listen“ fassen und in ihren Zustimmungswerten vergleichen.

---

<sup>67</sup> Die Bewertungsangaben sind im Beitrag von Bug und Münch (2012, S. 168) in einem Säulendiagramm dargestellt. Da nur der Prozentwert der Bewertung *sehr gut* für die Interviewten mit Vorwissen im Text genannt wird und die Bewertung *eher gut* aus dem Diagramm abgelesen werden muss, handelt es sich bei dieser Angabe lediglich um eine Schätzung, die nicht der konkreten Prozentzahl entspricht. Inwiefern sich in diesem Zusammenhang Änderungen hinsichtlich der Beurteilung *sehr gut* ergaben, ist dem Beitrag aus diesem Grund ebenfalls nicht zu entnehmen.



Die Erfassung von Terrorverdächtigen, die mit der Antiterrordatei 2007 in Betrieb genommen wurde, ist lediglich in der Studie von Lüdemann und Schlepper (2013) erfasst worden. Sie ist die am zweitbesten bewertete Maßnahme (ebd., S. 155). 74,6 Prozent der Befragten befinden sie als *eher gut* bis *sehr gut* (vgl. Tab. 4). Vergleicht man diese Zustimmungswerte mit der in der Studie von Pietsch und Fiebig (2011, S. 269) erfragten Maßnahme der zentralen Erfassung der Fingerabdrücke in einer Zentralkartei zum Zweck der Terrorismusbekämpfung – und die Speicherung der Fingerabdrücke aller Reisepassinhaber in den Passregistern, um sie polizeilich zugänglich zu machen, ist im Kontext der Einführung des eReisepasses durchaus politisch diskutiert worden –, so zeigt sich hier erneut mit 57 Prozent (*stimme zu* und *stimme eher zu*) ein deutlich geringerer Zustimmungswert (vgl. Tab. 5).

#### 4.2.1.5 Akzeptanz weiterer Maßnahmen

Während sich das SIRA-Projekt unterschiedlichen Sozialräumen und der Wahrnehmung der jeweils installierten Maßnahmen widmet, richtet sich der Fokus des VESPER+-Projekts auf nur einen spezifischen Sicherheitsraum. Sicherheitsmaßnahmen im Schiffsverkehr sind einerseits Ausdruck „institutioneller Aufrüstung und Vernetzung der Sicherheitsmaßnahmen“ (siehe Kapitel 4.1.2). Auf der anderen Seite sind mit dem seit dem 24. März 2004 geltenden International Ship and Port Facility Code (ISPS-Code) zahlreiche neue Sicherheitsmaßnahmen an der Schnittstelle Schiff/Hafen etabliert bzw. ausgeweitet worden. Dazu gehören z.B. die komplette Abschottung der Hafenanlagen, lückenlose Zugangskontrollen und die Kontrolle von Fahrzeugen, Gepäck und Passagieren.<sup>68</sup> Das VESPER+-Teilprojekt „Gesellschaftliche und wirtschaftliche Auswirkungen neuer Sicherheitsmaßnahmen im Fährverkehr“ untersucht die Akzeptanz der durch die Implementation des ISPS-Codes erhöhten Sicherheitsmaßnahmen im Fährverkehr und ermittelt mögliche Grenzen dieser bei einer potentiellen Erhöhung der Gefahrenlage auf die Gefahrenstufe 2,<sup>69</sup> wie es im ISPS-Code zumindest in abstrakter Form vorgegeben ist.<sup>70</sup> Indikatoren zur Messung der Akzeptanz sind hier die Bewertung der Wichtigkeit von 17 Sicherheitsmaßnahmen, die sowohl klassische

---

<sup>68</sup> Letztere zwei Maßnahmen variieren jedoch nach Schiffstyp.

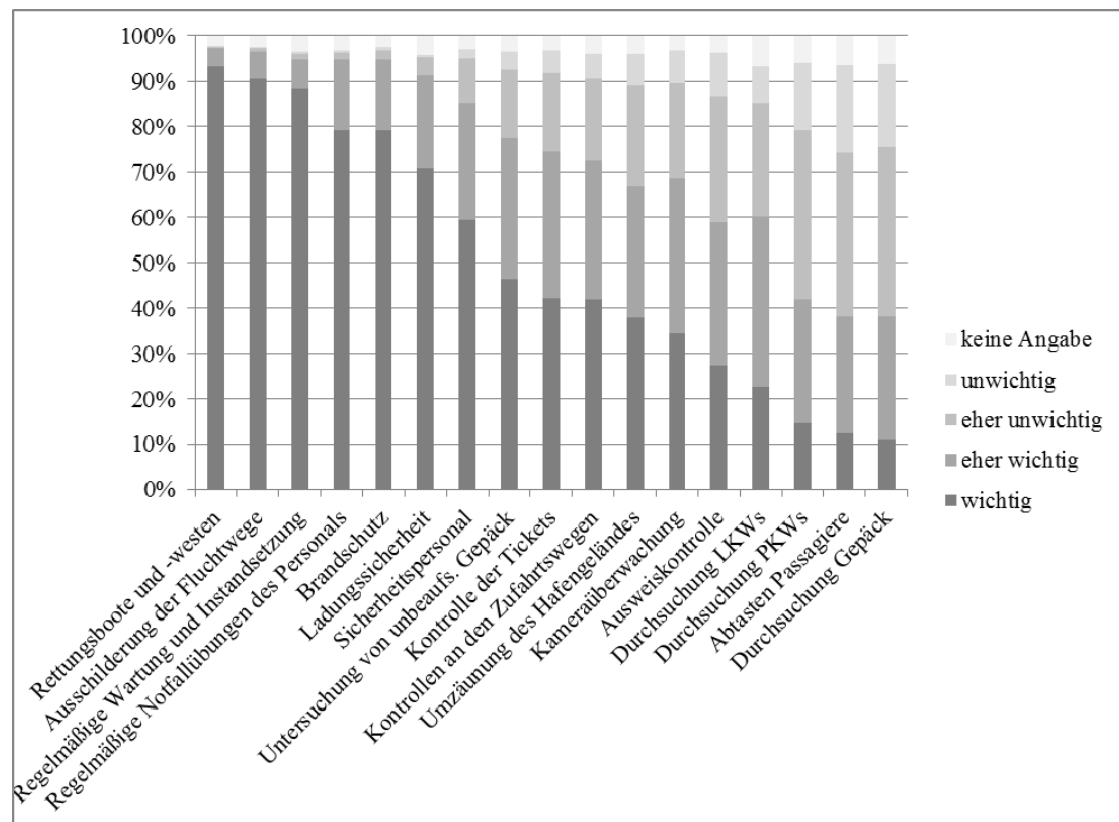
<sup>69</sup> Da unklar ist, welche Maßnahmen bei Eintreten der Gefahrenstufe 2 konkret ergriffen werden, wurde die Akzeptanz zu einer Reihe von Maßnahmen erfragt, die in Erwägung gezogen werden.

<sup>70</sup> Als Maßnahme der präventiven Gefahrenabwehr verpflichtet der ISPS-Code die maritime Wirtschaft in Deutschland auf der Basis von Risikobewertungen technische und personelle Instrumente (z.B. Zugangskontrollen und/ oder Überwachungsmaßnahmen) zur Abwehr externer Bedrohungen in die Arbeitsprozesse auf Schiffen und in Hafenanlagen zu integrieren. Der ISPS-Code findet seine Anwendung universell auf allen international verkehrenden Schiffen und unzähligen Hafenanlagen weltweit. Gefahrenstufe 2 findet Anwendung, sobald und solange ein erhöhtes Risiko eines sicherheitsrelevanten Ereignisses besteht. Allerdings sind die in den Sicherheitsvorschriften formulierten Maßnahmen eher unspezifischer Natur (siehe hierzu Schlepper et al. 2013).



„safety“- als auch „security“-Maßnahmen umfassen (vgl. Abb. 5). Berücksichtigt werden muss, dass letztere, außer der Ticketkontrolle, zwar theoretisch als eingesetzt gelten. Die befragten Passagiere haben die Maßnahmen jedoch nicht erfahren, sie fanden während der Befragung nicht statt. In der Studie wurde deshalb nicht die Bewertung der Maßnahmen selbst erfragt, sondern, als Indikatoren der Akzeptanz, die Wichtigkeit für das Sicherheitsempfinden, die Sicherheitseinschätzung zu einzelnen Maßnahmen sowie das Ausmaß einer antizipierten Belästigung.

Abbildung 5: Wichtigkeit von Maßnahmen für das Sicherheitsempfinden im Fährverkehr



Quelle: VESPER+-Projekt, eigene Berechnungen 2012 (N = 766)

Die Autoren zeigen, dass die befragten Fährpassagiere für den Kontext Fährverkehr vor allem klassische „safety-Maßnahmen“ als zentral für das persönliche Sicherheitsgefühl identifizieren. Sie erreichen insofern eine hohe Zustimmung (vgl. Abb. 5).

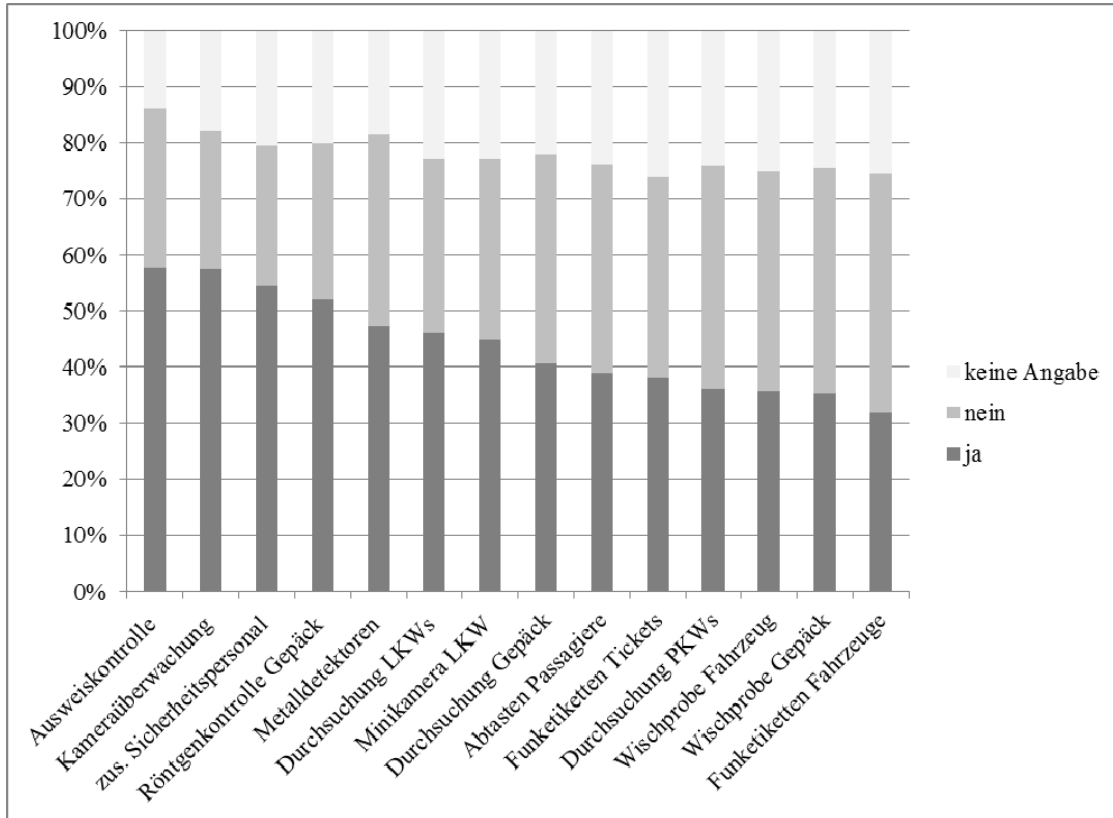
Hinsichtlich der Maßnahmen, die erst bei einer Erhöhung auf die Gefahrenstufe 2 zu etablieren wären, wie in Abbildung 6 dargestellt, erhalten vor allem die Ausweiskontrolle, Kameraüberwachung, zusätzliches Sicherheitspersonal, die Röntgenkontrolle





des Gepäcks, Metalldetektoren und die Durchsuchung von LKWs die höchsten Sicherheitszuschreibungen.<sup>71</sup>

Abbildung 6: Maßnahmen mit hoher Sicherheitszuschreibung im Fährverkehr bei Gefahrenstufe 2



Quelle: VESPER+-Projekt, eigene Berechnungen 2012

Das APFeL-Projekt widmete sich der Einschätzung der Bevölkerung von *intelligenter Videoüberwachung an Flughäfen* (Feltet et al. 2013)<sup>72</sup>. In der quantitativen Studie am Flughafen Hannover wurden 1.400 Flugpassagiere vor Ort nach dem Nutzen (z.B. zur individuellen kognitiven Risikowahrnehmung), den instrumentellen Folgen des Einsatzes (d.h. zur kriminalpräventiven Wirkung) und den Kosten der Maßnahme, wie z.B. individuellen Konsequenzen für die persönliche Freiheit (Datenschutz, Gefühl des Unwohlseins), gefragt. Im Ergebnis schreibt etwa die Hälfte der befragten Flugpassagiere der Videoüberwachung grundsätzlich eine kriminalpräventive Wirkung zu. Der Aussage *Der Einsatz von Videoüberwachung wird dazu beitragen, dass Straftaten wie Diebstahl, Raub und Körperverletzung verhindert werden*, stimmten 60,6 Prozent der Befragten zu bzw. *voll und ganz zu*.

<sup>71</sup> Die Frage lautete: *Bitte stellen Sie sich vor, dass folgende Maßnahmen im Fährverkehr eingeführt würden. Woran denken Sie bei den einzelnen Maßnahmen?* Erfragt wurde die Zustimmung zur Aussage *hier ist es sicher*. Als Antwortmöglichkeiten standen *ja* und *nein* zur Verfügung.

<sup>72</sup> Die standardisierte Befragung wurde im September 2010 am Flughafen Hannover durchgeführt.



Diese Zustimmung zum kriminalpräventiven Nutzen erhöht sich noch mit dem Bezug auf *moderne Technik (wie intelligente Videoüberwachung)* auf 60,6 Prozent bzw. mit der Kontextualisierung auf den Flughafenbereich auf 68,5 Prozent (ebd., S. 17). Der Einschätzung, dass Videoüberwachung Terrorismus verhindern könne, schließen sich 56,4 Prozent der Befragten an. Dass *der Einsatz von moderner Technik (wie intelligenter Videoüberwachung) [...] Terroristen erfolgreich davon abhalten [wird], Anschläge zu verüben* wird dagegen von 44,0 Prozent bejaht, ein Wert, der sich mit der Kontextualisierung auf den Flughafenbereich, erneut, auf 58,2 Prozent erhöht (Feltes et al. 2013, S. 15ff.).

Auch im SIRA-Projekt wird in der Befragung zur Akzeptanz von *Sicherheitsmaßnahmen am Flughafen* auf die Erlebbarkeit von (hier ausschließlich faktisch installierten) Sicherheitsmaßnahmen fokussiert (Bug & Wagner 2013). Neben qualitativen Befragungen am Flughafen Frankfurt wurden auf der Basis der Repräsentativuntersuchung 799 Flugpassagiere, d.h. Personen, die im Durchschnitt mindestens einmal pro Jahr fliegen, zu ihren Einschätzungen von Sicherheitsmaßnahmen (im Allgemeinen) und ihrem Sicherheitsgefühl durch die Maßnahmen befragt. Flugpassagiere, die angaben, sich durch Sicherheitsmaßnahmen am Flughafen gestört zu fühlen, wurden zudem gebeten, unterschiedliche *störende Aspekte (verletzen die Privatsphäre, sind übertrieben, werden nachlässig durchgeführt und/oder sind zeitraubend)* zu bewerten.<sup>73</sup> Am häufigsten wurde von diesen 253 befragten Flugpassagieren dem Item *zeitraubend* zugestimmt (50,6 Prozent), dem folgt mit 43,1 Prozent die Bewertung, dass diese *nachlässig durchgeführt* werden. Dass die Sicherheitsmaßnahmen im Flugbereich *übertrieben* seien, meinten 40,7 Prozent der Befragten, und lediglich 27,7 Prozent befanden in diesem Vergleich, dass diese *die Privatsphäre verletzen*.

Pietsch und Fiebig (2011) haben, ebenfalls auf der Basis der Daten der Bevölkerungsumfrage des Sozialwissenschaftlichen Instituts der Bundeswehr 2010, Einstellungen der Bürger zu „denkbaren“ *Einsätzen der Bundeswehr im Inland* untersucht. Diese umfassten die *Verteidigung bei einem militärischen Angriff auf unser Land, Katastrophenhilfe und die Suche und Rettung von Vermissten, die Überwachung des deutschen Luftraums bzw. der Küste zur Verhinderung von Terroranschlägen mit Flugzeugen bzw. Schiffen, Schutz von öffentlichen Gebäuden (Flughäfen, Bahnhöfen) und Infrastrukturanalagen wie Atomkraft- oder Chemiewerken*. Die Autoren ermittelten eine generell hohe Zustimmung zu den Maßnahmen. In der Reihenfolge der Nennung stimmten diesen zwischen 90 Prozent und 71 Prozent der Befragten zu. Lediglich der

---

<sup>73</sup> In die Befragung einbezogen wurden nur Flugpassagiere, die die Frage, ob sie etwas an den Sicherheitsmaßnahmen störe, mit *ja* beantworteten (Bug & Wagner 2013).



Einsatz der Bundeswehr zur *Sicherung der Landesgrenze gegen illegale Einwanderer* erhält mit 56 Prozent eine geringere Zustimmung (*stimme zu*).<sup>74</sup>

Die mit dem *Flugsicherheitsgesetz* angedachte Möglichkeit, *von Terroristen gekaperte Flugzeuge im Notfall abzuschießen, auch wenn dabei unschuldige Passagiere getötet werden*, erhält dagegen mit 11 Prozent (*stimme zu*) eine eher geringe Zustimmung.<sup>75</sup> Allerdings ist diese Maßnahme anders kontextualisiert. Wie der Tabelle 5 zu entnehmen ist, wurde sie anders als jene „denkbaren Einsätze“ in den Kontext der Gefahrenabwehr des Terrorismus gestellt.

#### 4.2.2 Zentrale Ergebnisse zu Bedingungen und Grenzen der Akzeptanz

In der Zusammenschau der Ergebnisse der quantitativen Studien zeigt sich, zunächst unabhängig von (kontextbezogenen) Bewertungen einzelner Maßnahmen und der methodischen Konzeption, eine eher zustimmende Haltung der Bürger gegenüber den seit 2001 etablierten Sicherheitsmaßnahmen. Dies gilt auch für Maßnahmen, die, wie z.B. die Videoüberwachung, bereits vor 9/11 etabliert wurden (in den Untersuchungen sollten sie durch die Befragten als Maßnahme der Terrorismusbekämpfung bewertet werden). Inwiefern die Bürger die Maßnahmen angesichts eigener Bedrohungswahrnehmung bzw. zur Erhöhung des persönlichen Sicherheitsgefühls als adäquat empfinden, lässt sich anhand der Studien allerdings keinesfalls eindeutig beantworten.

##### 4.2.2.1 Bedrohungswahrnehmungen und Sicherheitserwartungen

Dass Personen mit einer hohen Furcht vor terroristischen Anschlägen staatlichen Terrorismusbekämpfungsmaßnahmen einen höheren Nutzen zuschreiben und diese positiver bewerten, zeigen Lüdemann und Schlepper in ihrer Studie.<sup>76</sup> Die Bürger, so das Resümee (ebd. 2013, S. 58), lassen sich in ihrer durchweg eher positiven Bewertung von ihren (auch von existentiellen Ängsten beeinflussten) Bedrohungsgefühlen leiten. Während Pietsch und Fiebig (2011, S. 274) ebenfalls einen signifikanten Effekt der allgemeinen Bedrohungswahrnehmung auf die Zustimmung zu Maßnahmen der

---

<sup>74</sup> Ein vergleichbares Maß der Zustimmung ermittelten die Autoren in ihrer Analyse auf Basis der Bevölkerungsbefragung des Sozialwissenschaftlichen Instituts der Bundeswehr 2008 (Fiebig & Pietsch 2010, S. 101)

<sup>75</sup> In der Untersuchung von Fiebig und Pietsch (2010, S. 102) auf Basis der Daten der Bevölkerungsbefragung des Sozialwissenschaftlichen Instituts der Bundeswehr aus dem Jahr 2008 ergibt sich mit 15 Prozent (7 Prozent *stimme vollkommen zu* und 8 Prozent *stimme überwiegend zu*) ein etwas höherer Anteil der Zustimmung.

<sup>76</sup> Die in der Studie postulierten Zusammenhänge (Ängste, Erfahrungen mit staatlicher Kontrolle, Kosten- und Nutzenerwartungen sowie punitive Einstellungen auf die Bewertung der Maßnahme) wurden anhand eines Strukturgleichungsmodells überprüft (Lüdemann & Schlepper 2013).



Terrorabwehr ausmachen, weisen sie die Wirkung eines individuellen Bedrohungsgefühls auf die Zustimmung hingegen als relativ gering aus.

Ähnliche Ergebnisse im Sinne einer vom Großteil der Befragten eher als gering eingeschätzten persönlichen Bedrohung zeigen, wie bereits dargestellt, Bug und Wagner (2013). Unter anderem deshalb halten Bug und Wagner die Bewertung der „Zweckmäßigkeit“ der Sicherheitsmaßnahmen für ein entscheidendes Kriterium für die Akzeptanz. Auf die Frage *Halten Sie die bisherigen Sicherheitsmaßnahmen zur Abwehr von terroristischen Anschlägen rund ums Fliegen für zweckmäßig* antworteten 23,8 Prozent der befragten Flugpassagiere mit *sehr zweckmäßig* und 52,7 Prozent mit *eher zweckmäßig*, während sich eine verschwindend geringe Zahl von Flugverweigerern aufgrund von Sicherheitsmaßnahmen in der Repräsentativbefragung ermittelten ließ. Dies werten die Autoren als entscheidende Erklärung für einen hohen „Zuspruch“ zu den Maßnahmen. Auch im Kontext Fährverkehr geht ein von den meisten Befragten als gering eingeschätztes Risiko, Opfer eines terroristischen Anschlags zu werden, mit einem hohen Sicherheitsgefühl im konkreten Kontext einher (Schlepper et al. 2013, S. 7ff.).

Ungeachtet des je unterschiedlichen Erhebungsdesigns der Studien, sind demnach rein theoretisch drei Lesarten des Verhältnisses von Sicherheitsmaßnahmen und Sicherheitsgefühl denkbar: a) Bedrohungswahrnehmungen bestimmen die positive Bewertung von Maßnahmen, da sie das Sicherheitsgefühl erhöhen, b) Bedrohungswahrnehmungen werden kognitiv nicht zwangsläufig mit der Notwendigkeit der in Frage stehenden Maßnahmen verknüpft,<sup>77</sup> und c) unabhängig von individuellen Bedrohungsgefühlen werden Sicherheitsmaßnahmen mit einem hohen Sicherheitsgefühl assoziiert, das die Zustimmung anleitet. Dies könnte im Umkehrschluss bedeuten, dass die seit 2001 etablierten Maßnahmen keineswegs durchweg auf ein allgemein ausgeprägtes Sicherheitsbedürfnis der Bürger reagieren.

Zudem deuten einige Studien darauf hin, dass die Wahrnehmung – und Akzeptanz – von Sicherheitsmaßnahmen mit dem Kontext ihrer Anwendung bzw. Nutzung variieren.

#### 4.2.2.2 Sicherheitsräume, (un)normale Kontrolle und die Situation ‚selbst‘

Schlepper et al. (2013) haben in ihrer Untersuchung zeigen können, dass unterschiedliche Sozial- und Kontrollräume mit ungleichen Wahrnehmungen von Sicherheit bzw. Unsicherheit verbunden sind. Dass die befragten Fährpassagiere das höchste Sicherheitsgefühl auf Fähren und das geringste in Flugzeugen haben, ist verknüpft mit den

---

<sup>77</sup> Apelt & Möllers (2011, S. 587) zeigen dies in ihrer Zusammenschau von Studien zur Akzeptanz von Videoüberwachung, wonach keine Korrelation des subjektiven Sicherheitsgefühls mit Akzeptanz nachweisbar ist.



jeweils antizipierten kontextuell verschiedenen Bedrohungswahrscheinlichkeiten (ebd.; vgl. dazu auch Kapitel 2). Derartige Unterschiede verweisen auf eine kulturelle und sozialräumliche Prägung von Sicherheitswahrnehmungen. So sind es in der Studie von Schlepper et al. (ebd.) vor allem klassische „safety“-Maßnahmen, d.h. traditionell im Schiffsbereich etablierte Maßnahmen der Betriebssicherheit, die – analog zum Risiko widriger Wetterbedingungen – Einfluss auf das Sicherheitsempfinden haben (z.B. Rettungsboote, Ausschilderung und Fluchtwege, regelmäßige Wartung und Instandsetzung, regelmäßige Notfallübungen des Personals, Brandschutz und Ladungssicherung). „Security“-Maßnahmen, wie z.B. Kontrollen von Person, Gepäck oder Fahrzeug, haben aus Sicht der Befragten dagegen weniger Bedeutung für das individuelle Sicherheitsempfinden im Fährverkehr.

Dass die Einschätzung von Sicherheitsmaßnahmen abhängig vom Kontext ihres Einsatzes und auch mit der je spezifischen Technologie variieren, zeigen Schlepper et al. (2013) am Beispiel vom Fährverkehr auch bei einer Erhöhung der Gefahrenstufe.

Abbildung 7 stellt die Häufigkeiten der Sicherheitszuschreibungen (vgl. Abb. 6) zu den einzelnen Maßnahmen sowie das durch diese antizipierte Belästigungsgefühl<sup>78</sup> nebeneinander. Es zeigt sich, dass die Sicherheitsmaßnahmen, die bereits aus anderen Kontexten bekannt sind und auch mit „Sicherheit“ assoziiert werden, potentiell das geringste Gefühl der Belästigung auslösen (Schlepper et al. 2013).

Das Sicherheitsgefühl, das sich mit bestimmten Sicherheitsmaßnahmen und -technologien verbindet, scheint demnach auch mit einer lebensweltlichen Vertrautheit bzw. einer (diskursiv vermittelten) Assoziation mit Sicherheit zusammenzuhängen. So sind die Technologien, die aufgrund des ISPS-Codes zum Einsatz kommen könnten und laut der Studie ein Sicherheitsgefühl vermitteln, gerade die, die bereits aus anderen Kontexten bekannt sind, wie z.B. die Ausweiskontrolle, Kameraüberwachung, zusätzliches Sicherheitspersonal, Röntgenkontrolle des Gepäcks oder Metalldetektoren (ebd., vgl. Abb. 6).

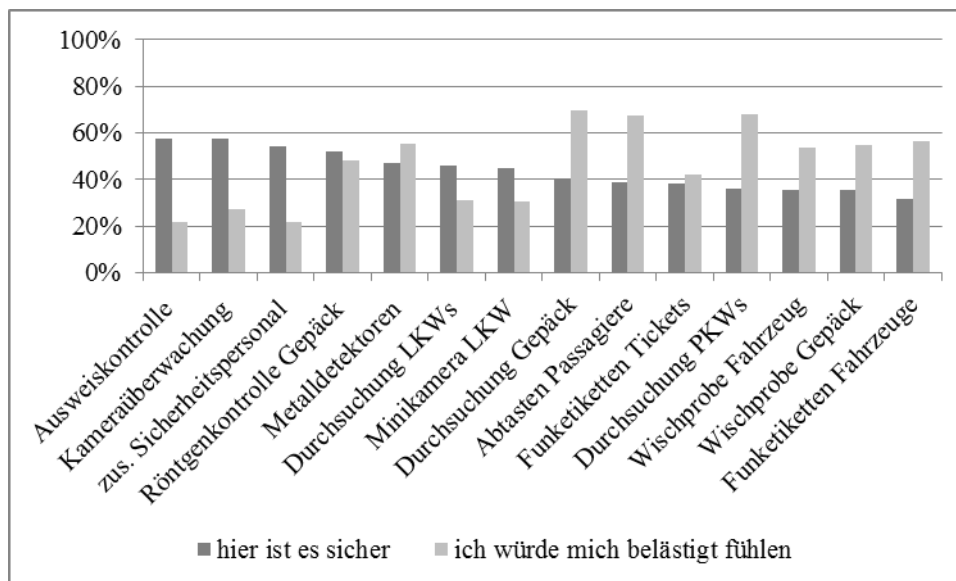
Die Relevanz kulturell sozialräumlicher Kontextuierungen legt auch die in der Studie von Bug und Wagner (2013) ermittelte Bewertung der „Zweckmäßigkeit“ der Sicherheitsmaßnahmen am Flughafen nahe (wobei die Frage auf den Schutz vor terroristischen Anschlägen zielt).

---

<sup>78</sup> Das Belästigungsgefühl wurde durch folgende Frage erhoben: *Würden Sie sich durch folgende Maßnahmen belästigt fühlen?* Als Antwortkategorien standen *nein, gar nicht, ja etwas, aber ich würde die Fähre weiterhin nutzen, ja sehr, wenn möglich würde ich auf die Fährfahrt verzichten* und *weiß nicht* zur Verfügung. In Abbildung 7 wurden die Antwortkategorien *ja etwas, aber ich würde die Fähre weiterhin nutzen, ja sehr, wenn möglich würde ich auf die Fährfahrt verzichten* zusammengefasst.



Abbildung 7: Sicherheitszuschreibungen und Belästigungsgefühl bei Maßnahmen im Fährverkehr



Quelle: eigene Berechnungen, N = 766

Im Vergleich zu anderen Sozialräumen wird man im Flughafen, auch unabhängig von 9/11, mit einer Vielzahl von Sicherheitsmaßnahmen konfrontiert, mit denen vor allem Vielflieger vertraut sind. Für die Akzeptanz könnte dies bedeuten, dass derartige Maßnahmen keine besondere Aufmerksamkeit (mehr) erlangen und gleichsam als gegeben hingenommen werden.

Auch in dem von der DFG geförderten Projekt „Biometrie als ‚soft surveillance‘. Zur Akzeptanz von Fingerabdrücken im Alltag“ variieren die Einschätzungen der biometrischen Technologie mit dem Kontext ihres Einsatzes. Hier wurden Antragsteller des ePasses und des elektronischen Personalausweises in Situationen der Antragsstellung beobachtet und anschließend in offenen, leitfadengestützten Interviews u.a. zu ihren Beweggründen und Vorstellungen der (Nicht-)Nutzung von digitalisierten Fingerabdrücken in nationalen Identitätsdokumenten befragt. Im politischen Diskurs seit 9/11 wird die Biometrie generell als eine Technologie verhandelt, die sowohl mehr Sicherheit als auch Annehmlichkeiten verspricht. Da die Fingerabdrucktechnologie überdies zunehmend auch in alltäglichen Kontexten Anwendung findet (Kühne & Schlepper 2013; Kühne & Wehrheim 2013), wurden Interviews und Beobachtungen von Anmelde- und Nutzungssituationen in weiteren exemplarischen Anwendungskontexten vorgenommen: in einer Zahnarztpraxis (zur Zeiterfassung), im Supermarkt, in Schulmensen (als alternative Bezahlungsfunktion) sowie in einer 24-Stunden-Videothek (als Zugangsmechanismus zum DVD-Automaten).



Dabei lässt sich der jeweilige Kontext nicht nur als ein spezifisches Anwendungssetting begreifen, sondern kann sehr Unterschiedliches heißen: die konkrete Interaktionssituation in der Behörde bei der Beantragung des Ausweispapieres oder beim Bezahlen im Supermarkt; die Grade der Vertrautheit mit dem Betreiber der Technologie (z.B. im Falle des lokalen Supermarkts); aber auch die imaginierte Anwendungssituation wie etwa bei Polizeikontrollen oder auch in Settings, die eher aus der Welt des Crime & Fiction bekannt sind (Krasmann & Kühne 2014).

So wurde in den qualitativen Interviews deutlich, dass die Befragten mit der Technologie nicht nur verschiedene Sicherheitserwartungen oder auch Sicherheitsrisiken verbinden, sondern auch die Sicherheitsthematik selbst von ganz unterschiedlichen Vorstellungen geprägt ist. So verbindet sich die Sicherheitserwartung mal mit der Terrorismusbekämpfung, mal eher mit der allgemeinen Strafverfolgung (z.B.: mit dem Fingerabdruck werden „Kriminelle eher geschnappt“), aber auch mit Notfallszenarien (z.B.: der Fingerabdruck erleichtert im Falle eines Unfalls die Identifizierung) und sogar mit den Rechten und Pflichten eines Bürgers, mit dem Fingerabdruck gewissermaßen seine „Papiere in Ordnung“ zu haben. Positive Sicherheitsassoziationen können sich demnach an den im politischen Diskurs vermittelten Zweck einer Technologie (z.B. die „Terrorismusbekämpfung“), aber auch an die zugeschriebenen bzw. angenommenen Fähigkeiten der Technologie selbst heften (wobei die Vorstellung, der Fingerabdruck sei ein effektiveres Mittel der Verbrechensbekämpfung, häufig in Referenz auf Szenen aus dem Genre des „Krimi“ entwickelt wird). Dass allerdings auch Personalausweis Antragsteller, die sich gegen eine Aufnahme des Fingerabdrucks in den ePersonalausweis entschieden, positive Sicherheitserwartungen haben, deutet zudem daraufhin, dass diese unabhängig von der tatsächlichen Nutzung sind.

Die Befunde weisen also nicht nur darauf hin, dass Sicherheitserwartungen ebenso wie der thematische Bezug der Sicherheitsvorstellungen mit dem Anwendungskontext variieren, sondern darüber hinaus situative Momente eine nicht unerhebliche Rolle bei der Konstitution dieser Vorstellungen spielen: Und so lässt sich das Ergebnis, dass von den in der Studie von Schlepper et al. (2013, vgl. Abb. 7) geprüften Kontrollvariablen lediglich die Anzahl der in den letzten zwölf Monaten gemachten Fährfahrten das Belästigungsgefühl beeinflusst – die Intensität der antizipierten Belästigung steigt mit der Häufigkeit unternommener Fährfahrten<sup>79</sup> –, in Übereinstimmung mit einer Einsicht aus der sozialwissenschaftlichen Technikakzeptanzforschung, dahingehend deuten, dass sich der Zweck einer Maßnahme überhaupt erst „in der Performanz [...] in einem konkreten Kontext realisieren“ kann (Rammert 1999, S. 7f.). Dies zeigt sich auch im Biometrie-Projekt. So ist für die Befragten durchaus entscheidend, ob eine Kontrollmaßnahme in einem freundlichen Ton vorgenommen oder der Check-in am Flughafen

---

<sup>79</sup> Allerdings muss berücksichtigt werden, dass es sich dabei um einen sehr schwachen Zusammenhang handelt, der nicht hochsignifikant ist (Schlepper et al. 2013).



als rüde Tortur empfunden wird. Auch in den Auszügen der qualitativen Interviews mit Flugpassagieren in der Studie von Bug und Wagner (2013) deutet sich ein solcher Zusammenhang an.

#### 4.2.2.3 (Un-)Sichtbare Kontrolle

Vor allem die sogenannten *Surveillance Studies* kritisieren, wie oben bereits angedeutet, das mit der Digitalisierung von Daten und der Automatisierung von Kontrolle einhergehende Verschwinden bzw. Unsichtbarwerden der Überwachung und entsprechender Technologien – mit entsprechenden Folgen nicht nur für die Möglichkeit der Kontrolle, sondern auch ihrer Einschätzung und Bewertung. Demnach müssten die Ergebnisse der Erhebungen zur Akzeptanz nicht nur mit unterschiedlichen methodischen Ansätzen bzw. Frageformulierungen variieren, sondern auch mit der Sichtbarkeit und Wahrnehmbarkeit der Technologien. Tatsächlich zeigen sich in den Studien auch in dieser Hinsicht kontextuelle Unterschiede.

Während die Fluggastdatenspeicherung in der Studie von Bug und Wagner (2013) von mehr als der Hälfte der befragten 799 Flugpassagiere (72,6 Prozent) mit *sehr gut* oder *eher gut* bewertet wird und auch bei der Mehrheit als geeignet erscheint, das Sicherheitsempfinden zu erhöhen, erntet die Vorratsdatenspeicherung, wie bereits gezeigt, eine vergleichsweise geringe Zustimmung. Dass sie darüber hinaus auch bei Internetnutzern überwiegend nicht mit einer höheren Sicherheitseinschätzung einhergeht – nur 33 Prozent der Befragten mit Vorwissen zu dieser Maßnahme fühlen sich auf *jeden Fall sicher* bis *sicher*, führen Bug und Münch (2012, S. 169) darauf zurück, dass es sich um eine „abstrakte, nicht sichtbare Maßnahme“ handelt.

Darüber hinaus hat die „Undurchschaubarkeit“ von Kontrolltechnologien offenbar auch prinzipiell Einfluss auf deren Beurteilung. So kann ein Gefühl des „Unheimlichen“ hinsichtlich dessen, was sich jenseits des Sichtbaren abspielt, mal positiv, mal negativ bewertet werden, wie Bug und Wagner (2013) anhand ihrer qualitativen Interviews zeigen: Während die nicht sinnlich nachvollziehbaren Möglichkeiten der Datenverwendung bei den einen „ein diffuses Gefühl des Beobachtetseins“ auslösen, ist für andere gerade die Tatsache, dass Maßnahmen unsichtbar bleiben, ein Indikator für deren Sicherheitswirkungen.

Ein beunruhigendes Gefühl diffuser Überwachung thematisieren auch die Befragten im Biometrie-Projekt. So bringen sie in Bezug auf das System der elektronischen Datenerfassung in der Behörde ihre Unsicherheit über den Verbleib der eigenen Daten zum Ausdruck und hoffen, dass Speicherung und Verwendung rechtmäßig geschehen. Faktische oder vorstellbare Möglichkeiten der Datenverwendung werden nicht selten in Rekurs auf Metaphern thematisiert, die auch im bürgerrechtsorientierten Diskurs verbreitet sind. Der „gläserne Bürger“ beispielsweise steht für die eigene Sichtbarkeit





– im Gegensatz zur Undurchschaubarkeit der Überwachung. Solche Einschätzungen deuten auf zwei weitere Aspekte der Bedingung von Akzeptanz hin: die antizipierte eigene Betroffenheit sowie die imaginierten Konsequenzen der Maßnahmen. Pietsch und Fiebig (2011, S. 269f.) ermitteln in ihrer Studie, dass Sicherheitsmaßnahmen in dem Moment ein geringeres Maß an Zustimmung erlangen, in dem sie sich auf die gesamte Bevölkerung erstrecken können. Wie in Tabelle 5 dargestellt werden die in dieser Studie erfragten ersten sieben Sicherheitsmaßnahmen – also jene, die sich auf spezifische, konkret verdächtige Personen richten und sich mit bestimmten Sanktionen verbinden (z.B. *Potentielle Terroristen vorbeugend in Gewahrsam nehmen*) – deutlich positiver bewertet als die Maßnahmen, die sich eher unkonkret auf die gesamte Bevölkerung beziehen könnten (z.B. *Die Möglichkeiten zum Abhören von Telefonen und Privaträumen ausweiten*). Je mehr sich Bürger von den in Frage stehenden Maßnahmen in ihrem eigenen Alltag betroffenen fühlen, umso geringer fällt demnach ihre Zustimmung zu diesen aus.

Interessanterweise beruhen die „guten“ Gründe, eine Technologie ausdrücklich zu akzeptieren oder sie kategorisch abzulehnen, und auch das ist ein wichtiger Gesichtspunkt für die Akzeptanzforschung, jedoch nicht zwangsläufig auf einem gesicherten Wissen darüber, was eine Technologie leisten kann. In der Biometrie-Studie beziehen viele Interviewte ihr Unbehagen gleichermaßen auf „tatsächliche“ Maßnahmen, etwa die, wenn auch zum Zeitpunkt der Interviews überholte, Vorratsdatenspeicherung, wie auch auf eher abstrakte argumentative Figuren, etwa den „gläsernen Bürger“ oder auch die Dystopie eines Orwell’schen Überwachungsstaats, die wiederum auch im kritischen Bürgerrechtsdiskurs zu finden sind. Umgekehrt entsprechen aber auch skeptische Einschätzungen über die Verwendung der Daten (wie etwa die, dass die Fingerabdrücke in behördlichen Zentraldateien gespeichert werden) nicht immer den faktischen Gegebenheiten (in diesem Fall schließt das Gesetz über den Personalausweis dies ausdrücklich aus). Die häufig zu vernehmende politische Forderung, dass der Bürger doch aufgeklärt sein muss, um „wachsam“ und „kritisch“ zu sein, greift so gesehen – bei aller Vorsicht im Hinblick auf die Reichweite der empirischen Ergebnisse – zu kurz.

#### *4.2.2.4 Was kostet die Freiheit? Akzeptanz zwischen (fehlendem) Widerstand und positiver Bewertung*

In quantitativen Untersuchungen kann man sich der Frage, mit welchen Risiken oder „Kosten“ Terrorismusbekämpfungsmaßnahmen verbunden sind – und das heißt auch ob diese von den Bürgern als Sicherheits- oder als Überwachungsmaßnahmen wahrgenommen werden –, empirisch auf zwei Ebenen nähern. Auf der Verhaltensebene kann man untersuchen, ob bestimmte Handlungen praktiziert oder nicht praktiziert werden, um diese Maßnahmen zu unterlaufen (Lüdemann & Schlepper 2011) oder gar



nicht erst mit diesen in Kontakt zu geraten (Bug & Wagner 2013). Auf der kognitiven Ebene werden den Sicherheitsgewinnen die (gefühlten) „Kosten“ (vgl. Lüdemann & Schlepper 2013; ähnlich auch Feltes et al. 2013) bzw. „Unannehmlichkeiten“ (Bug & Wagner 2013; ähnlich auch Bug & Münch 2012) oder „Belästigungen“ (Schlepper et al. 2013) gegenübergestellt und erhoben.

#### (1) Verhaltensebene

Welche Maßnahmen die Bürger ergreifen, um sich vor der Preisgabe ihrer Daten zu schützen, wurde im Projekt „Der überwachte Bürger zwischen Apathie und Protest“ untersucht (Lüdemann & Schlepper 2011).

Die Befragten sollten angeben, ob sie schon einmal *bestimmte Dinge getan haben, um ihre persönlichen Daten nicht preisgeben zu müssen*. Im Anschluss wurde gefragt, ob sie sich vorstellen könnten, dies *in Zukunft unter Umständen wieder zu tun*. Personen, die entsprechende Handlungen noch nie praktiziert hatten, wurden gefragt, ob sie sich vorstellen könnten, dies *in Zukunft unter Umständen zu tun*.

Neben dem faktischen Verhalten wurde also auch die Verhaltensintention erhoben. Die absoluten und relativen Häufigkeiten sind in Tabelle 6 dargestellt.<sup>80</sup>

Es hat sich gezeigt, dass zwar nicht die Mehrheit, aber ein beachtlicher Teil der Befragten bereits einmal Vorkehrungen zum Schutz seiner telefonischen und Internet-Kommunikation getroffen hat. Betrachtet man die rechte Spalte, so zeigt sich eine deutlich steigende Tendenz, alternative Wege zu suchen, um anonym im Internet zu surfen und abhörsicher zu telefonieren.<sup>81</sup>

Obschon diese Forschungsergebnisse noch relativ aktuell sind, erscheinen sie bereits in zweifacher Weise durch das aktuelle Zeitgeschehen überholt. Zum einen war die Regelung zur Vorratsdatenspeicherung zum Zeitpunkt der Befragung (Herbst 2009) noch in Kraft.

---

<sup>80</sup> Die Prozentangaben zu folgenden Aktivitäten beziehen sich nur auf Internetnutzer (N = 1.699): Kryptographie nutzen, Programm für die Erzeugung von Passwörtern nutzen, Email mit falschem Namen schreiben, Internet-Telefonie (z.B. Skype) nutzen, Anonymisierungsprogramm nutzen, Internet-Café besuchen. Die Prozentangabe zum Erwerb einer ePass-Hülle bezieht sich nur auf ePass-Besitzer (N = 267). Alle übrigen Prozentzahlen beziehen sich auf die gesamte Stichprobe (N = 2.176). Beim Verhalten beim Einwohnermeldeamt nicht an- oder umgemeldet wurde nur nach dem praktizierten Verhalten und nicht nach der entsprechenden Intention gefragt, weil – wie sich im Pretest (N = 50) gezeigt hat – die Verwendung einer doppelten Negation in der Frage in Kombination mit den Antwortvorgaben ja und nein für Befragte zu schwierig und verwirrend gewesen wäre.

<sup>81</sup> Natürlich sind die Ergebnisse unter dem Vorbehalt der sozialen Erwünschtheit zu betrachten, deren Einfluss bei dieser Frage zu erwarten ist.



Tabelle 6: Häufigkeiten praktizierter und intendierter Schutzmaßnahmen der Bürger gegen Kontroll- und Überwachungstechnologien

<i>Wenn man seine persönlichen Daten nicht preisgeben möchte, kann man verschiedene Dinge tun. Ist es schon einmal vorgekommen, dass...</i>	<i>praktiziertes Verhalten</i>	<i>intendiertes Verhalten</i>
<i>sie sich über die Datenschutzrichtlinien einer Behörde informiert haben? (N = 2.176)</i>	702 32,3%	1693 78,8%
<i>sie ein Programm zur Verschlüsselung von E-Mails oder Dateien eingesetzt haben? (N = 1.699)</i>	461 27,5%	888 53,1%
<i>sie sich geweigert haben, einer Behörde bestimmte persönliche Daten oder Informationen zu geben? (N = 2.176)</i>	505 23,3%	1472 70,3%
<i>sie ein Programm zur Erzeugung von Passwörtern verwendet haben? (N = 1.699)</i>	316 18,8%	629 37,8%
<i>sie eine E-Mail-Adresse mit falschem Namen angelegt haben? (N = 1.699)</i>	269 15,9%	384 22,8%
<i>sie, um abhörsicher zu telefonieren, Internet-Telefonie, z.B. Skype, genutzt haben? (N = 1.699)</i>	253 15%	631 37,7%
<i>sie ein Programm oder einen Anonymisierungsdienst zum anonymen Surfen im Internet genutzt haben? (N = 1.699)</i>	216 12,8%	559 33,6%
<i>sie sich beim Einwohnermeldeamt <u>nicht</u> an- oder umgemeldet haben? (N = 2.176)</i>	185 8,5%	-- --
<i>sie zu einer Telefongesellschaft gewechselt sind, die Ihre Telefon- bzw. Internetverbindungsdaten nicht auf Vorrat speichert? (N = 2.176)</i>	125 6,4%	1016 53,4%
<i>sie, um anonym zu surfen, ein Internet-Cafe besucht haben? (N = 1.699)</i>	86 5,1%	331 19,5%
<i>sie ein abhörsicheres Telefon bzw. Handy benutzt haben? (N = 2.176)</i>	105 5%	578 27,7%
<i>Haben Sie eine Hülle für den biometrischen Reisepass erworben, die das unbemerkte Auslesen der gespeicherten Ausweisdaten verhindert? (N = 2.176)</i>	8 3%	96 36,8%

Quelle: Lüdemann & Schlepper 2011, S. 133

Unter diesen Bedingungen äußerte über die Hälfte der Befragten die Absicht, zu einem Provider zu wechseln, der Telefon- und Internetverbindungsdaten nicht auf Vorrat speichert. Auch dies zeugt davon, dass die Vorratsdatenspeicherung von breiten Bevölkerungskreisen als Überwachungsmaßnahme wahrgenommen wurde.<sup>82</sup> Beinahe

<sup>82</sup> Ein eindrucksvolles Beispiel liefert auch eine repräsentative forsa-Umfrage (N = 1.002) aus dem Mai 2008, welche der Arbeitskreis Vorratsdatenspeicherung (2009, S. 3) in seiner Antwort auf den Fragebogen der Europäischen Kommission anführt: „Die Mehrheit der Befragten würde wegen der Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer



ebenso viele würden Emails oder Dateien verschlüsseln. Immerhin über ein Drittel der Befragten würde ein Programm für die Erzeugung von Passwörtern, Internet-Telefonie (z.B. Skype) oder ein Anonymisierungsprogramm verwenden.

Die Wirksamkeit solcher Schutzmaßnahmen – und hierin ist die zweite zeitliche Vergänglichkeit der Ergebnisse der Studie zu sehen – ist allerdings angesichts des Bekanntwerdens der Überwachungsmöglichkeiten durch PRISM neu zu beurteilen.<sup>83</sup> Die Motivation, diese Vorkehrungen zu treffen, trifft auf andere Voraussetzungen. Der Mehrwert dieser Untersuchung ist also in erster Linie darin zu sehen, dass sie ein nicht zu vernachlässigendes Abwehr- oder Widerstandspotenzial in der Bevölkerung – unabhängig ob und wie sich dieses in der Praxis realisieren würde – festgestellt hat. Auch im Hinblick auf die ausstehende Neuregelung der Vorratsdatenspeicherung ist dieses Ergebnis in Betracht zu ziehen: Eine derart extensive Verlagerung des Kommunikationsverhaltens der Bürger auf alternative Kommunikationswege, wie es die Ergebnisse des Projekts nahelegen, kann aus Sicht des Gesetzgebers nicht wünschenswert sein. Sie würde die Vorratsdatenspeicherung letztlich ad absurdum führen, weil sie ihren Zweck nicht mehr erreichen könnte (vgl. Schlepper & Leese 2011, S. 74).

Gleichsam als passiver Widerstand begreifen lässt sich die im SIRA-Projekt gestellte Frage danach, ob aufgrund der Sicherheitsmaßnahmen im Flugverkehr keine Flugreisen unternommen werden (Bug & Wagner 2013). 1,6 Prozent der im Rahmen der Repräsentativbefragung Interviewten gaben an, aus diesem Grund nicht fliegen zu wollen. Es handelt sich dabei also um eine sehr kleine Gruppe.

## (2) Kognitive Ebene

Auf der kognitiven Ebene kann man erheben, ob Maßnahmen eher mit Sicherheit oder Überwachung assoziiert werden. Zumeist handelt es sich dabei um Fragen, die auf die Einschätzung der Einschränkung der persönlichen Privatheit oder der Nachvollziehbarkeit der Datenverwendung zielen (z.B. das *Gefühl darüber verlieren, wie die Daten verwendet und gespeichert werden*). Auf die Frage *Fühlen Sie sich durch diese Maßnahmen in Ihrer Privatsphäre verletzt?* antworteten 17,4 Prozent der Befragten im ISIP-Projekt (2009, eigene Berechnungen, N = 2.176) mit *ja, auf jeden Fall*. Eine ähnlich hohe Zustimmung ermittelten auch Feltes et al. (2013, S. 15). 20,7 Prozent der

---

Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen.“

<sup>83</sup> Glenn Greenwald und Ewen MacAskill: Boundless Informant: the NSA's secret tool to track global surveillance data, in: *The Guardian*, 11. Juni 2013.

Verfügbar unter <http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining> [25.06.2013].



befragten Flugpassagiere stimmten der Aussage *Videoüberwachung verletzt mein Recht auf Datenschutz* zu (*trifft voll und ganz zu / trifft zu*).

Tabelle 7: Empfinden von Kontrollverlusten

<b>Gefühl des Kontrollverlusts: Erhebung von Daten</b>	
<i>Haben Sie das Gefühl, die Kontrolle darüber zu verlieren, ob, wann und in welchem Ausmaß Sie vom Staat überwacht werden?</i> (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	28,7% Zustimmung (ja, auf jeden Fall)
<i>Haben Sie das Gefühl, die Kontrolle darüber zu verlieren, wie Ihre Ausweis-, Telefon-, Passagier- und Bankdaten verwendet und gespeichert werden?</i> (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	33% Zustimmung (ja, auf jeden Fall)
<i>Haben Sie das Gefühl, dass Sie mit der Vorratsdatenspeicherung die Kontrolle über den Umgang mit Ihren Telefon- und Internetdaten verlieren?</i> (Bug & Münch 2012, S. 170, N = 1.257)	23,8% Zustimmung (ja, auf jeden Fall)
<i>(Passagierdaten) Haben Sie das Gefühl, dass Sie die Kontrolle über die Preisgabe Ihrer Daten verlieren?</i> (Bug & Wagner 2013, N = 378) <sup>84</sup>	15,1% Zustimmung (ja, auf jeden Fall)
<b>Gefühl des Kontrollverlusts: Verwendung der erhobenen Daten</b>	
<i>Glauben Sie, dass Behörden Ihre Ausweis-, Telefon-, Bank-, Passagier- und Internetdaten nur zu Zwecken verwenden, denen Sie zugestimmt haben?</i> (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	16,7% Ablehnung (nein, auf keinen Fall)
<i>Glauben Sie, dass Behörden mit Ihren Ausweis-, Telefon-, Passagier-, Bank- und Internetdaten vertrauenswürdig umgehen?</i> (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	15,8% Ablehnung (nein, auf keinen Fall)
<i>Gehen Sie davon aus, dass Behörden im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen?</i> (Bug & Münch 2012, S. 169f., N = k.A.) <sup>85</sup>	15,6% Ablehnung (nein, auf keinen Fall)
<i>(Passagierdaten) Gehen Sie davon aus, dass Behörden mit den Daten vertrauenswürdig umgehen?</i> (Bug & Wagner 2013, N = 378)	5,8% Ablehnung (nein, auf keinen Fall)
<i>Ich glaube, dass die durch Videokameras aufgezeichneten Daten zweckentfremdet werden könnten.</i> (Feldes et al. 2013, S. 15, N = 1.358)	46,8% Zustimmung (trifft voll und ganz zu/trifft zu) <sup>86</sup>

<sup>84</sup> Die tiefergehende Befragung zur Passagierdatenspeicherung bezieht sich nur auf Flugpassagiere, d.h. Personen, die im Durchschnitt mindestens einmal pro Jahr fliegen und die zudem die Frage, ob ihnen bekannt sei, dass Passagierdaten von allen Flug- und Schifffreisenden durch die Bundespolizei erfasst werden, bejahten.

<sup>85</sup> Diese Frage wurde lediglich dem Teil der Gesamtstichprobe (1.257 Befragte) gestellt, die die Frage, ob sie bereits von der Vorratsdatenspeicherung gehört hätten, bejahten. Dies entspricht einem Anteil von 81,2 Prozent an der Gesamtstichprobe (Bug & Münch 2012, S. 166).

<sup>86</sup> Wenngleich in der Studie die Bewertung auf einer fünfstufigen Skala erfolgte, ist dem Projektbericht (Feldes et al., 2013) aufgrund der Zusammenfassung der Bewertungen zu drei Kategorien *ablehnend*, *neutral* und *zustimmend* (*trifft voll und ganz zu/ trifft zu*) keine Differenzierung letzterer zu entnehmen. Aus diesem Grund wird hier, anders als bei den vorangehenden Studienergebnissen, lediglich das zusammengefasste Maß der Zustimmung dargestellt.



Im APFEL-Projekt (ebd., S. 19) wurde zudem die Einstellung zu folgender Aussage erhoben: *Die Sicherheitslage in Deutschland wird durch die zunehmende Beschneidung von Bürgerrechten stärker bedroht als durch Terroristen*. Ca. vierzig Prozent stimmten dieser Aussage zu (*trifft voll und ganz zu / trifft zu*), knapp ein Drittel war unentschieden und ungefähr ein Viertel lehnte sie ab. Daraus lässt sich durchaus eine kritische Haltung der Befragten gegenüber Terrorismusbekämpfungsmaßnahmen ableiten, nämlich in Sinne von zu viel oder übertriebenen Sicherheitsmaßnahmen.

Die Ergebnisse in Tabelle 7 zeigen darüber hinaus exemplarisch, dass sich ein Teil der Befragten nicht nur in ihrer Privatsphäre eingeschränkt fühlt. Die Studien fragen auch nach dem Gefühl, die Kontrolle über die eigenen Daten zu verlieren bzw. das Ausmaß der Überwachung nicht mehr einschätzen zu können.

Kontrollmaßnahmen, so zeigt sich, nehmen die Bürger, selbst wenn sich mit den Maßnahmen ein Gefühl der Sicherheit verbindet, durchaus kritisch wahr, dann nämlich wenn sie sich beispielsweise in ihrer Privatsphäre oder in ihrem „Recht auf informationelle Selbstbestimmung“ eingeschränkt fühlen.

Auch der Untersuchung von Lüdemann und Schlepper (2013) zufolge befördert das Sicherheitsempfinden auf der einen Seite eine positive Bewertung und kann etwa das durchaus vorhandene Misstrauen in die staatliche Datenverwendung überlagern. Auf der anderen Seite ist jedoch, wie gezeigt, durchaus eine Ab- oder Gegenwehr in der Bevölkerung auszumachen (Lüdemann & Schlepper 2011).

#### 4.2.3 Kritik und methodische Probleme

Mit der zunehmenden Bedeutung der Akzeptanzforschung im Hinblick auf neue Sicherheits- und Kontrolltechnologien haben sich nicht nur die Forschungsansätze und methodischen Herangehensweisen, sondern auch die Befunde vervielfältigt. Gleichzeitig wird „die“ Akzeptanzforschung insgesamt gleichsam zum Gradmesser eines gesellschaftlichen Konfliktpotentials.

Allerdings ist die Annahme, dass Bedrohungsgefühle und Sicherheitserwartungen die Voraussetzung für eine Zustimmung zu Sicherheitsmaßnahmen sind, wie vor allem bei quantitativen Untersuchungen unterstellt, nicht unproblematisch. Denn nicht nur können die entsprechenden Fragen, wie in Kapitel 2.3 erörtert, ihrerseits Artefakte produzieren, indem Unterschiede in der Bewertung auf die jeweilige Itemkonstruktion, d.h. der Maßnahme und ihrer Eigenschaft, rückführbar sind.<sup>87</sup> Sie *erfragen* und evozieren

---

<sup>87</sup> Ohnehin erscheint eine, über die deskriptive Darstellung hinausgehende, Vergleichbarkeit aufgrund des je unterschiedlichen Forschungsdesigns (z.B. Paneldaten gegenüber Querschnitts-



gleichsam Bedrohungswahrnehmungen. Untersucht wird dann weniger eine Akzeptanz als vielmehr eine „Passung“ – die Antworten passen zu den Fragen. Die Fokussierung auf Bedrohungs- und Sicherheitsgefühle ermittelt zudem dann weniger eine Akzeptanz im Sinne ausdrücklicher Zustimmung, vielmehr stellt sie einen Zusammenhang zwischen Sicherheitsbedürfnissen und -technologien her. Letztere erscheinen dann als Mittel, um jene zu befriedigen – die Untersuchungen werden auf diese Weise zu Effektivitätsprüfungen eines (Un-)Sicherheitsdiskurses. Wenn diese Beobachtung richtig ist, würde das bedeuten, dass die Studien zur Akzeptanz die in politischen Diskursen etablierten und medial reproduzierten Bilder und Deutungen zur Terrorismusbedrohung und -bekämpfung nicht nur fort-, sondern auch gleichsam festschreiben. Hegemoniale Deutungen werden im Moment der Befragung reproduziert.

Überdies wirft ein solcher methodisch-theoretischer Zugang nicht nur die Frage auf, ob Akzeptanz sinnvoll als eine Frage der (mehr oder weniger feststehenden) Einstellung zu begreifen ist, sondern ebenfalls inwiefern sie sich auch im Verhalten widerspiegelt.<sup>88</sup> Am Beispiel der Videoüberwachung im Flughafenbereich konstatieren Feltes et al. (2013, S. 16) in diesem Sinne denn auch einen Zwiespalt zwischen dem „Glauben daran, dass Videoüberwachung zu einem mehr an objektiver und subjektiver Sicherheit beitragen kann [...], und dem Misstrauen, dass die aufgezeichneten Daten rechtmäßig verwendet werden“.

Wenn die Studien allerdings derartige Oppositionen in der Taxonomie von Kosten-Nutzen-Kalkülen begreifen – indem sie die antizipierten negativen Konsequenzen der Kontrolltechnologien den positiven Folgen (z.B. eine Erhöhung des Sicherheitsgefühls) gegenüberstellen –, dann folgt daraus für die Frage der Akzeptanz, dass sie dann als gegeben angenommen werden kann, sobald der Nutzen der Maßnahme die Beeinträchtigung überwiegt. Derartige Rechnungen gehen allerdings davon aus, dass Sicherheitsmaßnahmen bzw. -kontrolltechnologien *eindeutig* wahrgenommen werden und die Bewertungen das Ergebnis letztlich expliziter bzw. explizierbarer Abwägungen sind. Situative und kontextabhängige Momente der Akzeptanz*herstellung* bleiben dabei unberücksichtigt.

Akzeptanz, das haben auch andere Studien gezeigt (z.B. Barben 2010; Bonß & Wagner 2012), lässt sich nicht als stabile und situationsabhängige Eigenschaft einer Technologie verstehen.

---

daten, je unterschiedliche Erhebungszeitpunkte, jeweils differenzierte Befragungsgruppen u.a. nach theoretischer und faktischer Betroffenheit) eingeschränkt.

<sup>88</sup> Der Fokus auf die Ermittlung und Festlegung akzeptanzdeterminierender Faktoren auf der Einstellungsebene leitet vor allem wirtschaftswissenschaftliche und klassisch techniksoziologische Akzeptanzforschung an. Im Mittelpunkt dieser Untersuchungen stehen hier allerdings weniger Akzeptanzbedingungen, sondern vielmehr das Ziel, auf der Verhaltensebene Akzeptanz herzustellen (siehe hierzu am Beispiel der Akzeptanz biometrischer Technologien Al-Harby 2010; Weber 2005).



Die Bedeutung von Technologien wird vielmehr in sozialen Aushandlungsprozessen erst und streng genommen immer wieder neu hergestellt (Pinch & Bijker 1984). Wie die Biometrie-Studie zeigt, können sogar gänzlich disparate situative Faktoren, wie etwa bei der Antragstellung des Personalausweises die Erwägung, nicht mit weiteren Fragen auffallen oder aufhalten zu wollen, über die Aufnahme des Fingerabdrucks in den Pass entscheiden.

Es ist dann weniger die Technologie selbst, zu der sich die Nutzer ins Verhältnis setzen, sondern die Routine und die Vorstellung von einem „normalen“ Ablauf in der Behörde. Wenn man unter Akzeptanz überhaupt fassen will, dass Bürger eine Technologie nutzen oder sich deren Anwendung nicht aktiv widersetzen, dann handelt es sich dabei keineswegs immer um eine „ausdrückliche und aktive Annahme“. Man könnte in einigen Fällen vielmehr auch von einem „gefälligen“ oder auch desinteressierten „Hinnehmen“ sprechen (Krasmann & Kühne 2013). Überdies ist auch eine praktische Nutzung der Technologie zu beobachten, obwohl der sicherheitspolitische Nutzen eher skeptisch oder sogar auch negativ im Sinne von immer mehr Überwachung und Kontrolle eingeschätzt wird. Man kann dies als „ambivalentes Einvernehmen“ bezeichnen (ebd; Krasmann & Kühne 2014).

Akzeptanz geht demnach, so lässt sich schlussfolgern, nicht in der Abwägung von Kosten und Nutzen, von Sicherheitsgewinnen oder Überwachungsbefürchtungen einer Maßnahme auf. Dies zeigt sich in aller Deutlichkeit im Biometrie-Projekt: Ebenso wie die tatsächliche Abgabe des Fingerabdrucks nicht gleichbedeutend sein muss mit dem Akzeptieren der Technologie, zieht eine kritische Beurteilung von Sicherheitsmaßnahmen auch nicht gleich die faktische Ablehnung nach sich. Variieren die Einschätzungen schon im Hinblick auf den jeweiligen Zweck einer Technologie – faktisches Wissen und Vertrautheitsgrad spielen dabei ebenso eine Rolle wie individuelle Bedürfnisse und Erfahrungen –, so gilt dies umgekehrt auch für die als „kritisch“ erachteten Aspekte einer Sicherheitstechnologie.







## 5. Akzeptanz und Vertrauen

Zumeist zielt die Forschung zur gesellschaftlichen Akzeptanz von Technik darauf, Grenzen der Akzeptanz über objektivierbare Risiken zu bestimmen, die dann ihrerseits festlegen sollen, welcher Risikograd einer Technologie im Sinne einer „ethischen Verantwortbarkeit“ akzeptabel ist (Renn 2005, S. 29). Mit solchen Bewertungen und Entscheidungen sind Akzeptanzfragen nicht nur normative, sondern auch genuin politische Fragen. Wie im Folgenden zu zeigen sein wird, lässt sich diese politische Frage theoretisch wie empirisch als eine Frage des Vertrauens im Verhältnis zwischen Bürger und Staat ausbuchstabieren.

### 5.1 Vertrauen im Schnittfeld von Sicherheit und Freiheit

Das ambivalente, wenn nicht gar paradoxe Verhältnis von Kontrolle und Vertrauen gilt als konstitutiv für demokratische Gesellschaften (z.B. Eisenstadt 2001; Putnam 1993; Sztompka 1998). Vertrauen etabliert sich dort, wo kein umfassendes oder explizites Wissen vorhanden ist bzw. sein kann (Simmel 1992). Mehr noch, als Modus eines „Verhältnisses“ (vgl. Hartmann 2011, S. 17), sei es zu Personen oder Institutionen, bedeutet es einen bewussten Verzicht auf vollständiges Wissen (Luhmann 2000) als Mittel der Kontrolle. Es ist jedoch keineswegs der Verzicht auf jegliche Information oder „gute Gründe“ (Baier 2001, S. 43). Vertrauen ist nicht naiv.

In einem allgemeinen Sinne ist Vertrauen ein Modus, Ungewissheit aufzuheben (Möllering 2006). Es bedeutet Entlastung darin, dass „Verhältnisse gegenseitigen Vertrauens in die Lage versetzen, andere Zwecke zu verfolgen als solche, die mit dem Vertrauen selbst verbunden sind.“ (Hartmann 2011, S. 17) Und „Vertrautheit“ markiert das Selbstverständliche unseres alltagsweltlichen Handelns (Schütz & Luckmann 1979, S. 174ff.). Vertrauen beinhaltet aber auch ein Moment der Gabe und Verletzungsoffenheit: „Vertraut man anderen, dann räumt man ihnen die Gelegenheit der Verletzung ein und zeigt sich sogleich zuversichtlich, dass sie diese Gelegenheit nicht nutzen werden.“ (Baier 2001, S. 43)

Im Besonderen bezieht der Begriff sich darauf, einem Gegenüber die Ausführung einer Angelegenheit vertrauensvoll zu übertragen bzw. die Sorge und Pflegschaft einer Sache, die einem „besonders am Herzen liegt“, zu überlassen (ebd., S. 45). Für das „treuhänderische Verhältnis“ zwischen Bürger und Staat, so fasst es John Locke in seiner *Zweiten Abhandlung über die Regierung*, bedeutet dies für das Ineinandergreifen von Vertrauen und Kontrolle zweierlei: Mit dem Gewaltmonopol erhält der Staat die Aufgabe, das „Eigentum“ der Bürger zu schützen.



Zu treuen Händen erlangt dieser so die (ausschließliche) Möglichkeit, eine individuelle gewaltsame Rechtsdurchsetzung zu kontrollieren und zu sanktionieren und damit Sicherheit (im gesellschaftlichen Gefüge) herzustellen (Locke 1977; dazu auch Hartmann 2011).<sup>89</sup> Für den Bürger ist dieses „Anvertrauen“ von natürlichen Rechten jedoch auch riskant, denn unter dem Begriff des Eigentums ist nicht nur der Schutz des Lebens zu verstehen, im Gesellschaftsvertrag verwirklichen sollen sich vielmehr auch die individuellen Freiheitsrechte wie z.B. die Bewegungs- oder Meinungsfreiheit (Locke 1977; in dieser Lesart auch Hartmann 2013).

„Obwohl die Erde und alle niedrigeren Geschöpfe den Menschen gemeinsam gehören, so hat doch jeder Mensch ein *Eigentum* an seiner eigenen *Person*; auf diese hat niemand ein Recht als nur er allein.“ (Locke 1977, S. 216, Herv. i. O.)

Eine vertrauensvolle Übertragung von Kontrolloptionen geht deshalb zugleich mit einem Misstrauen gegenüber der mit dieser Macht verbundenen Potenz einher, sind doch, in den Worten der Moralphilosophin Annette Baier (2001, S. 45), „diejenigen, denen wir vertrauen, um die uns wichtigen Dinge zu erschaffen und zu erhalten, jene, denen eine Verletzung am leichtesten fiele“.

Um Sicherheit und Freiheit gleichermaßen zu gewährleisten, sind in demokratischen Kulturen dem „Ermessensspielraum“ (Baier 2001, S. 46ff.) staatlichen Handelns, einschließlich der Reichweite fürsorglicher staatlicher Kontrolle, in Form „institutionalisierten Misstrauens“ (Sztompka 1998, S. 26) Grenzen gesetzt. Das Prinzip der Gewaltenteilung, eine unabhängige Justiz und unabhängige Medien, die verfassungsmäßige Regierung und Rechtsstaatlichkeit sowie der Schutz der Bürgerrechte durch die Verfassung etablieren Mechanismen, welche die rechtsetzenden und rechtsdurchsetzenden Institutionen selbst der Kontrolle unterziehen (ebd., S. 26). Sie bestimmen im gegenseitigen Verweis aufeinander den Freiheitsraum, und zwar sowohl staatlichen als auch zivilgesellschaftlichen Handelns. Indem diese Prinzipien und Mechanismen (z.B. in Gestalt verbürgter Grundrechte oder indem die Gesetze hinreichend eindeutig und konsistent sind und ihre Anwendung berechenbar ist) „normative Gewissheit“ etablieren, ermöglichen sie ein „Gefühl“ der Rechtmäßigkeit und existentieller Sicherheit<sup>90</sup> und entlasten vom „Risiko der Vertrauensgewähr“ (Luhmann 2000, S. 4). Sie ermöglichen somit auf beiden Seiten eine Freiheit des Handelns, die sich der Notwendigkeit vollständigen Wissens entledigen kann und damit Vertrauen erst ermöglicht.

Ein solches Vertrauen in staatliches Handeln bewirkt im Verzicht auf Gewalt auch das Vertrauen der Bürger ineinander. Unter dem Eindruck, dass dem eigenen Handeln

---

<sup>89</sup> So liegt die wörtliche Bedeutung des „Vertrauens“ im Kontext einer spätmittelhochdeutschen Wortfamilie, die auch das Wort „treu“ umfasst (vgl. Weltecke 2003, S. 74ff.).

<sup>90</sup> In den Worten Sztompkas (1998, S. 23): „a feeling of orderliness, predictability, regularity and existential security“.



innerhalb definierter Grenzen vertraut wird, gestattet es überdies ein Selbstvertrauen, frei handeln zu können. Demnach liegt die spezifische Sicherheit des Vertrauens darin, dass es „Zukunft vorweg[nimmt]“ (Luhmann 2000, S. 9). Es wird möglich, sich darauf zu verlassen, dass die Konditionen des eigenen Handelns, ebenso wie die Konsequenzen, die dieses mit sich bringt, auch morgen noch die gleichen sein werden wie gegenwärtig. Ein solches Vertrauen ermöglicht, trotz einer an sich kontingenten Zukunft, ein Handeln, das sich der eigenen Erwartungen versichern kann und so bewirkt, diesen zu vertrauen (vgl. ebd., S. 1ff.). Eine sich unter diesen Bedingungen etablierende „Vertrauenskultur“ ermöglicht Spontanität und Offenheit im Handeln, sowohl individuell als auch staatlich, da sie von Überwachung und Kontrolle entlastet (vgl. Sztompka 1998, S. 21f.). In Lockes (1977, S. 234, Herv. i. O.) Worten bedeutet das Gesetz dann

„in seinem eigentlichen Sinn [...] nicht so sehr die Beschränkung, sondern vielmehr die *Leitung eines frei und einsichtig Handelnden* in seinem eignen Interesse, und seine Vorschriften reichen nicht weiter, als es dem allgemeinen Wohl derer dient, die unter diesem Gesetz stehen. [...] Auch wenn es noch so oft mißverstanden werden mag, es ist nicht das *Ziel des Gesetzes*, die *Freiheit* abzuschaffen oder einzuschränken, sondern *sie zu erhalten und zu erweitern*. Denn bei sämtlichen Geschöpfen, die zu einer Gesetzgebung fähig sind, gilt der Grundsatz: *Wo es kein Gesetz gibt, da gibt es auch keine Freiheit.*“

## 5.2 Institutionalisation von Misstrauen seit 9/11

Das Verhältnis von Vertrauen und Misstrauen richtet sich demnach nicht nur auf die Grenzen des Wissbaren in komplexen Gesellschaften,<sup>91</sup> die auf versachlichte Formen des Vertrauens durch „symbolische Zeichen“, Institutionen, Expertensysteme angewiesen sind (Giddens 1996). Vielmehr verweist es eben auch auf die Grenzen eines Bedürfnisses nach Wissen und den durch das „institutionalisierte Misstrauen“ definierten „Ermessensspielraum“ staatlichen Kontrollhandelns.

Demgegenüber ist für die seit 2001 etablierten Sicherheitsgesetze ein ausgeprägtes Wissensbedürfnis bezeichnend. Unter dem Leitgedanken „Prävention durch Information“ (Glaeßner 2010, S. 181) haben diese, wie in Abschnitt 4.1 dargestellt, staatliche Kontrollbefugnisse deutlich erweitert. Das Begehren nach Wissen steht dem Vertrauen, sowohl im Verhältnis zur Gegenwart als auch Zukunft, prinzipiell konträr entgegen.

---

<sup>91</sup> Vertrauen und Misstrauen sind folglich nicht als Gegensätze, sondern vielmehr als „funktionale Äquivalente“ zu betrachten (Luhmann 2000, S. 92). Wesentlich ist hier ihr begründetes (ausgewogenes) Verhältnis zueinander.



Dabei ist das Vertrauen selbst, obgleich auf die Zukunft gerichtet, vergangenheitsorientiert. Es bezieht sich auf eine vertraute Welt, die, wie Luhmann (2000, S. 23, vgl. 9ff.) es ausdrückt, als „Hintergrundsicherung“ die Erwartungen an die Zukunft ermöglicht. Die Regierung der Sicherheit verlässt sich jedoch nicht länger auf die Gewissheiten vertrauter Welten. Ein Sicherheitsbestreben, das selbst vor der nicht-wissbaren Zukunft nicht kapituliert, diese vielmehr proaktiv mit Hilfe immer neuer Technologien der Kontrolle und Überwachung zu bearbeiten sucht, läuft Gefahr, das Vertrauensverhältnis zwischen Bürger und Staat zu verspielen. Deshalb werden Sicherheitsmaßnahmen und -technologien als eine erweiterte „Institutionalisierung von Misstrauen“, nämlich des Staates gegenüber seinen Bürgern und damit als Umkehr dieses Prinzips kritisiert, weil jener diese unter Generalverdacht stellt (z.B. Prantl 2002). Die Kontrollinstrumente selbst werden als Ausdruck eines Überwachungsbedürfnisses des Staates gedeutet, der Vertrauen durch die Erhebung und Speicherung von Informationen über die Bürger ersetzt (z.B. Tauss 2008). Der Zugriff auf Kontodaten unterschiedlicher Behörden und Institutionen markiere, so etwa der Bundesdatenschutzbeauftragte Peter Schaar, eine generelle Tendenz, dem Bürger vorab mit Misstrauen zu begegnen.<sup>92</sup> Als „Misstrauenserklärung“ an die Bevölkerung fasst auch Rolf Gössner (2002) die Integration von digitalen biometrischen Daten in nationale Identitätsdokumente, denn die Bürger müssten sich nun „behandeln lassen wie bislang nur Tatverdächtige oder Kriminelle im Zuge einer Erkennungsdienstlichen Behandlung“. Dabei wird die Besonderheit der Biometrie in der „Übersetzung“ körperlicher Merkmale und Eigenschaften gesehen, die angesichts der „Normalität von Unsicherheit“ ein Mehr an Informationen und Informationssicherheit erbringen sollen (vgl. Aas 2006, S. 144), und zwar unabhängig von einem konkreten Verdacht.<sup>93</sup> Als mittlerweile etablierter Teil von deutschen Identitätsdokumenten erscheinen die biometrischen Daten als Bestandteil eines „visible imperative“ (Haggerty 2009), der ein fehlendes Vertrauen des Staates in (die Freiheit) seine(r) Bürger bekundet (Goold 2009). Der Bürger wird gleichsam sichtbarer, während die Kontrolltechnologien selbst, wie bereits gesagt, unsichtbar: kleiner, mobiler, unscheinbarer werden (Murakami Wood 2011). Wenn sich hiermit das Prinzip des institutionalisierten Misstrauens umkehrt, dann liegt der Vertrauensbruch weniger darin, dass sich mit den Sicherheitstechnologien eben auch Kontrolle und Eingriffe verbinden, als vielmehr, so die Kritik, „dass die Bürger am Prozess der genauen Abstimmung von Sicherheits- und Freiheitsbedürfnissen nicht wirklich beteiligt werden“ (Hartmann 2013, S. 622).

---

<sup>92</sup> Zit. in: Orwell light in Deutschland. *Die Welt*, 15.03.2005. Verfügbar unter: <http://www.welt.de/print-welt/article558123/Orwell-light-in-Deutschland.html> [14. September 2013]

<sup>93</sup> Oliver Lepsius (2004, S. 78ff.) spricht in diesem Zusammenhang auch von einer „Entindividualisierung im Sicherheitsrecht“.



Vertrauen als Verhältnis, das sich um ein „anvertrautes“ Gut etabliert, setzt die Kooperation gerade voraus: indem auch derjenige, dem vertraut wird, sich auf die Vertrauenswürdigkeit und Kompetenz des Vertrauensgebers verlässt (vgl. Hartmann 2011, S. 240ff.; Baier 2001). In diesem Sinne buchstabiert sich die Problematisierung der Sicherheitsgesetzgebung seit 2001 in Übereinstimmung mit dem von Peter Sztompka (1998, S. 23ff.) entwickelten Modell vertrauensversichernder kontextueller Bedingungen demokratischer Rechtsstaatlichkeit aus. Neben dem „Schutz der Würde, Integrität und Autonomie“ und der „normativen Gewissheit“ wird eine fehlende „Transparenz“ der Sicherheitsgesetzgebung selbst kritisiert, einschließlich ihrer Zwecke, der Funktionsweise und Kompetenzen entsprechender Institutionen sowie der Möglichkeiten ihrer nachträglichen Überprüfung (vgl. Lange 2006, S. 101; Tausch 2008, S. 65).

Die potentiellen Konsequenzen einer solchen Regierung der Sicherheit mit Blick auf das Vertrauen lassen sich auf drei Ebenen nachzeichnen: im Verlust des Vertrauens in die eigene Person, im Vertrauensverlust der Bürger einander gegenüber sowie in den Staat.

### 5.2.1 Vertrauensverluste der Bürger in sich selbst

In der Taxonomie einer Theorie des Vertrauens lassen Anti-Terrorismusmaßnahmen sich als ein Versuch verstehen, sich mit dem „Unvertrauten“ vertraut zu machen, die unbekannt Bedrohung gewissermaßen mit Hilfe von Techniken der Generierung von „Wissen“, Informationen und Kontrolle einzuholen. Sicherheitsmaßnahmen und -technologien können Sicherheit herstellen, sie können Sicherheitsgefühl steigern, sie können Gefahren und Bedrohungen abwehren usw. Ebenso können sie aber auch, als Wissens- und Kontrollambitionen, Verunsicherung und Misstrauen erzeugen, wie bereits anhand der empirischen Studien gezeigt vor allem in dem Maße, in dem der Verdacht ubiquitär und insofern nicht mehr nachvollziehbar wird (Cole 2002; Hartmann 2013, S. 624). Die undifferenzierte Überwachung bzw. die diffuse Allgegenwärtigkeit von Kontrolltechnologien können das Vertrauen in die eigenen Erwartungen und die eigene Handlungssicherheit erschüttern: Wenn morgen schon alles zum Risiko werden kann, worauf kann ich mich dann noch verlassen, woran mein Handeln ausrichten? Angesichts eines solchen „Unvertrautwerdens“ mit der Welt (vgl. Luhmann 2000, S. 22ff.) gerät auch das eigene Handeln zum Risiko. Denn freies Handeln heißt auch die Möglichkeit wahrnehmen zu können, dies fernab der Erwartungen Anderer entfalten zu können. So zeigt sich hier exemplarisch der Zusammenhang von Vertrauen und Privatheit verstanden als ein Recht, „nicht gegen den eigenen Willen gekannt zu werden, das Recht, nicht jede Handlung, jede Aussage, jede Form menschlichen Kontakts vor einem möglichen Auge einer panoptischen Öffentlichkeit abwägen zu müssen“ (Ammicht-Quinn & Rampp 2010, S. 146). Dieser „Kernbestand menschlicher Würde



und Autonomie“ (ebd.) erscheint durch Überwachungstechnologien zumindest in dem Moment eingeschränkt, in dem diese eine ständige Auseinandersetzung mit Normalitätsanforderungen (vgl. Endreß & Rampp 2013, S. 150) bzw. Aufforderungen zur Unschuldsversicherung hervorrufen (vgl. Hartmann 2013, S. 824).

### 5.2.2 Vertrauensverluste der Bürger in ihre Mitmenschen

Wenn die diffuse Allgegenwärtigkeit von Überwachungstechnologien eine Aufforderung zur Verhaltensanpassung transportieren und gleichzeitig Ungewissheit darüber erzeugen, ob man den vermeintlichen Normalitätsanforderungen auch genügen kann, dann müsste diese Verunsicherung auch das Verhältnis der Bürger zueinander beeinflussen (vgl. Endreß & Rampp 2013, S. 156). In einer Situation diffuser Risiken, so das Argument, halten die Bürger selbst nach Anzeichen einer Gefahr Ausschau (vgl. Hartmann 2013, S. 623). Misstrauen tritt an die Stelle von Vertrauen und Selbstverständlichkeit. Und wenn Grundlage des Vertrauens in Interaktionen eine spezifische „Kultur des Taktes“ im „wechselseitigen Voneinander-Notiz-Nehmen“ (Endreß 2012, S. 88) ist, dann, so lässt sich weiterdenken, verkleinert die Wahrnehmung einer neuen Verantwortung im allgegenwärtigen Verdacht den Raum, der normalerweise durch „die höfliche Unaufmerksamkeit“ geboten ist (vgl. Endreß & Rampp 2013, S. 156f.). Man kann allerdings auch die gegenteilige Schlussfolgerung ziehen. Die erhöhte, undifferenzierte Überwachung führt vielmehr, Benjamin Goold (2009, S. 212f.) zufolge, zu einer Verringerung wechselseitiger sozialer Kontrolle. Angesichts von Kontrolltechnologien, z.B. im Flughafenbereich, seien die Bürger mehr mit der Selbstmodulation ihres Verhaltens beschäftigt – d.h. sie richten alle Aufmerksamkeit auf das Vermeiden eigener „Auffälligkeiten“ und eben nicht mehr auf das möglicherweise auffällige Verhalten ihrer Umgebung und anderer Personen.

Die *Surveillance Studies* sehen ein institutionalisiertes Misstrauen in der Praxis der Kontrolltechnologien selbst angelegt, denn wie sich Menschen identifizieren, zeigt auch, wie sie Vertrauen etablieren. Dies gelte insbesondere für die Funktionsweise biometrischer Authentifizierungstechnologien (vgl. Aas 2006, S. 144ff.), mit denen das Geheimhalten von Passwörtern ebenso obsolet wird wie das Sichern eines „Tokens“ (vgl. Pato & Millet 2010, S. 5). Auf der Basis körperlicher Merkmale entscheidet die Technologie in der ihr eigenen binären Logik über den Zugang und die Vertrauenswürdigkeit des Gegenübers. Das in die Technologie eingeschriebene Misstrauen verfestigte sich in einer allgemeinen „Misstrauenskultur“:



Indem Menschen zunehmend und ungleich einem Mehr an Kontrolle ausgesetzt seien, verlören sie gleichsam die Fähigkeit, einander auf eine vertrauensvolle Weise zu begegnen (vgl. Ellis 2011).<sup>94</sup>

### 5.2.3 Vertrauensverluste der Bürger in den Staat

Wenn das Vertrauen in staatliches Handeln im Recht verankert ist und das „Vertrauen in die Funktionsfähigkeit [der] immanente[n] Kontrollen“ einschließt (Luhmann 2000, S. 77), dann beschränkt es sich darauf allerdings nicht. Es hat vielmehr selbst einen „intrinsischen“ Wert (in diesem Sinne v.a. Hartmann 2011; auch Baier 2001): Auch wenn das institutionalisierte Misstrauen dazu dient, die eigene Vertrauenswürdigkeit unter Beweis zu stellen (Sztompka 1998, S. 3), zieht es seine Stärke daraus, dass die (Selbst-)Kontrollmechanismen ihrerseits eher im Hintergrund bleiben (ebd., S. 29). Wenn diese Beobachtung zutreffend ist, dann stellt sich allerdings die Frage, ob Evaluationen über die Einhaltung institutioneller Regeln nicht kontrafaktisch sind, oder anders gesagt: Ob diese sich in der Konsequenz nicht faktischer Überprüfbarkeit entzieht. Die vertrauensvolle Übertragung von Kontrolloptionen bedeutet, sich darauf zu verlassen, dass derjenige, dem diese Macht zugestanden wird, wohlwollend, d.h. zu *meiner* Sicherheit mit diesen Potentialen umgehen wird (vgl. Baier 2001, S. 43, dazu auch Hartmann 2011). Bürger befolgen Entscheidungen der Regierung und staatlicher Institutionen nicht aufgrund von Sanktionsdrohungen, sondern aufgrund des Glaubens, dass diese prinzipiell in ihrem Interesse bzw. zu ihrem Wohl handeln. So beruht die Akzeptanz staatlichen Handelns eben auch auf der Wahrnehmung und Erfahrung etwa einer fairen Behandlung (Tyler 1990).

Vertrauen ist insofern auch die Voraussetzung dafür, dass sich die Ausübung von Zwang in behördlichem Handeln erübrigt. Freilich ist es trotz fehlenden oder schwindenden Vertrauens weiterhin möglich, sich auf die Herstellung von Sicherheit zu verlassen. Fraglich zu werden droht dabei aber, um wessen Sicherheit es sich schließlich handelt (vgl. Baier 2001, S. 42ff.). Wenn Sicherheitsmaßnahmen als Zwangsmaßnahmen und das Handeln von Sicherheitsbehörden nicht mehr als zurechenbar, sondern

---

<sup>94</sup> Darren Ellis (2011) analysiert die Effekte institutionellen Misstrauens auf die Fähigkeit personelles Vertrauen auszubilden. Er bezieht sich u.a. auf eine Studie von Greg Noble (2005) „The Discomfort of Strangers: Racism, Incivility and Ontological Security in a Relaxed and Comfortable Nation“, zu Erfahrungen „ontologischer Unsicherheit“ (S. 5) von v.a. islamischer Migranten in Australien nach den Ereignissen des 11. Septembers 2001. Danach seien Islamophobie und ihr Wiederhall in politischen Diskursen Ausdruck institutionalisierten Misstrauens. Für die von dieser kontinuierlichen Erfahrung betroffenen Bürger seien damit tiefe emotionale Einflüsse verbunden, die sich auf die Fähigkeit personelles Vertrauen aufzubauen, auswirkten (Ellis 2011, S. 9).





als intransparent oder willkürlich wahrgenommen werden,<sup>95</sup> gilt eine „Schwelle“ des Handelns als erreicht (Luhmann 2000, S. 37), die das Vertrauen in den Staat und seine Institutionen bedroht. An die Stelle der „Täuschung“ des Vertrauens (ebd., S. 38) tritt die „Enttäuschung“.

Ein solcher Vertrauensverlust kann, wie Goold (2009, S. 208ff.) in Bezug auf Überwachungstechnologien wie etwa den umfangreichen Einsatz von Videokameras in Großbritannien problematisiert, weitreichende Konsequenzen für eine demokratische Kultur haben. Der Vertrauensverlust der Bürger in den Staat könne nicht nur den Entzug einer, zumindest minimalen, Unterstützung der Regierung, sondern, im Grunde in Form eines expliziten Misstrauens, auch die Hinwendung zu alternativen nicht-demokratischen Regierungsformen nach sich ziehen: „The increasing trend towards greater levels of state surveillance has the potential to undermine well-established norms of governance based on consent and a shared commitment to democratic forms of government“ (ebd., S. 207).

Ob diese eher theoretischen Analysen zur gesellschaftlichen Logik des Vertrauens indes auch die aktuelle Situation in Deutschland beschreiben, wird im Folgenden zu erörtern sein.

### 5.3 Sicherheitsmaßnahmen und das Vertrauen der Bürger

Die Auswirkungen staatlichen Sicherheitshandelns seit 2001 in Deutschland auf das Vertrauen der Bürger in den Staat sind empirisch bislang selten adressiert worden. Die Studie „Der ‚überwachte Bürger‘ zwischen Apathie und Protest“ (z.B. Schlepper & Lüdemann 2010), die Untersuchungen im Teilprojekt „Der Einfluss institutioneller Regimes auf die Billigung sicherheitspolitischer Maßnahmen“ des Forschungsverbundes SIRA (z.B. Bug & Münch 2012; Bug & Wagner 2013) oder im APFEL-Projekt (Feldes et al. 2013) erheben Vertrauenseinstellungen auf der Basis quantitativer Befragungen. Bei der nachfolgenden Präsentation der Ergebnisse dieser Untersuchungen werden wir auch erörtern, inwiefern eine solche Konzeptualisierung geeignet erscheint, die „Vertrauensfrage“ hinreichend zu erfassen, und welche Einsichten ein qualitativer Zugang darüber hinaus zu ermitteln vermag. Deshalb diskutieren wir anschließend noch einmal exemplarische Ergebnisse aus dem Projekt zur Akzeptanz von Fingerabdrücken im Alltag.

---

<sup>95</sup> Wenn „organisierte Unverantwortlichkeit [...] von daher als Krisenszenario gelten“ muss (Endreß 2012, S. 94), dann könnte sich beispielsweise die seit dem 6. Juni 2013 andauernde Debatte zum geheimen Überwachungsprogramm PRISM der US-amerikanischen National Security Agency, als eine solche Krise des Vertrauens erweisen.



Inwieweit staatliche Überwachungsmaßnahmen zur Terrorismusbekämpfung zum Vertrauen der Bürger beitragen, wurde im Rahmen des Projektes „Der ‚überwachte Bürger‘ zwischen Apathie und Protest“ über eine Einschätzung der Befragten zu der Frage *Wieviel Vertrauen haben Sie in die Bundesregierung?* auf einer vierstufigen Skala von *sehr großes Vertrauen* bis *überhaupt kein Vertrauen* ermittelt (Schlepper & Lüdemann 2010, S. 572f.). Wie die in Tabelle 8 dargestellten Ergebnisse zeigen, setzt mehr als die Hälfte der Befragten nur ein geringes Vertrauen in die Regierung.

Tabelle 8: Häufigkeiten der Antworten auf die Frage nach dem „Vertrauen in die Regierung“

Antwortkategorie	N	%
<i>sehr großes Vertrauen</i>	61	2,8
<i>großes Vertrauen</i>	783	36,0
<i>geringes Vertrauen</i>	1136	52,2
<i>überhaupt kein Vertrauen</i>	179	8,2
<i>weiß nicht</i>	16	0,7
<i>verweigert</i>	1	0
<i>Summe</i>	2176	100

Quelle: Schlepper & Lüdemann 2010, S. 573

Der u.a. aus der Governance-Forschung stammenden Prämisse folgend, dass die Bürger sich dann gut regiert fühlen, dem Staat vertrauen und folglich bereit sind, Gegenleistungen zu erbringen, wenn sie die staatliche Performanz, d.h. die „Leistungen“ des Staates als hoch einschätzen, spiegelt sich in der Studie wider: Je geringer der Nutzen der Maßnahmen eingeschätzt wurde, umso geringer war auch das Vertrauen in die Regierung (zu weiteren Einflussfaktoren siehe Schlepper & Lüdemann 2010). Umgekehrt, so das Ergebnis der Studie, stärkt eine positiv bewertete Performanz staatlichen Handelns auch das Vertrauen in die Regierung. Gleichwohl weisen die Autoren darauf hin, dass ein solcher Effekt nicht zwangsläufig langfristig sein muss und die große Beteiligung an Bürgerrechtsaktionen wie z.B. „Freiheit statt Angst“ gleichermaßen belegt,<sup>96</sup> dass die Sicherheitsmaßnahmen durchaus mit Blick auf die weiterreichenden Konsequenzen für die persönliche Freiheit wahrgenommen werden (ebd., S. 574f.).<sup>97</sup>

---

<sup>96</sup> „Freiheit statt Angst“ ist das Motto einer Großdemonstration, die in Deutschland seit 2006 jährlich stattfindet. Informationen finden sich unter <http://blog.freiheitstattangst.de/>.

<sup>97</sup> Hinsichtlich der für diesen Zusammenhang ermittelten Einflussfaktoren wie z.B. der Kriminalitätsfurcht oder des Nutzens der Maßnahmen (Sicherheitsgefühl) müssen zudem die bereits in den Abschnitten 2.2.3 und 4.2.3 diskutierten methodisch bedingten Einschränkungen berücksichtigt werden.



Darüber hinaus sind – auch bei einer klaren theoretischen Konzeptualisierung des „Vertrauens in politische Institutionen“ wie in der Studie von Schlepper und Lüdemann (2010) – generalisierende Fragen, wie *Wieviel Vertrauen haben Sie in die Regierung* oder „Inwiefern würden Sie der folgenden Aussage *Den meisten Menschen kann man vertrauen* zustimmen“ nicht unproblematisch. Sie verlangen dem Bürger, gleichsam trotz und ungeachtet der ex ante gebildeten Hypothesen über Zusammenhänge des Vertrauens, im Moment der Fragestellung eine „Abstraktion von Sozialbeziehungen“ ab (Fuhse 2002, S. 424). Die Idee einer generellen Vertrauenseinstellung, die sich hinter der Aufforderung zu einer solchen Beurteilung verbirgt, provoziert, wenn die Frage zufriedenstellend beantwortet werden soll, die Gegenfrage: „wobei?“ (ebd., hier zur Problematik von Fragen, wie „kann man Menschen im Allgemeinen vertrauen?“).

Eine weitere Möglichkeit, der Frage des Vertrauens nachzugehen, bieten Items, die, wie bereits in Abschnitt 4.2.2.4 dargestellt, die Vertrauenswürdigkeit des staatlichen Kontrollhandelns thematisieren. Sowohl in der Studie „Der ‚überwachte Bürger‘ zwischen Apathie und Protest“ als auch im SIRA-Projekt wurden die Befragten gebeten anzugeben, inwieweit sie davon ausgehen bzw. daran glauben, dass Behörden mit den erfassten Daten vertrauenswürdig umgehen. In der in Tabelle 9 dargestellten Verteilung der Antworten zeigt sich, dass die Befragten diesbezüglich eher geteilter Meinung sind.

Tabelle 9: Glaube an einen vertrauenswürdigen Umgang mit Daten durch die Behörden

	<i>ja, auf jeden Fall</i>	<i>eher ja</i>	<i>eher nein</i>	<i>nein, auf keinen Fall</i>
<i>Glauben Sie, dass Behörden mit Ihren Ausweis-, Telefon-, Passagier-, Bank- und Internetdaten vertrauenswürdig umgehen?</i> (ISIP-Projekt, eigene Berechnungen, N = 2.176)	7,9%	36,1%	39%	15,8%
<i>Gehen Sie davon aus, dass Behörden im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen?</i> (Bug & Münch 2012, S. 169f., N = k.A.) <sup>98</sup>	7,1	43,3	k.A. <sup>99</sup>	15,6%
<i>(Passagierdaten) Gehen Sie davon aus, dass Behörden mit den Daten vertrauenswürdig umgehen?</i> (Bug & Wagner 2013, N = 378) <sup>100</sup>	19,6%	52,1%	22,2%	5,8%

<sup>98</sup> Diese Frage wurde dem Teil der Gesamtstichprobe (1.257 Befragte) gestellt, die die Frage, ob sie bereits von der Vorratsdatenspeicherung gehört hätten, bejahten. Dies entspricht einem Anteil von 81,2 Prozent an der Gesamtstichprobe, eine genaue Zahl ist dem Beitrag jedoch nicht zu entnehmen (Bug & Münch 2012, S. 166).

<sup>99</sup> Dem Beitrag von Bug und Münch sind differenzierte Zahlen zu den Antwortkategorien *eher nein* und *nein, auf keinen Fall* nicht direkt zu entnehmen. 15,6 Prozent bezeichnen die Autoren als „die sehr kritische Gruppe“ (2012, S. 170), sodass hier davon ausgegangen wird, dass es sich dabei um die Personengruppe handelt, die die Kategorie *nein, auf keinen Fall* angaben.



Was hier in Frage zu stehen scheint, deutet auf eine antizipierte Diskrepanz zwischen dem angekündigten Handeln der Institution (Luhmann 2000) und den Vorstellungen oder Erfahrungen darüber, welche Zwecke dieses tatsächlich verfolgt bzw. verfolgen könnte. Wenngleich sich die Fragestellung hier deutlich konkreter auf staatliches Handeln bezieht, lässt sich aus der Bewertung der Vertrauenswürdigkeit keineswegs ein Vertrauensverlust oder fehlendes Vertrauen oder gar Misstrauen ableiten. Ebenso stellt sich erneut die Frage, ob mit Fragen nach dem Vertrauen die fehlende Vertrauenswürdigkeit nicht womöglich erst kommuniziert wird.

Doch auch wenn die quantitativen Untersuchungen die Gründe für ein Unbehagen der Bürger gegenüber dem staatlichen Umgang mit den erhobenen Daten, das sich hier andeutet, unbeschrieben lassen, so zeigen sie, auch unabhängig von den theoretischen und methodischen Unterschieden, dass unter dem Eindruck einer Betroffenheit von Kontrollmaßnahmen eine „kritische Masse“ (Bug & Wagner 2013) von Bürgern auszumachen ist. Eine solche „kritische Betroffenheit“ drückt sich eben nicht nur in dem Gefühl aus, unberechtigt verdächtigt und in der eigenen Freiheit eingeschränkt zu werden. Die „verunsichernden Nebeneffekte“ (Bug & Münch 2012, S. 171) beziehen sich vielmehr auch auf eine neue Ungewissheit über den tatsächlichen Verwendungszweck der erhobenen Daten. Davon auszugehen ist, wie bereits erörtert, dass diese Ungewissheit und das Unbehagen auch über die konkrete Maßnahme, auf die sie sich beziehen, hinausgehen und unabhängig davon sind, ob die jeweilige Maßnahme auch befürwortet oder zumindest positiv bewertet wird.

Auf die Definition des Vertrauens zurückgewendet: Einem Gegenüber ein wichtiges Gut anzuvertrauen und im Gegenzug dem Anderen Macht darüber einzuräumen, muss auch heißen, dass sich dieser nicht um mehr kümmert, als ihm anvertraut wurde (Baier 2001, S. 46). Vor allem neue Kontrolltechnologien, die mit digitalisierten Daten operieren, können das Vertrauen zumindest zu irritieren, gerade weil sie schwer kontrollierbar: durchschaubar sind.

Inwiefern den Befragten ein (potentieller) Missbrauch – auch im Sinne einer nicht-intendierten Ver- bzw. Entwendung von Daten – oder aber die nachträgliche Erweiterung eines ursprünglichen Verwendungszwecks vorstellbar erscheint, wird je nach Kontext unterschiedlich bewertet. Die Ergebnisse der quantitativen Studien zeigen, dass verschiedenen Akteuren, die im Rahmen der Maßnahmen Zugang zu Daten erhalten, eine unterschiedliche Vertrauenswürdigkeit im Umgang mit diesen zugeschrieben wird. Die in Tabelle 10 dargestellten Daten aus dem SIRA-Projekt machen deutlich, dass mehr Befragte von einem nicht vertrauenswürdigen Umgang mit den Daten durch Kommunikationsunternehmen bzw. Verkehrsunternehmen als durch Behörden ausgehen.

---

<sup>100</sup> Befragt wurden nur Passagiere mit Vorwissen zur Fluggastdatenspeicherung (N = 378).



Tabelle 10: Glaube an einen vertrauenswürdigen Umgang mit erhobenen Daten durch nicht-staatliche Institutionen

<i>Gehen Sie davon aus, dass <u>Behörden</u> im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen? (Bug &amp; Münch 2012, S. 169f., N = k.A.)<sup>101</sup></i>	15,6% Ablehnung (nein, auf keinen Fall)
<i>Gehen Sie davon aus, dass <u>Kommunikationsunternehmen</u> im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen? (Bug &amp; Münch 2012, S. 169, N = k.A.)<sup>102</sup></i>	26,8% Ablehnung (nein, auf keinen Fall)
<i>(Passagierdaten) Gehen Sie davon aus, dass <u>Behörden</u> mit den Daten vertrauenswürdig umgehen? (Bug &amp; Wagner 2013, N = 378)<sup>103</sup></i>	5,8% Ablehnung (nein, auf keinen Fall)
<i>(Passagierdaten) Gehen Sie davon aus, dass <u>Verkehrsunternehmen</u> mit den Daten vertrauenswürdig umgehen? (Bug &amp; Wagner 2013, N = 378)<sup>104</sup></i>	7,1% Ablehnung (nein, auf keinen Fall)

Im Projekt zur Akzeptanz von Fingerabdrücken zeigen sich ebenfalls derartige kontextuelle Unterschiede. Darüber hinaus wird jedoch in den Interviews deutlich, woran sich Nutzer von Fingerabdrucktechnologien in ihrer Bewertung orientieren. Zunächst handelt es sich um Unterscheidungen, die Fragen einer grundsätzlichen Legitimität der Erfassung von Daten aufwerfen und sowohl an Zwecken als auch an kontextuell etablierten Regeln der Datenpreisgabe orientiert sind. So kann es auf der einen Seite als angemessen erscheinen, den Fingerabdruck im normalen Behördenkontext zum Zwecke der Versicherung der Identität im Falle einer polizeilichen Kontrolle preiszugeben, den Fingerabdruck dem Arbeitgeber zum Zwecke der Zeiterfassung zu überlassen jedoch „ginge gar nicht“, wie es ein Befragter ausdrückt. Wenn sich hier kontextuelle „Vertrauensprofile“ (Endreß 2012, S. 97) andeuten, dann ließe sich in Anlehnung an Helen Nissenbaums Konzept der „kontextuellen Integrität“ (2004) die Frage aufwerfen, wer zu welchem Zweck welche (persönlichen) Daten einfordern und verwenden darf – eben auch mit Blick auf die kontextuell je unterschiedlichen, etablierten Regeln des Informationsaustausches. Exemplarisch ist etwa die im Vorfeld der geplanten Integration des Fingerabdrucks in deutsche Ausweispapiere öffentlich diskutierte Frage, ob es sich nicht um eine unzulässige Verdachtserweiterung handle, die lediglich im bis dato etablierten kriminalistischen Anwendungsbereich legitim sei (Gössner 2007).

Für die Frage nach dem Vertrauen muss eine solche Maßgabe jedoch um die Einsicht ergänzt werden, dass das Vertrauen sich gerade nicht zwangsläufig durch ein Abmessen der kontextuellen und gleichsam rechtlichen Grenzen ergibt. Vertrauen entsteht

<sup>101</sup> Diese Frage wurde dem Teil der Gesamtstichprobe (1.257 Befragte) gestellt, die die Frage, ob sie bereits von der Vorratsdatenspeicherung gehört hätten, bejahten. Dies entspricht einem Anteil von 81,2 Prozent an der Gesamtstichprobe, eine genaue Zahl ist dem Beitrag jedoch nicht zu entnehmen (Bug & Münch 2012, S. 166).

<sup>102</sup> Vgl. Fußnote 96.

<sup>103</sup> Befragt wurden nur Passagiere mit Vorwissen zur Fluggastdatenspeicherung (N=378).

<sup>104</sup> Vgl. Fußnote 97.



sukzessive durch Interaktionsgeschichten und in der Etablierung einer politischen Kultur eben auch des Umgangs mit Kontroll- und Überwachungstechnologien (Gaycken 2013). Und es sind häufig Elemente der vertrauten Normalität, die das Vertrauen erhalten, wenn also, wie sich im Biometrie-Projekt zeigt, der Zweck der Nutzung einer Kontrolltechnologie darin liegen kann, die Ausweispapiere „korrekt“ zu haben; oder wenn aufgrund des etablierten Vertrauensverhältnisses zum Arbeitsgeber das „eigentlich komische“ Fingerabdruckverfahren zum Zwecke der Zeiterfassung in der vertrauten Arbeitsumgebung akzeptiert wird.

Vertrauen ist nicht statisch, es ist kontextuell und situativ variabel. Das Vertrauen in staatliches Kontrollhandeln kann, wie unsere Studie gezeigt hat, ambivalent sein, und es kann sich auch auf ganz unterschiedlichen Ebenen manifestieren: bezogen etwa auf die Technologie selbst oder aber auf den (gegebenenfalls als unklar und undurchsichtig empfundenen) Zweck bzw. die potentiell erweiterbaren Möglichkeiten. Nutzer von Fingerabdrucktechnologien fühlen sich nach eigenen Angaben durchaus sicherer dadurch und haben Vertrauen in die Funktionsweise oder auch die Handhabung und den jeweiligen Betreiber. Doch schließt das größere Sicherheitsempfinden oder auch eine Wahrnehmung der mit der Technologie verbundenen Annehmlichkeiten, wie gesagt, umgekehrt keineswegs ein Misstrauen gegenüber den Betreibern aus. So fühlen sich viele Nutzer der Fingerabdrucktechnologie in Ausweisdokumenten „betroffen“ angesichts dessen, dass ihnen staatliches Handeln zunehmend nicht mehr durchsichtig oder auch berechenbar erscheint – könnten die Fingerabdrücke doch morgen Zwecken zugeführt werden, die nicht absehbar waren. So kommunizieren Befragte, für die sich mit dem Fingerabdruck im Personalausweis durchaus Vorteile verbinden, gleichsam Vertrauensvorbehalte gegenüber staatlichen Institutionen angesichts einer möglichen unberechtigten Weitergabe und Nutzung ihres Fingerabdrucks durch staatliche Behörden.

Zugleich deutet ein solcher, bei vielen Befragten anzutreffender Vertrauensvorbehalt keineswegs auf die Etablierung einer *allgemeinen* Misstrauenskultur hin, wie die *Surveillance Studies* argwöhnen – auch wenn diese zu Recht einen Bias gegenüber gesellschaftlichen Minderheiten monieren (etwa Ellis 2011; International Helsinki Federation for Human Rights 2005). Misstrauen ist nicht als das Gegenteil von Vertrauen zu verstehen, sondern vielmehr als sein „funktionales Äquivalent“ (Luhmann 2000, S. 92). Die Ambivalenz, welche die Befragten zum Ausdruck bringen, lässt sich insofern eher als ein gesundes Misstrauen gegenüber staatlichen Sicherheitsambitionen lesen.





## 6. Zusammenfassung und Empfehlungen

Terroristische Anschläge können verheerende Folgen haben. Sie können Leben zerstören, sie können Angst und Schrecken erzeugen, und sie können Gesellschaften verunsichern. Doch nicht nur terroristische Aktionen, auch terroristische Bedrohungen sind real. Obgleich sie von Erwartungen und nicht von Tatsachen handeln, die schon eingetreten sind, sind Bedrohungen, zum Beispiel als Befürchtungen oder in Form von Angst, erlebbar und erfahrbar. Auch können Bedrohungen sichtbar sein. Wir können die Zeichen lesen, die uns eine Gefahr anzeigen. In der Terrorismusbekämpfung – wie übrigens bei terroristischen Anschlägen – ist genau dies im Spiel: die Zeichen, die Deutung, die Diskussionen um den Terrorismus und vor allem die terroristische Bedrohung. Sie alle formen unsere Wahrnehmung dieser Bedrohung bzw. bringen diese in gewisser Weise erst hervor. Deutungen und Sinnzuschreibungen sind freilich notwendig. Wir könnten uns ohne sie nicht darüber verständigen, mit was für einer Art von Bedrohung und ob wir es überhaupt zum Beispiel mit einer terroristischen Bedrohung zu tun haben.

Wenn diese Fragen nicht selten umstritten sind, so ist das nicht nur auf unterschiedliche Meinungen oder Interessen, sondern überhaupt auf unterschiedliche Einschätzungen zurückzuführen. *Die gesellschaftliche Konstruktion von Sicherheit* setzt an dieser Frage an, wie wir zu unseren Einschätzungen von Bedrohungen bzw. zu einem Gefühl von Sicherheit oder auch Unsicherheit gelangen. Dabei gehen die Autoren davon aus, dass gesellschaftliche *Konstruktionen* nicht allein Deutungen und Sinnzuschreibungen sind. Die Wahrnehmung von Bedrohungen ist vielmehr wesentlich *medial* vermittelt, und das heißt durch die Massenmedien, vor allem das Fernsehen, aber auch durch die Sicherheitsmaßnahmen und Überwachungstechnologien selbst.

Eine einfache Antwort darauf, wie man sich den Zusammenhang zwischen „tatsächlichen“ Anschlägen einerseits, Mediendarstellungen, politischen Diskursen und Sicherheitsmaßnahmen andererseits und schließlich der gesellschaftlichen Wahrnehmung von Bedrohungen bzw. Sicherheit vorstellen muss, lässt sich nicht geben. Ein unmittelbarer Zusammenhang, soviel ist allerdings gewiss, zwischen terroristischen Aktionen und gesellschaftlicher Verunsicherung ist nicht ableitbar. Mehr noch macht eine solche Aussage sozialwissenschaftlich betrachtet überhaupt keinen Sinn, weil man davon ausgehen muss, dass auch tatsächliche Aktionen stets vermittelt: kommuniziert werden müssen. Die kriminologische Forschung zur „subjektiven Sicherheit“ hat überdies gezeigt, dass über das Thema von Kriminalität und Terrorismus hinaus hier noch ganz andere Aspekte eine zentrale Rolle spielen. Sicherheit ist eben auch soziale Sicherheit, abhängig auch von der Zufriedenheit mit der eigenen, ökonomischen und sozialen, Lebenssituation; und entscheidend ist schließlich auch die „politische Kultur“, das heißt, ob und in welcher Weise die Bürger politisch einbezogen werden und





vor allem, ob sie ihrer Regierung und staatlichen Institutionen vertrauen können. Sicherheitsdiskurse und Sicherheitsmaßnahmen führen keineswegs unbedingt zu mehr (subjektiver) Sicherheit, im Gegenteil. Sicherheitsmaßnahmen und Überwachungstechnologien können auch Unsicherheit erzeugen, und Diskurse über Sicherheit, so lautet ein zentrales sozialwissenschaftliches Argument, haben vor allem eine Funktion: Sicherheitsmaßnahmen zu initiieren und zu begründen.

Die vorliegende Studie lotet deshalb zunächst die „Logik der Sicherheit“ selbst aus: Sicherheit ist ein spezifisch modernes Problem, und das heißt einerseits verhaftet in einer Vorstellung von Machbarkeit und einem Ideal von Sicherheit, die unbedingt erstrebenswert ist, und andererseits mit der Chance und Fähigkeit versehen, die Widersprüche dieser Sicherheitsvorstellungen reflektieren zu können. Eines der Paradoxa liegt darin, dass Sicherheit stets mit einem Nicht-Wissen zu kämpfen hat: mit Gefahren und Bedrohungen, die noch nicht eingetreten sind und die wir in diesem Sinne auch noch nicht kennen – während wir aber schon meinen, agieren zu müssen, um die Bedrohung abzuwehren. Die Regierung der Sicherheit muss deshalb mit diesem Wissensmangel, sie muss selbst mit Ungewissheit fertig werden. Zugleich ist genau dies ihr Potenzial: Sicherheitsmaßnahmen können sich selbst begründen.

Die gesellschaftliche Bedrohungs- und Risikowahrnehmung lässt sich zunächst mit Blick auf die Rolle von Massenmedien bestimmen. Dabei macht die in der Medienwirkungsforschung und auch in der Kriminologie verbreitete Kritik an einer Überzeichnung, Verzerrung und übertriebenen Darstellung des „Terrorismus-Themas“, so der Ansatzpunkt hier, wenig Sinn: Es fehlt der objektive Referenzpunkt. Vielmehr bilden mediale Darstellungen eine eigene Realität aus, und als solche sind sie daraufhin zu analysieren, welche Bilder von Terrorismus, von einer Bedrohung und dem „Sinn“ von Sicherheitsmaßnahmen sie zeichnen.

Die Befragungen zur Bedrohungs- und Risikowahrnehmung von terroristischen Anschlägen in der Bevölkerung wiederum lassen kaum ein einheitliches Bild erkennen. Zwar hat sich in einigen Studien gezeigt, dass sich die wahrgenommene allgemeine Bedrohung durch terroristische Anschläge durchaus auf einem ähnlichen Niveau mit existenziellen, gesundheitlichen und sozialen Bedrohungsfaktoren bewegt. Die Antworten sind aus methodischer Sicht in vielfacher Hinsicht kritisch zu bewerten. Zum einen ist in Zweifel zu ziehen, dass die Befragten derartige Differenzierungsleistungen überhaupt vornehmen, das heißt eine Vielzahl verschiedener Bedrohungsfaktoren klar voneinander trennen und im Befragungsmoment tatsächlich unmittelbar abrufen. Zum anderen fallen die Ergebnisse auch abhängig davon aus, *wann* nach der Bedrohungswahrnehmung gefragt wird (z.B. nach spektakulären Ereignissen) und *wie* gefragt wird: Sie variieren mit den verwendeten Indikatoren. Je nachdem, ob Ängste, Sorgen, Bedrohungsgefühl, Beunruhigung oder Verunsicherung erhoben werden, divergieren die Befunde teilweise erheblich.



Gleiches gilt für die Fragetechnik (offen vs. geschlossen). Wird Terrorismus nicht als Antwortkategorie vorgegeben, wird er nur selten als Bedrohungsfaktor genannt.

Eine Schlussfolgerung für die sozialwissenschaftliche Forschung wäre demnach, nicht nur Einstellungen und Einschätzungen abzufragen, sondern vielmehr das tatsächliche Verhalten der Bürger zu untersuchen: Stimmt die „gefühlte“ und gesagte Bedrohung damit überein, dass sich die Bürger aus bestimmten Zonen zurückziehen oder sich von bestimmten Praktiken abhalten lassen? Die lebensweltliche Relevanz ist auch ein Indikator für die gesellschaftliche Relevanz des Themas – und eine Maßgabe für die Herstellung einer politischen Kultur des Umgangs mit Sicherheitsfragen.

Dabei haben Studien zur Akzeptanz von Sicherheitstechnologien – etwa am Beispiel des digitalen Fingerabdrucks – gezeigt, dass politische Einstellungen und tatsächliches Verhalten, also die tatsächliche Nutzung einer Technologie, wiederum nicht einfach auf einen Nenner zu bringen sind. Die Frage, ob man sich beispielsweise für die Aufnahme des Fingerabdrucks in den Personalausweis entscheidet, hängt vielmehr nicht unerheblich von situativen Faktoren (der Interaktion mit Behördenmitarbeitern, praktischen Anforderungen der Antragstellung usw.) ab. Auch muss eine kritische Einschätzung der Technik oder der Sicherheitspolitik insgesamt keineswegs zu einer direkten Ablehnung der Nutzung führen. Ebenso sagt auch der Informationsstand über die rechtlichen und technischen Möglichkeiten der Technologie noch wenig über die Entscheidung bzw. das Verhalten selbst aus. Umgekehrt bedeutet die Nutzung einer Technologie keineswegs, dass man sie akzeptiert. Die Bürger zeigen sich durchaus als mündig und haben eigene Vorstellungen von und Ansprüche an Privatheit, Datenschutz und Rechtssicherheit. Technische Prozesse müssen dafür nicht vollständig durchschaut werden. Auch sind die Bürger durchaus nicht so verunsichert, wie Politik und auch die Wissenschaft das offenbar manchmal gern hätten. Vielmehr erweist sich das vielfach in den Vordergrund gestellte „Bedürfnis nach Sicherheit“ als eine Frage des Vertrauens in die Politik.

Gesellschaftspolitisch geboten ist daher zuallererst die Förderung bzw. Unterstützung einer demokratischen Kultur, die rechtliche und politische (Selbst-)Kontrollmechanismen im Feld der Sicherheit einschließt. Die Sicherheitspolitik seit den Terroranschlägen vom 11. September 2001 lässt hier zu wünschen übrig. So muss das Argument der notwendigen Geheimhaltung allzu oft dafür herhalten, dass der Sinn und Nutzen von Sicherheitsmaßnahmen und -strategien obskur bleibt.

Zu einer funktionierenden politischen Kultur gehören zivilgesellschaftliche Kräfte. Diese zu stärken und im Sinne einer Kultur der Resilienz die Handlungs- und Widerstandsfähigkeit der Bevölkerung zu fördern, ist für sich genommen zu begrüßen. Allerdings ist eine zentrale Voraussetzung auch hier, dass Erwartungen und Probleme behördlicherseits klar kommuniziert werden müssen.



Und Resilienz kann kein staatliches Ausstiegsprogramm aus der Sicherheitsversorgung sein. Die Frage ist allerdings, was Sicherheit überhaupt bedeutet.

Grundsätzlich sind die Bürger nur begrenzt dafür verantwortlich, für ihre Sicherheit selbst zu sorgen. Aufgabe des Staates ist es nach wie vor, seine Bürger zu schützen, auch vor staatlichen Übergriffen und Kontrollambitionen im Namen der Sicherheit. Dies heißt zuallererst, entsprechende gesetzliche Regelungen zu treffen und dafür Sorge zu tragen, dass diese auch durchgesetzt werden können. Dazu gehört ferner, demokratische Kontrollmechanismen in der Sicherheitsgesetzgebung zuzulassen und z.B. geeignete strukturelle Voraussetzungen für Evaluationsverfahren zu schaffen. Sicherheitsgesetze müssen auch wieder zurückgenommen werden können. Vom Versprechen absoluter Sicherheit oder der Sicherheit als einem Grundrecht schließlich gilt es Abschied zu nehmen. Dies täuscht vor, dass der Staat seinen Bürgern Sicherheit garantieren kann, und es täuscht darüber hinweg, dass wir auf diese Weise selbst eine Gesellschaft der Kontrolle und der Kultur des Verdachts kreieren. Das „Bedürfnis nach Sicherheit“ lässt sich auch anders ansprechen: Eine politische Gemeinschaft stellt sich auch über ihr Selbstverständnis als eine faire und mündige Gesellschaft her – und auch eine funktionierende demokratische Kultur schafft Sicherheit.



## Literatur

- Aas, K.F. (2004). From narrative to database. *Punishment & Society*, 6 (4), 379-393.
- Aas, K.F. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture*, 2 (2), 143-158.
- Aden, H. (2013). „Sichere“ versus „unsichere“ Ökonomie? Probleme und Kosten weltweiter und europäischer Terrorlisten. In D. Klimke & A. Legnaro (Hrsg.). *Politische Ökonomie und Sicherheit* (S. 260-285). Weinheim: Beltz Juventa.
- Al-Harby, F. (2010). Towards an understanding of user acceptance to use biometric authentication systems in e-commerce: using an extension of the Technology Acceptance Model. *International Journal of E-Business Research: an official publication of the Information Resources Management Association*, 6 (3), 34-55.
- Altheide, D.L. (2009). Moral panic: From sociological concept to public discourse. *Crime Media Culture*, 5 (1), 79-99.
- Ammicht Quinn, R. & Rampp, B. (2010). „It'll turn your heart black you can trust“: Angst, Sicherheit und Ethik. In T. Brück & H. Engerer (Hrsg.). *Ökonomie der Sicherheit* (S. 136-149). Vierteljahreshefte zur Wirtschaftsforschung 2009. Berlin: Duncker & Humblot.
- Amoore, L. (2008). Risk before Justice: When the Law Contests Its Own Suspension. *Leiden Journal of International Law*, 21 (4), 847-861.
- Amoore, L. & de Goede, M. (2008). Introduction. Governing by risk in the war on terror. In Dies. (Hrsg.). *Risk and the War on Terror* (S. 5-19). London: Routledge.
- Anderson, B. (2010). Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography*, 34 (6), 777- 798.
- Apell, S. & Lüders, H. (2011). Etikettenschwindel, Unschärfen und kreative Gesetzesanwendung. Eine kritische Lektüre des „Evaluationsberichts“ zum Terrorismusbekämpfungsergänzungsgesetz. In *Mitteilungen der Humanistischen Union*, 214 (3), 6-8.
- Apelt, M. & Möllers, N. (2011). Wie „intelligente“ Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung. *Zeitschrift für Außen- und Sicherheitspolitik* 4 (4), 585-593.
- Arbeitskreis Vorratsdatenspeicherung (2009). Antworten auf den Fragebogen der Europäischen Kommission vom 30.09.2009 zur Vorratsdatenspeicherung. Verfügbar unter [http://www.vorratsdatenspeicherung.de/images/antworten\\_kommission\\_vds\\_2009-11-13.pdf](http://www.vorratsdatenspeicherung.de/images/antworten_kommission_vds_2009-11-13.pdf) [17. September 2013]



- Arquilla, J. & Ronfeldt, D. (2001). *Networks and Netwars. The Future of Terror, Crime, and Militancy*. RAND Corporation. Verfügbar unter [http://www.rand.org/pubs/monograph\\_reports/MR1382.html](http://www.rand.org/pubs/monograph_reports/MR1382.html) [14. August 2013]
- Baccelli, E., Gerhold, L., Guettier, C., Schiller, J., Schmidt, T. C., Sella, G., Meissen, U., Voisard, A., Wählich, M. & Wittenburg, G. (2012). SAFEST: A Framework for Early Security Triggers in Public Spaces. In Proc. of WISG 2012 Workshop Interdisciplinaire sur la Securite Globale.
- Baier, A. (2001). Vertrauen und seine Grenzen. In M. Hartmann & C. Offe (Hrsg.). *Vertrauen. Die Grundlage des sozialen Zusammenhalts* (S. 37-84). Frankfurt/M.: Campus.
- Balzacq, T. (2011). *Securitization Theory: How Security Problems Emerge and Dissolve*. London: Routledge.
- Barak, G. (Hrsg.) (1994). *Media, Process and the Social Construction of Crime*. New York: Garland.
- Barben, D. (2010). Analyzing Acceptance Politics: Towards an Epistemological Shift in the Public Understanding of Science and Technology. *Public Understanding of Science*, 19 (3), 274-292.
- Barber, B. (1995). *Jihad vs. McWorld*. New York: Ballantine Books.
- Bauman, Z. (1992). *Moderne und Ambivalenz. Das Ende der Eindeutigkeit*. Hamburg: Junius.
- Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt/M.: Suhrkamp.
- Beckett, K. (1997). *Making Crime Pay. Law and Order in Contemporary American Politics*. New York: Oxford University Press.
- Beestermöller, G. & Brunkhorst, H. (Hrsg.). (2006). *Rückkehr der Folter. Der Rechtsstaat im Zwielflicht?* München: Beck.
- Bellanova, R. & Fuster, G.G. (2013). Politics of Disappearance: Scanners and (unobserved) Bodies as Mediators of Security Practices. *International Political Sociology*, 7 (2), 188-209.
- Bidlo, O. (2011). Von Leserreportern und Kontrolleuren. In O. Bidlo, C. J. Englert & J. Reichertz (Hrsg.). *Securitainment. Medien als Akteure der Inneren Sicherheit* (S. 111-134). Wiesbaden: VS.



- Bidlo, O., Englert, C.J. & Reichertz, J. (Hrsg.) (2011). *Securitainment. Medien als Akteure der Inneren Sicherheit*. Wiesbaden: VS.
- Bidlo, O., Englert, C.J. & Reichertz, J. (Hrsg.) (2012). *Tat-Ort Medien. Medien – Kultur – Kommunikation*. Wiesbaden: VS.
- Billig, M. (1995). *Banal Nationalism*. London: Sage.
- Blair, A.J. (2004). The Rhetoric of Visual Arguments. In C. A. Hill & M. Helmers (Hrsg.). *Defining Visual Rhetorics* (S. 41-61). London: Lawrence Erlbaum Associates.
- Böckenförde, E.-W. (2006). Bleibt die Menschenwürde unantastbar? In *Recht, Staat, Freiheit. Studien zur Rechtsphilosophie, Staatstheorie und Verfassungsgeschichte. Erweiterte Ausgabe* (S. 408-419). Frankfurt/M.: Suhrkamp.
- Bonß, W. (2010). (Un-)Sicherheit als Problem der Moderne. In H. Münkler, M. Bohlander & S. Meurer (Hrsg.). *Handeln unter Risiko. Gestaltungsansätze zwischen Wagnis und Vorsorgen* (S. 33-63). Bielefeld: transcript.
- Bott, K. & Koch-Arzberger, C. (2012). Der Faktor Furcht: Auswirkungen der islamistischen Terrorgefahr. Befunde einer repräsentativen Studie in Hessen. *Monatschrift für Kriminologie und Strafrechtsreform*, 95 (2), 132-141.
- Bonß, W. & Wagner, K. (2012). Risiken und symbolische Politik: Anmerkungen zu einem Konzept und seiner Bedeutung für die Luftsicherheit. In L. Gerhold & J. Schiller (Hrsg.). *Perspektiven der Sicherheitsforschung. Beiträge aus dem Forschungsforum Öffentliche Sicherheit* (S. 41-53). Berlin: Peter Lang.
- Bourke, J. (2006). *Fear. A Cultural History*. London: Virago.
- Britz, G. (2008). Vertraulichkeit und Integrität informationstechnischer Systeme. Einige Fragen zu einem neuen Grundrecht. *Die Öffentliche Verwaltung*, 61 (10), 411-415.
- Bröckling, U. (2012). Dispositive der Vorbeugung. Gefahrenabwehr, Resilienz, Vorbeugung. In C. Daase, P. Offermann & V. Rauer (Hrsg.). *Sicherheitskultur – Soziale und politische Praktiken der Gefahrenabwehr*. (S. 93-108). Frankfurt/M.: Campus.
- Bronner, S. & Schott, H.J. (2012). Die Gewalt der Zeichen. Terrorismus als symbolisches Phänomen. Einführung. In Dies. (Hrsg.). *Die Gewalt der Zeichen. Terrorismus als symbolisches Phänomen* (Bamberger Studien zu Literatur, Kultur und Medien) (S. 7-46). Bamberg: Bamberg University Press.
- Bug, M. & Münch, U. (2012). Politik verändert Internet (und Medien) – Innere Sicherheit, Vorratsdatenspeicherung und die Wahrnehmung durch die Bevölkerung. In M. Schröder (Hrsg.). *Die Web-Revolution. Das Internet verändert Politik und Medien* (S. 147-174). München: Olzog.



Bug, M. & Wagner, K. (2013). Der digitalisierte Passagier. In S. Humer (Hrsg.). *Terrorismus A/D: Wechselwirkungen zwischen analoger und digitaler Sphäre*. Reihe Digitale Wissenschaft. Winnenden: CWS Verlag [im Erscheinen].

Bulmahn, T. (2010). *Sicherheits- und verteidigungspolitisches Meinungsklima in Deutschland. Ergebnisse der Bevölkerungsbefragung Oktober/November 2009. Kurzbericht*. Strausberg: Sozialwissenschaftliches Institut der Bundeswehr.

Bulmahn, T. (2011). Bedrohungswahrnehmung und Sicherheitsgefühl. In T. Bulmahn, R. Fiebig & C. Hilpert (Hrsg.). *Sicherheits- und verteidigungspolitisches Meinungsklima in der Bundesrepublik Deutschland. Ergebnisse der Bevölkerungsbefragung 2010 des Sozialwissenschaftlichen Instituts der Bundeswehr* (S. 91-97). Strausberg: Sozialwissenschaftliches Institut der Bundeswehr.

Bulmahn, T., Fiebig, R. & Hilpert, C. (Hrsg.) (2011). *Sicherheits- und verteidigungspolitisches Meinungsklima in der Bundesrepublik Deutschland. Ergebnisse der Bevölkerungsbefragung 2010 des Sozialwissenschaftlichen Instituts der Bundeswehr*. Strausberg: Sozialwissenschaftliches Institut der Bundeswehr.

Bundesministerium des Inneren (BMI) (2009). *Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie)*. Verfügbar unter [http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile) [15. Mai 2012]

Bundesministerium für Bildung und Forschung (BMBF) (2012). *Forschung für die zivile Sicherheit 2012-2017: Rahmenprogramm der Bundesregierung*, Bonn. Verfügbar unter [http://www.bmbf.de/pub/rahmenprogramm\\_sicherheitsforschung\\_2012.pdf](http://www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf) [15. Mai 2012]

Burgess, J.P. (2011). *The Ethical Subject of Security: Geopolitical Rationality and the Threat against Europe* (PRIO New Security Studies). London: Routledge.

Burri, R.V. (2008). *Doing Images. Zur Praxis medizinischer Bilder*. Bielefeld: transcript.

Busch, H. (2006). Kontrollwahn ohne Sinn und Verstand. Jedermann wird erkenntnisdienlich behandelt! In T. Müller-Heidelberg, U. Finckh, E. Steven, J. Kühn, J. Micksch, W. Kaleck, M. Kutscha, R. Gössner & F. Schreiber (Hrsg.). *Grundrechte-Report 2006. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 29-32). Frankfurt/M.: Fischer.

Busch, H. (2012). Terrorismusbekämpfungsergänzungsverlängerungsgesetz. In T. Müller-Heidelberg, U. Finckh, E. Steven, M. Pelzer, M. Heimig, M. Kutscha, R. Gössner, U. Engelfried & M. Küster (Hrsg.). *Grundrechte-Report 2012. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 21-24). Frankfurt/M.: Fischer.



- Büsching, S. (2010). *Rechtsstaat und Terrorismus. Untersuchung der sicherheitspolitischen Reaktionen der USA, Deutschlands und Großbritanniens auf den internationalen Terrorismus*. Berlin: Peter Lang.
- Buzan, B., Wæver, O. & de Wilde, J. (1998). *Security. A New Framework For Analysis*. Boulder/Col.: Lynne Rienner.
- Campbell, A. (2010). Imagining the war on terror. Fiction, film and framing. In K. Hayward & M. Presdee (Hrsg.). *Framing Crime. Cultural Criminology and the Image*. (S. 98-114). Oxon: Routledge.
- Castel, R. (1983). Von der Gefährlichkeit zum Risiko. In M.M. Wambach (Hrsg.). *Der Mensch als Risiko. Zur Logik von Prävention und Früherkennung* (S. 51-74). Frankfurt/M.: Suhrkamp.
- Chandler, D. (2013). Resilience and the Autotelic Subject: Toward a Critique of the Societalization of Security. *International Political Sociology*, 7 (2), 210–226.
- Chèroux, C. (2011). *Diplopie. Bildpolitik des 11. September*. Konstanz: University Press.
- Cohen, S. (1972/2002). *Folk Devils and Moral Panics. The Creation of Mods and Rockers*. London: Routledge.
- Cole, D. (2002). Enemy Alien. *Stanford Law Review*, 54 (5), 953-1004.
- Conze, W. (1984). Sicherheit, Schutz. In O. Brunner, W. Conze & R. Koselleck (Hrsg.). *Geschichtliche Grundbegriffe: Historisches Lexikon zur politisch-sozialen Sprache in Deutschland*, Band 5 (S. 831-862). Stuttgart: Klett-Cotta.
- Conze, W. (2005). Sicherheit als Kultur. Überlegungen zu einer modernen „Politikgeschichte“ in der Bundesrepublik Deutschland. *Vierteljahreshefte für Zeitgeschichte*, 53 (3), 357-380.
- Conze, W. (2012). Securitization. Gegenwartsdiagnose oder historischer Analyseansatz? *Geschichte und Gesellschaft*, 38 (3), 453-467.
- Daase, C. (2009). Der erweiterte Sicherheitsbegriff. In M.A. Ferdowski (Hrsg.) *Internationale Politik als Überlebensstrategie* (S. 137-153). München: Bayerische Landeszentrale für politische Bildung.
- Daase, C. (2012). Sicherheitskultur als interdisziplinäres Forschungsprogramm. In Ders., P. Offermann & V. Rauer (Hrsg.). *Sicherheitskultur – Soziale und politische Praktiken der Gefahrenabwehr* (S. 23-44). Frankfurt/M.: Campus.





- Daase, C. & Deitelhoff, N. (2013). *Privatisierung der Sicherheit. Eine Sozialwissenschaftliche Expertise*. Berlin: Schriftenreihe Forschungsforum Öffentliche Sicherheit 11. Verfügbar unter [http://www.sicherheit-forschung.de/schriftenreihe/sr\\_v\\_v/sr\\_11.pdf](http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_11.pdf) [2. Oktober 2013]
- Daase, C., Offermann, P. & Rauer, V. (2012). Einleitung. In Dies. (Hrsg.). *Sicherheitskultur - Soziale und politische Praktiken der Gefahrenabwehr* (S. 7-19). Frankfurt/M.: Campus.
- de Goede, M. (2012). *Speculative security: The politics of pursuing terrorist monies*. Minneapolis: University of Minnesota Press.
- Dean, M. (1998). Risk, Calculable and Incalculable. *Soziale Welt*, 49 (1), 25-42.
- Denninger, E. (2008). Prävention und Freiheit. Von der Ordnung der Freiheit. In S. Huster & K. Rudolph (Hrsg.). *Vom Rechtsstaat zum Präventionsstaat* (S. 85-106). Frankfurt/M.: Suhrkamp.
- Denninger, E. (2009). Neues Computergrundrecht? Das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung. In T. Müller-Heidelberg, U. Finckh, E. Steven, M. Assall, A. Würdinger, M. Kutscha, R. Gössner, & U. Engelfried (Hrsg.). *Grundrechte-Report 2009. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 20-26). Frankfurt/M.: Fischer.
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2003). *Tätigkeitsbericht 2001-2002. 19. Tätigkeitsbericht*. Verfügbar unter [http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB\\_BfDI/19TB\\_2001\\_02.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/19TB_2001_02.pdf?__blob=publicationFile) [1. Oktober 2013]
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2009). *Tätigkeitsbericht 2007-2008. 22. Tätigkeitsbericht*. Verfügbar unter [http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB\\_BfDI/22TB\\_2007\\_2008.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/22TB_2007_2008.pdf?__blob=publicationFile) [1. Oktober 2013]
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2011). *Tätigkeitsbericht 2009-2010. 23. Tätigkeitsbericht*. Verfügbar unter [http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB\\_BfDI/23\\_TB\\_09\\_10.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile) [2. September 2013]
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2013). *Tätigkeitsbericht 2011-2012. 24. Tätigkeitsbericht*. Verfügbar unter [http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB\\_BfDI/24TB\\_2011\\_2012.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_2011_2012.pdf?__blob=publicationFile) [2. September 2013]
- Der Derian, J. (2005). Imaging Terror: Logos, Pathos and Ethos. *Third World Quarterly*, 26 (1), 23-37.



- Derrida, J. (2006). Autoimmunisierung, wirkliche und symbolische Selbstmorde (S. 117-178). In J. Habermas & J. Derrida: *Philosophie in Zeiten des Terrors*. Zwei Gespräche, geführt, eingeleitet und kommentiert von Giovanna Borradori. Hamburg: EVA.
- Deutsche Telekom & T-Systems (Hrsg.) (2011). *Sicherheitsreport 2011. Eine repräsentative Studie zum Thema Sicherheit in Deutschland im Auftrag von T-Systems*. Verfügbar unter [http://www.ifd-allensbach.de/uploads/tx\\_studies/7660\\_Sicherheitsreport2011\\_01.pdf](http://www.ifd-allensbach.de/uploads/tx_studies/7660_Sicherheitsreport2011_01.pdf) [26. August 2013]
- Dewey, J. (1993). *Demokratie und Erziehung: Eine Einleitung in die philosophische Pädagogik*. Weinheim: Beltz.
- Drechsel, B. (2005). *Politik im Bild. Wie politische Bilder entstehen und wie digitale Bildarchive arbeiten*. Frankfurt: Campus.
- Dzudzek, I., Kunze, K. & Wullweber, J. (Hrsg.) (2012). *Diskurs und Hegemonie. Gesellschaftskritische Perspektiven*. Bielefeld: transcript.
- Eckert, J. (2007). Zivilgesellschaft und Friedensstaatlichkeit: Herausforderungen der neuen Sicherheitspolitik. In D. Graulich & D. Simon (Hrsg.). *Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Perspektiven* (S. 335-343). Berlin: Akademie.
- Eisenstadt, S. (2001). Vertrauen, kollektive Identität und Demokratie. In M. Hartmann & C. Offe (Hrsg.). *Vertrauen. Die Grundlage des sozialen Zusammenhalts* (S. 333-363). Frankfurt/M.: Campus.
- Ellis, D. (2011). Islamophobia and Ontological Insecurity: The Impacts of Impersonal Trust upon Interpersonal Trust. *Research and Practice in Social Sciences* 7 (1), 1-16.
- Elster J. (1985). *Sour Grapes, Studies in the subversion of rationality*. Cambridge: Cambridge University Press.
- Endreß, M. & Rampp, B. (2013). Vertrauen in der Sicherheitsgesellschaft. In *Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin* 116 (S. 145-160). Verfügbar unter [http://leibnizsozietat.de/wp-content/uploads/2013/06/13\\_endressrampp.pdf](http://leibnizsozietat.de/wp-content/uploads/2013/06/13_endressrampp.pdf) [22. August 2013]
- Endreß, M. (2012). Vertrauen und Misstrauen – Soziologische Überlegungen. In C. Schilcher, M. Will-Zocholl & M. Ziegler (Hrsg.). *Vertrauen und Kooperation in der Arbeitswelt* (S. 81-102). Wiesbaden: VS.
- Ericson, R.V. & Haggerty, K.D. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.



- Ernst, A. (2008). Zwischen Risikowahrnehmung und Komplexität: Über die Schwierigkeiten und Möglichkeiten kompetenten Handelns im Umweltbereich. In I. Bormann & G. de Haan. (Hrsg.). *Kompetenzen der Bildung für nachhaltige Entwicklung. Operationalisierung, Messung, Rahmenbedingungen, Befunde.* (S. 45-59). Wiesbaden: VS.
- Esposito, E. (1998). Fiktion und Virtualität. In S. Krämer (Hrsg.). *Medien – Computer – Realität* (S. 269-296). Frankfurt/M.: Suhrkamp.
- Esposito, E. (2007). *Die Fiktion der wahrscheinlichen Realität.* Frankfurt/M.: Suhrkamp.
- Europäische Kommission (2007a). *Soziale Wirklichkeit in Europa. Eurobarometer Spezial 273. Bericht.* Verfügbar unter [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_273\\_de.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_273_de.pdf) [26. August 2013]
- Europäische Kommission (2011). *Internal Security. Special Eurobarometer 371. Report.* Verfügbar unter [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_371\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf) [05. Oktober 2013]
- Ewald, F. (1993). *Der Vorsorgestaat.* Frankfurt/M.: Suhrkamp.
- Ewald, F. (1998). Die Rückkehr des *genius malignus*: Entwurf zu einer Philosophie der Vorbeugung. *Soziale Welt*, 49 (1), 5-23.
- Felgentreff, C., Kuhlicke, C. & Westholt, F. (2012). *Naturereignisse und Sozialkatastrophen.* Forschungsforum öffentliche Sicherheit. Schriftenreihe Sicherheit Nr. 8. Verfügbar unter [http://www.sicherheit-forschung.de/schriftenreihe/sr\\_v\\_v/sr\\_8.pdf](http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_8.pdf) [28. August 2013]
- Feltes, T., Kudlacek, D. & Ruch, A. (2013). *Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel).* Bochum: Ruhr-Universität Bochum.
- Fiebig, R. & Pietsch, C. (2010). Bundeswehr im Einsatz: Erweitertes Aufgabenspektrum und dessen Wahrnehmung im Spiegel der öffentlichen Meinung. *Sicherheit und Frieden* 28 (2), 95-103.
- Foucault, M. (1974). *Die Ordnung der Dinge. Eine Archäologie der Humanwissenschaften.* Frankfurt/M.: Suhrkamp.
- Foucault, M. (2004). *Geschichte der Gouvernementalität I: Sicherheit, Territorium, Bevölkerung. Vorlesung am Collège de France 1977-1978* (Herausgegeben von Michel Senellart). Frankfurt/M.: Suhrkamp.



Fox, N.J. (1999). Postmodern reflections on “risk”, “hazards” and life choices. In D. Lupton (Hrsg.). *Risk and sociocultural theory: new directions and perspectives* (S. 12-33). Cambridge: Cambridge University Press.

Frankenberg, G. (2005). Kritik des Bekämpfungsrechts. *Kritische Justiz*, 38 (4), 370-386.

Frankenberg, G. (2006). Nochmals: Angst im Rechtsstaat. *WestEnd. Neue Zeitschrift für Sozialforschung*, 3 (2), 55-63.

Frankenberg, G. (2010). *Staatstechnik. Perspektiven auf Rechtsstaat und Ausnahmezustand*. Berlin: Suhrkamp.

Frindte, W. & Haußecker, N. (Hrsg.) (2010). *Inszenierter Terrorismus. Mediale Konstruktionen und individuelle Interpretationen*. Wiesbaden: VS.

Fuhse, J.A. (2002). Kann ich dir vertrauen? Strukturbildung in dyadischen Sozialbeziehungen. *Österreichische Zeitschrift für Politikwissenschaft*, 31 (4), 413-426.

Galloway, A.R. & Thacker, E. (2007). *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.

Garland, D. (2008a). *Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart*. Frankfurt/M.: Campus.

Garland, D. (2008b). On the Concept of Moral Panic. *Crime Media Culture*, 4 (1), 9-30.

Garland, D. (2010). *Peculiar Institution. America's Death Penalty in an Age of Abolition*. Cambridge: The Belknap Press of Harvard University Press.

Gaycken, S. (2013): Freiheit und Sicherheit in der fortgeschrittenen Informationsgesellschaft. In Ders. (Hrsg.). *Jenseits von 1984. Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Eine Versachlichung* (S. 15-26). Bielefeld: transcript.

Gerhards, J., Schäfer, M., Al-Jabiri, I. & Seifert, J. (2011). *Terrorismus im Fernsehen. Formate, Inhalte und Emotionen in westlichen und arabischen Sendern*. Wiesbaden: VS.

Gerhold, L. (2009). *Umgang mit makrosozialer Unsicherheit. Zur Wahrnehmung und Bewältigung gesellschaftlich-politischer Phänomene*. Lengerich: Pabst Science Publishers.

Gericke, C. (2011). Bis auf weiteres unbestimmt. Strafbarkeit von vermeintlichen Verstößen gegen »EU-Terrorliste«. In T. Müller-Heidelberg, U. Finckh, E. Steven, M.



Pelzer, M. Heiming, M. Kutscha, R. Gössner, U. Engelfried & P. Hase (Hrsg.): *Grundrechte-Report 2011. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 159-163). Frankfurt/M.: Fischer.

Ghamari-Tabrizi, S. (2005). *The Worlds of Herman Kahn: The Intuitive Arts of Thermonuclear War*. Cambridge/Mass.: Harvard University Press.

Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford: Stanford University Press.

Giddens, A. (1996). *Konsequenzen der Moderne*. Frankfurt/M.: Suhrkamp.

Glaeßner, G.-J. (2010). Die Innen- und Rechtspolitik der Großen Koalition. In S. Bukow & W. Seemann (Hrsg.). *Die Große Koalition. Regierung – Politik – Parteien 2005-2009* (S. 174-190). Wiesbaden: VS.

Goersch, H. & Werner, U. (2011). *Empirische Untersuchung der Realisierbarkeit von Maßnahmen zur Erhöhung der Selbstschutzzfähigkeit der Bevölkerung*, Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Goold, B. (2009). Technologies of surveillance and the erosion of institutional trust. In K.F. Aas, H. Oppen Gundhus & H. Mork Lomell (Hrsg.). *Technologies of Insecurity: The Surveillance of Everyday Life* (S. 207-218). New York: Routledge-Cavendish.

Goold, B.J. & Lazarus, L. (2007). *Introduction. Security and Human Rights: The Search for a Language of Reconciliation* (S. 1-24). In Dies. (Hrsg.). *Security and Human Rights*, Oxford: Hart.

Gössner, R. (2002). Kollateralschäden an der "Heimatfront". *Ossietsky. Zweiwochenschrift für Politik/Kultur/Wirtschaft 2*. Verfügbar unter <http://www.sopos.org/aufsaeetze/3c764f6821a7e/1.phtml> [10. September 2013]

Gössner, R. (2007). *Menschenrechte in Zeiten des Terrors*. Hamburg: Konkret.

Grahek, N. (2001). *Feeling Pain and Being in Pain*. Oldenburg: BIS.

Grimm, D. (Hrsg.) (1996). *Staatsaufgaben*. Frankfurt/M.: Suhrkamp.

Grusin, R. (2004). Premediation. *Criticism*, 46 (1), 17-39.

Gusy, C. (2004). Geheimdienstliche Aufklärung und Grundrechtsschutz. *Aus Politik und Zeitgeschichte*, B44. Verfügbar unter <http://www.bpb.de/apuz/28018/geheimdienstliche-aufklaerung-und-grundrechtsschutz?p=all> [14. September 2013]

Gusy, C. (2007). Präventionsstaat zwischen Rechtsgüterschutz und Abbau von Freiheitsrechten in Deutschland. In K. Graulich & D. Simon (Hrsg.). *Terrorismus und*



*Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Perspektiven* (S. 273-294). Berlin: Akademie.

Gusy, C. (2010). Sicherheitskultur – Sicherheitspolitik – Sicherheitsrecht. *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, 93 (2), 111-128.

Gusy, C. (2012). Vom „Neuen Sicherheitsbegriff“ zur „Neuen Sicherheitsarchitektur“. In T. Würtenberger, C. Gusy & H.-J. Lange (Hrsg.). *Innere Sicherheit im europäischen Vergleich. Sicherheitsdenken, Sicherheitskonzepte und Sicherheitsarchitektur im Wandel* (S. 71-106). Berlin: LIT.

Gusy, C. (2013). Vier Thesen: Resilienz der Gesellschaft oder resilient society? Verfügbar unter <http://www.sicherheitspolitik-blog.de/2013/05/21/resilienz-gusy/> [17. September 2013]

Haggerty, K.D. (2009). “Ten thousand times larger ...”: anticipating the expansion of surveillance. In B.D. Gougeon & D. Neyland (Hrsg.). *New Directions in Surveillance and Privacy* (S. 159-177). Cullompton: Willan.

Hall, S. (1989). Die strukturierte Vermittlung von Ereignissen. In N. Rätzsch (Hrsg.). *Stuart Hall. Ausgewählte Schriften. Ideologie, Kultur, Medien, Neue Rechte, Rassismus*. (S. 126-149) Hamburg: Argument.

Hall, S., Critcher, C., Jefferson, T., Clarke, J. & Roberts, B. (1978). *Policing the Crisis: Mugging, the State and Law and Order*. London: Macmillan.

Hartmann, M. (2011). *Die Praxis des Vertrauens*. Berlin: Suhrkamp.

Hartmann, M. (2013). Zerstörtes Vertrauen, zerstörte Freiheit. Die Folgen der Überwachung aus philosophischer Sicht. *Forschung und Lehre*, 20 (8), 622-624.

Hassemer, W. (2006) Sicherheit durch Strafrecht. In *HRRS. Onlinezeitschrift für Höchstgerichtliche Rechtsprechung im Strafrecht*, 7 (4), 130-143.

Haußecker, N. (2012). *Zur Inszenierung von Terrorismus in Fernsehnachrichten - visuelles Framing und emotionale Reaktionen*, Jena: unveröff. Dissertation an der Friedrich-Schiller-Universität Jena.

Haverkamp, R., Hummelsheim, D. & Armbrorst, A. (2013). Studien zur Sicherheit in Deutschland. In Max-Planck-Gesellschaft zur Förderung der Wissenschaften e. V. (Hrsg.): *Jahrbuch 2013 der Max-Planck-Gesellschaft*. München: MPG. Verfügbar unter [http://www.mpg.de/6841890/STRA\\_JB\\_2013?c=7291695](http://www.mpg.de/6841890/STRA_JB_2013?c=7291695) [26. August 2013]

Hentschel, L. (2008). Haupt oder Gesicht? Visuelle Gouvernementalität seit 9/11. In L. Hentschel (Hrsg.). *Bilderpolitik in Zeiten von Krieg und Terror. Medien, Macht und Geschlechterverhältnisse*. (S. 185-200). Berlin: b\_books.



- Herdegen, M. (2003). Artikel 1 GG. In: T. Maunz, G. Dürig & R. Herzog (Hrsg.). *Kommentar zum Grundgesetz*, 42. Aufl. München: Beck.
- Hirtenlehner, H. & Farrall, S. (2012). Modernisierungsängste, lokale Irritation und Furcht vor Kriminalität. Eine vergleichende Untersuchung zweier Denkmodelle. *Monatsschrift für Kriminologie und Strafrechtsreform*, 95 (2), 93-114.
- Hoffman, A.M., Jengelly, D.H.A., Duncan, N.T., Buehler, M. & Rees, M.L. (2010). How Does the Business of News Influence Terrorism Coverage? Evidence From The Washington Post and USA Today. *Terrorism and Political Violence*. 22 (4), 559-580.
- Hoffman, B. (2006). *Inside terrorism*. New York: Columbia University Press (Rev. and expanded edition).
- Holert, T. (2006). Smoking Gun. Über den Forensic Turn der Weltpolitik. In R.F. Nohr (Hrsg.). *Evidenz – „... das sieht man doch!“* (S. 20-39). Münster: Lit.
- Holert, T. (2008). Wie die Bilder zur Ordnung rufen. Geschlecht, Militär und Fotografie im ‚War on Terrorism‘. In L. Hentschel (Hrsg.). *Bilderpolitik in Zeiten von Krieg und Terror. Medien, Macht und Geschlechterverhältnisse* (S. 161-180). Berlin: b\_books.
- Horkheimer, M. & Adorno, T. W. (1971). *Dialektik der Aufklärung*. Frankfurt/M.: Fischer.
- Hough, M. & Roberts, J.V. (1999). Sentencing Trends in Britain. Public Knowledge and Public Opinion. *Punishment & Society*, 1 (1), 11-26.
- Howe, J. (2006). The Rise of Crowdsourcing. *Wired Magazine*, 14. Verfügbar unter [http://www.wired.com/wired/archive/14.06/crowds\\_pr.html](http://www.wired.com/wired/archive/14.06/crowds_pr.html) [4. Oktober 2013]
- Huster, S. & Rudolph, K. (2008). Vom Rechtsstaat zum Präventionsstaat? In Dies. (Hrsg.). *Vom Rechtsstaat zum Präventionsstaat* (S. 9-22). Frankfurt/M.: Suhrkamp.
- International Helsinki Federation for Human Rights (2005). *Intolerance and Discrimination against Muslims in the EU*. Verfügbar unter <http://www.art1.nl/nprd/factsheets/Intolerance%20against%20muslims%20in%20the%20EU%2003-2005.pdf> [12. September 2013]
- Jasanoff, S. (1991). Acceptable evidence in pluralistic society. In D.G. Mayo & R.D. Hollander (Hrsg.). *Acceptable evidence: Science and values in risk management* (S. 29-47). Oxford: Oxford University Press.
- Jenkins, P. (2003). *Images of Terror. What we can and can't know about terrorism*. Hawthorne: Aldine de Gruyter.



Juergensmeyer, M. (2004). *Terror im Namen Gottes. Ein Blick hinter die Kulissen des gewalttätigen Fundamentalismus*. Freiburg: Herder.

Junge, M. (2003). Die Deutungen des 11. September in ausgewählten Tageszeitungen. In R. Hitzler & J. Reichertz (Hrsg.). *Irritierte Ordnung. Die gesellschaftliche Verarbeitung von Terror*. (S. 125-138). Konstanz: UVK.

Kahn, P.W. (2013). Imagining Warfare. *The European Journal of International Law*, 24 (1), 199-226.

Kaufmann, F.-X. (2003). Sicherheit: Das Leitbild beherrschbarer Komplexität. In St. Lessenich (Hrsg.). *Wohlfahrtsstaatliche Grundbegriffe. Historische und aktuelle Diskurse* (S. 73-104). Frankfurt/M.: Campus.

Kaufmann, F.-X. (2012). *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Münster: Lit.

Kaufmann, S. (2011). Zivile Sicherheit: Vom Aufstieg eines Topos. In L. Hempel, S. Krasmann & U. Bröckling (Hrsg.). *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert (Leviathan Sonderheft 25/2010)* (S. 101-123). Wiesbaden: VS.

Kersten, J. (2009). Medien und Innere Sicherheit. In H.-J. Lange, H.P. Ohly & J. Reichertz (Hrsg.). *Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen*. (S. 293-305). Wiesbaden: VS.

Kessler, O. & Werner, W. (2008). Extrajudicial Killing as Risk Management. *Security Dialogue*, 39 (2-3), 289-308.

Kingdon, J.W. (1995). The Policy Window, and Joining the Streams. In J.W. Kingdon (Hrsg.). *Agendas, Alternatives and Public Policies* (S. 165-195). New York: Little, Brown and Company.

Kirchhoff, S. (2010). *Krieg mit Metaphern. Mediendiskurse über 9/11 und den "War on Terror"*. Bielefeld: transcript.

Kleinstauber, H.J. (2003): Terrorismus und Feindbilder. Zur visuellen Konstruktion von Feinden am Beispiel Osama Bin Laden und Saddam Hussein. In M. Beuthner, J. Buttler, S. Fröhlich, I. Neverla & S. Weichert (Hrsg.). *Bilder des Terrors – Terror der Bilder. Krisenberichterstattung am und nach dem 11. September*. (S. 206-237) Köln: Herbert von Halem.

Koep-Kerstin, W. & Will, R. (2009). Der 11. September 2001 und seine Folgen. In Gustav-Heinemann-Initiative & Humanistische Union (Hrsg.). *Graubuch Innere Sicherheit. Die schleichende Demontage des Rechtsstaates nach dem 11. September*





2001 (S. 5-11). Norderstedt: Books on Demand.

Koselleck, R. (1982). Krise. In O. Brunner, W. Conze & R. Koselleck (Hrsg.). *Geschichtliche Grundbegriffe: Historisches Lexikon zur politisch-sozialen Sprache in Deutschland*, Band 3 (S. 617-650). Stuttgart: Klett-Cotta.

Krämer, S. (2011). Der Bote als Topos oder: Übertragung als eine medientheoretische Grundkonstellation. In: T. Hellmann, A. von der Heiden & A. Tuschling (Hrsg.). *medias in res. Medienkulturwissenschaftliche Positionen* (S. 53-68). Bielefeld: transcript.

Krasmann, S. (2012a). Targeted Killing and Its Law. On a Mutually Constitutive Relationship. *Leiden Journal of International Law*, 25 (3), 665-682.

Krasmann, S. (2012b). Law's knowledge. On the susceptibility and resistance of legal practices to security matters. *Theoretical Criminology*, 16 (4), 379-394.

Krasmann, S. & Kühne, S. (2013). Big Data und Big Brother – was, wenn sie sich treffen? Über die vernachlässigte politische Dimension von Kontroll- und Überwachungstechnologien in der Akzeptanzforschung. *Kriminologisches Journal* [im Erscheinen].

Krasmann, S. & Kühne, S. (2014). "My fingerprint on Osama's cup." On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society* [im Erscheinen].

Kreissl, R. (2008). Öffentliche Inszenierung von Sicherheitsfragen. *Kritische Vierteljahrsschrift für Gesetzgebung und Rechtswissenschaft*, 94 (3), 322-332.

Kühne, S. & Schlepper, C. (2013). Die biometrische *Verheißung* – Zur Politischen Ökonomie der Versprechen. Unv. MS.

Kühne, S. & Wehrheim, J. (2013). Versicherheitlichung und Biometrie. Zur Verbreitung einer Kontrolltechnologie im Spannungsfeld von Staat, Ökonomie und Alltag. In D. Klimke & A. Legnaro (Hrsg.). *Politische Ökonomie und Sicherheit* (S. 303-318). Weinheim: Beltz Juventa.

Kuntze, M. (2003). Vision vom Endkampf zwischen Gut und Böse. Freund- und Feindbilder während der Krise am Beispiel von FAZ und NZZ. In M. Beuthner, J. Buttler, S. Fröhlich, I. Neverla & S. Weichert (Hrsg.). *Bilder des Terrors – Terror der Bilder. Krisenberichterstattung am und nach dem 11. September*. (S. 238-267) Köln: Herbert von Halem.

Kurz, C. (2008). Biometrie nicht nur an den Grenzen. Erkennungsdienstliche Behandlung für jedermann. In S. Gaycken & C. Kurz (Hrsg.). *1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien* (S. 101-113). Bielefeld: transcript.



- Kutscha, M. (2008). Mehr Schutz von Computerdaten durch ein neues Grundrecht? *Neue Juristische Wochenschrift*, 61 (15), 1042-1044.
- Lakoff, A. (2006). Techniques of Preparedness. In T. Monahan (Hrsg.). *Surveillance and Security: Technological Politics and Power in Everyday Life* (S. 265-273). New York: Routledge.
- Lange, H.-J. (2006). Innere Sicherheit und der Wandel von Staatlichkeit. In M.G. Schmidt, R. Zohlnhöfer (Hrsg.). *Regieren in der Bundesrepublik Deutschland. Innen- und Außenpolitik seit 1949* (S. 87-112). Wiesbaden: VS.
- Lange, H.-J. (2008). Der Wandel des föderalen Sicherheitsverbundes. In S. Huster & K. Rudolph (Hrsg.). *Vom Rechtsstaat zum Präventionsstaat* (S. 64-81). Frankfurt/M.: Suhrkamp.
- Law, J. (2009). Seeing Like a Survey. *Cultural Sociology*, 3 (2), 239-256.
- Leese, M. (2013). The Perceived Threat. Determinants and Consequences of Fear of Terrorism in Germany. In F. Flammini, R. Setola & G. Franceschetti (Hrsg.). *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues* (S.71-85). Boca Raton: CRC Press.
- Lentzos, F. & Rose, N. (2008). Die Unsicherheit regieren. Biologische Bedrohungen, Notfallplanung, Schutz und Resilienz in Europa. In P. Purtschert, K. Meyer & Y. Winter (Hrsg.). *Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault* (S. 75-201). Bielefeld: transcript.
- Leopold, N. (2011). Das neue SWIFT-Abkommen – kein Ruhmesblatt für den transatlantischen Datenschutz. In T. Müller-Heidelberg, U. Finckh, E. Steven, M. Pelzer, M. Heiming, M. Kutscha, R. Gössner, U. Engelfried & P. Hase (Hrsg.): *Grundrechte-Report 2011. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 41-46). Frankfurt/M.: Fischer.
- Lepsius, O. (2004). Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland. *Leviathan* 32 (1), 64-88.
- Lepsius, O. (2010). Sicherheit und Freiheit – ein zunehmend asymmetrisches Verhältnis. In G. F. Schuppert, W. Merkel, G. Nolte & M. Zürn (Hrsg.). *Der Rechtsstaat unter Bewährungsdruck* (S. 23-54). Baden-Baden: Nomos.
- Lianos, M. & Douglas, M. (2000). Dangerization and the end of deviance: the institutional environment. *British Journal of Criminology*, 40 (2); reprinted in D. Garland & R. Sparks (Hrsg.). *Criminology and Social Theory*. (S. 261-278) Oxford: Oxford University Press.



- Loader, I. & Walker, N. (2007). *Civilizing Security*. Cambridge: Cambridge University Press.
- Locke, J. (1977). *Zwei Abhandlungen über die Regierung*. (Herausgegeben und eingeleitet von Walter Euchner). Frankfurt/M.: Suhrkamp.
- Lübcke, B. & Irlenkaeuser, J. C. (2006). *Bedrohungsperzeption durch das Phänomen des Terrorismus und Bewertung der Gegenmaßnahmen der BR Deutschland*. Kiel: Institut für Sicherheitspolitik.
- Lucke, D. (2010). Akzeptanz und Legitimation. In J. Kopp & B. Schäfers (Hrsg.). *Grundbegriffe der Soziologie* (S. 12-17). Wiesbaden: VS.
- Lüdemann, C. & Schlepper, C. (2011). Der überwachte Bürger zwischen Apathie und Protest. Eine empirische Studie zum Widerstand gegen staatliche Kontrolle. In N. Zurawski (Hrsg.). *Überwachungspraxen. Praktiken der Überwachung und Kontrolle* (S. 119-138). Opladen: Barbara Budrich.
- Lüdemann, C. & Schlepper, C. (2013). Angst im Überwachungsstaat. Eine empirische Studie zur Akzeptanz neuer staatlicher Überwachungsmaßnahmen. In S. Gaycken (Hrsg.). *Jenseits von 1984. Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft* (S. 147-162). Bielefeld: transcript.
- Luhmann, N. (1991). *Soziologie des Risikos*. Berlin: de Gruyter.
- Luhmann, N. (1993). Die Moral des Risikos und das Risiko der Moral. In G. Bechmann (Hrsg.). *Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung* (S. 327-338). Opladen: Westdeutscher Verlag.
- Luhmann, N. (2000). *Vertrauen*. Stuttgart: Lucius & Lucius.
- Lyon, D. (2007). *Surveillance Studies: An Overview*. London: Polity.
- Lyon, D. (2010). Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies. *International Political Sociology*, 4 (4), 325-338.
- Massumi, B. (2005). Fear (The Spectrum Said). *Positions*, 13 (1), 31-48.
- Massumi, B. (2007). Potential Politics and the Primacy of Preemption. *Theory & Event*, 10 (2). Verfügbar unter [http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/theory\\_and\\_event/v010/10.2massumi.html](http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/theory_and_event/v010/10.2massumi.html) [25. Mai 2010]
- Massumi, B. (2010). The Future Birth of the Affective Fact. In M. Gregg & G. J. Seigworth (Hrsg.). *The Affect Theory Reader* (S. 52-70). Durham: Duke University Press.



Mayer, J. (2013). Resilienz und Bevölkerungsschutz – eine Frage des Selbstschutzes?! Verfügbar unter <http://www.sicherheitspolitik-blog.de/2013/05/15/resilienz-mayer/> [17. September 2013]

Mersch, D. (2006). *Medientheorien. Zur Einführung*. Hamburg: Junius.

Möllering, G. (2006). Das Aufheben von Ungewissheit als Kern des Vertrauens: Just do it? *MPIfG Working Paper 06/5*, September 2006. Verfügbar unter <http://www.mpifg.de/pu/workpap/wp06-5/wp06-5.html> [14. August 2013]

Mordini, E. (2009). Ethics and Policy of Biometrics. In M. Tistarello, Z.L. Stan & R. Chellappa (Hrsg.). *Handbook of Remote Biometrics for Surveillance and Security* (S. 293-309). Dordrecht: Springer.

Müller, C. (2008). Sorgen um den globalen Terrorismus in Deutschland. *Wochenbericht des DIW Berlin*, 37, 544-548.

Münkler, H. (2010). Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven. In H. Münkler, M. Bohlender & S. Meurer (Hrsg.). *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert* (S. 11-34). Bielefeld: transcript.

Münkler, H. (2013). Aufklärungs- und Kampfdrohnen: Waffen zwischen Krieg und Frieden. Verfügbar unter <http://www.sicherheitspolitik-blog.de/2013/03/13/ethik-der-drohnen-muenkler/> [27. Juli.2013]

Murakami Wood, D.M. (2011). Vanishing Surveillance: Why Seeing What is Watching Us Matters. Verfügbar unter [http://www.priv.gc.ca/information/research-recherche/2011/wood\\_201107\\_e.asp](http://www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp) [16. Januar 2013]

Mythen, G. & Walklate, S. (2006). Communicating the terrorist risk: Harnessing a culture of fear? *Crime Media Culture*, 2 (2), 123-142.

Nacos, B. & Torres-Reyna, O. (2003). Framing Muslim-Americans Before and After 9/11. In P. Norris, M. Kern & M. Just (Hrsg.). *Framing Terrorism. The News Media, the Government, and the Public*. (S. 133-157). New York: Routledge.

Nacos, B. (2002). *Mass-Mediated Terrorism: The Central Role of The Media in Terrorism and Counterterrorism*. Lanham/MD: Rowman & Littlefield.

Nassehi, A. (2012). Der Ausnahmezustand als Normalfall. Modernität als Krise. *Kursbuch 170*, 34-49.

Neidhardt, F. (2006). Kalkül mit der Angst. Terrorismus, Medien und die Grenzen der Gelassenheit. *WZB-Mitteilungen*. 113, 10-13.



- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review* 79 (1), 101-139.
- Norris, P., Kern, M. & Just, M. (2003). Framing Terrorism. In Dies. (Hrsg.): *Framing Terrorism. The News Media, the Government, and the Public* (S. 3-23). New York: Routledge.
- O'Malley, P. (2004). *Risk, Uncertainty and Government*. London: Glasshouse.
- Oehmichen A. & Klukkert, A. (2012). *Evaluation des Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten. (GVVG). Endbericht*. Verfügbar unter [http://www.krimz.de/fileadmin/dateiablage/E-Publikationen/Endbericht\\_GVVG\\_Evaluierung.pdf](http://www.krimz.de/fileadmin/dateiablage/E-Publikationen/Endbericht_GVVG_Evaluierung.pdf) [26. August 2013]
- Opitz, S. & Tellmann, U. (2011). Katastrophische Szenarien: Gegenwärtige Zukunft in Recht und Ökonomie. In L. Hempel, S. Krasmann & U. Bröckling (Hrsg.). *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert (Leviathan Sonderheft 25/2010)* (S. 27-52). Wiesbaden: VS.
- Pato, J.N. & Millets, L.I. (2005). *Biometric Recognition. Challenges and Opportunities*. Washington: The National Washington Academies Press.
- Pietsch, C. & Fiebig, R. (2011). „Keine besondere Bedrohungslage“: Die Einstellungen deutschen Bevölkerung zu Maßnahmen der Terrorabwehr. In T. Jäger (Hrsg.) *Die Welt nach 9/11* (S. 261-284). Wiesbaden: VS.
- Pinch, T.J. & Bijker, W.E. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, 14 (3), 399-441.
- Prantl, H. (2002). *Verdächtig. Der starke Staat und die Politik der inneren Unsicherheit*. Hamburg: Europa Verlag.
- Puschke, J. (2010). Anti-Terrorcamp-Gesetzgebung. Die endgültige Abkehr von einem rechtsstaatlichen Bürgerstrafrecht. In T. Müller-Heidelberg, U. Finckh, E. Steven, M. Pelzer, A. Würdinger, M. Kutscha, R. Gössner & U. Engelfried (Hrsg.). *Grundrechte-Report 2010. Zur Lage der Bürger- und Menschenrechte in Deutschland* (S. 220-224). Frankfurt/M.: Fischer.
- Putnam, R.D. (1993). *Making Democracy Work. Civic Traditions in Modern Italy*. Princeton: Princeton University Press.
- Pütter, N. (2008). Sicherheitsarchitekturen im Wandel. Polizei – Geheimdienste – Militär. *Bürgerrechte & Polizei/CILIP*, 90 (2), 3-12.



- Pütter, N., Narr, W.-D. & Busch, H. (2005). Bekämpfungsrecht und Rechtsstaat. Vorwärtsverrechtlichung in gebremsten Bahnen? *Bürgerrechte & Polizei/CILIP*, 82 (3), 6-15.
- Radtke, H. & Steinsiek, M. (2010). Terrorismusbekämpfung durch Vorfeldkriminalisierung? – Das Gesetz zur Verfolgung der Vorbereitung schwerer staatsgefährdender Gewalttaten. *Juristische Rundschau*, 64 (3), 107-109.
- Rammert, W. (1999). Technik. Stichwort für eine Enzyklopädie. *Technical University Technology Studies: Working Papers*, 1-1999. Verfügbar unter <http://nbn-resolving.de/urn:nbn:de:0168-ssoar-8811> [20. April 2013]
- Rauer, V. (2012). Apokalyptische Verunsicherung. Zur Bedrohlichkeit des Ununterscheidbaren (Working Paper 11). Verfügbar unter <http://www.sicherheitskultur.org/WorkingPapers/11-Rauer.pdf> [12. Juli 2013]
- Reckwitz, A. (2003). Grundelemente einer Theorie sozialer Praktiken. *Zeitschrift für Soziologie*, 32 (4), 282-301.
- Reeves, J. (2012). If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. *Surveillance & Society*, 10 (3/4), 235-248.
- Reichertz, J. (2011): Die Medien als Akteure für mehr Innere Sicherheit. In O. Bidlo, C.J. Englert & J. Reichertz (Hrsg.). *Securitainment. Medien als Akteure der Inneren Sicherheit*. (S. 11-42). Wiesbaden: VS.
- Renn, O. (2005). Technikakzeptanz: Lehren und Rückschlüsse der Akzeptanzforschung für die Bewältigung des technischen Wandels. *Technikfolgenabschätzung – Theorie und Praxis* 14 (3), 29-38.
- Ross, J.I. (2007). Deconstructing the terrorism – news media relationship. *Crime Media Culture*, 3 (2), 215-225.
- Rothe, D. & Muzzatti, S.L. (2004). Enemies from Everywhere: Terrorism, Moral Panic, and US Civil Society. *Critical Criminology*, 12 (3), 327-350.
- Said, E. (1978). *Orientalism*. New York: Random House.
- Sarasin, P. (2004). *Anthrax. Bioterror als Phantasma*. Frankfurt/M.: Suhrkamp.
- Saurer, J. (2005). Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung. *Neue Zeitschrift für Verwaltungsrecht*, 24 (3), 275-282.
- Scarry, E. (1992). *Der Körper im Schmerz*. Frankfurt/M.: Fischer.
- Scarry, E. (2011). *Thinking in an emergency*. New York: W.W. Norton.



- Schaar, P. (2009). *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*. München: Bertelsmann.
- Schäuble, W. (2008). *Das Konzept der vernetzten Sicherheit*. Rede von Bundesminister Dr. Wolfgang Schäuble beim 7. Symposium des Bundesamtes für Verfassungsschutz am 8. Dezember 2008 in Berlin. Verfügbar unter <http://www.wolfgang-schaeuble.de/index.php?id=30&textid=1227&page=18> [26. August 2013]
- Scherr, A. (2010). Innere Sicherheit und soziale Unsicherheit. Sicherheitsdiskurse als projektive Bearbeitung gesellschaftsstrukturell bedingter Ängste. In A. Groenemeyer (Hrsg.): *Wege der Sicherheitsgesellschaft* (S. 23-39). Wiesbaden: VS.
- Schetsche, M. (2008). *Empirische Analyse sozialer Probleme. Das wissenssoziologische Programm*. Wiesbaden: VS.
- Scheufele, B. (2001). Visuelles Medien-Framing und Framing-Effekte. Zur Analyse visueller Kommunikation aus der Framing-Perspektive. In T. Knieper & M.G. Müller (Hrsg.). *Kommunikation visuell. Das Bild als Forschungsgegenstand Grundlagen und Perspektiven*. (S. 144-158). Köln: Herbert von Halem.
- Scheufele, B. (2003). *Frames – Framing – Framing-Effekte. Theoretische und methodische Grundlegung sowie empirische Befunde zur Nachrichtenproduktion*. Wiesbaden: Westdeutscher Verlag.
- Schlepper, C. & Leese, M. (2011). Plädoyer für eine unabhängige und grundrechtsgerechte Evaluation der EU-Richtlinie zur Vorratsdatenspeicherung. *Neue Kriminalpolitik*, 23 (2), 70-75.
- Schlepper, C. & Lüdemann, C. (2010). Stärkung des Vertrauens in die Regierung durch Terrorismusbekämpfungsmaßnahmen? *Kriminalistik*, 64 (10), 570-575.
- Schlepper, C., Wickert, C., Wöbcke, J. & Paul, B. (2013). „... das kennt man ja vom Flughafen“. Über die Akzeptanz neuer Sicherheitsmaßnahmen im Fährverkehr. Unv. MS.
- Schmied-Knittel, I. (2010). Sichtbarmachung des Unsichtbaren. Visualisierung als Beglaubigungsstrategie. In H.-G. Soeffner (Hrsg.). *Unsichere Zeiten. Herausforderungen gesellschaftlicher Transformationen*, Verhandlungen des 34. Kongresses der Deutschen Gesellschaft für Soziologie in Jena, Wiesbaden (CD-ROM).
- Schütz, A. & Luckmann, T. (1979). *Strukturen der Lebenswelt*, Band 1. Frankfurt/M.: Suhrkamp.



- Selbmann, F. (2008). *Verfassungsbeschwerde der Schriftstellerin und Rechtsassessorin Juli Zeh und des Rechtsanwalts Dr. Frank Selbmann vom 28.01.2008*. Verfügbar unter <http://zelos.zeit.de/2008/06/Verfassungsbeschwerde28012008.pdf> [26. August 2013]
- Sheehan, I.S. (2012). Assessing and Comparing Data Sources for Terrorism Research. In Lum C. & Kennedy L.W. (Hrsg.). *Evidence-Based Counterterrorism Policy*. Springer Series on Evidence-Based Crime Policy 3. (S. 13-42). New York: Springer.
- Simmel, G. (1992). *Soziologie. Untersuchungen über die Formen der Vergesellschaftung*. Frankfurt/M.: Suhrkamp.
- Simon, D. (2008). Der Rechtsstaat. Vortrag gehalten auf der Internationalen Konferenz *Die Wahrheit der Illusion*, Einstein Forum, Potsdam, 7.-8. Februar.
- Singelstein, T. & Stolle, P. (2006). *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert*. Wiesbaden: VS.
- Smith, J.P. & Edmonston, B. (Hrsg.) (1998). *The Immigration Debate: Studies on the economic, demographic, and fiscal effects of immigration*. Washington: National Academy Press.
- Stäheli, U. (2000). *Sinnzusammenbrüche. Eine dekonstruktive Lektüre von Niklas Luhmanns Systemtheorie*. Weilerswist: Velbrück.
- Ströbele, C. & Erlenmeyer, H. (2006). Sicherheitspolitik nach dem 11.9. *Sicherheit und Frieden (S + F)*, 23 (3), 135-142.
- Sturken, M. & Cartwright, L. (2009). *Practices of Looking. An Introduction to Visual Culture*. New York: Oxford University Press.
- Sunstein, C.R. (2007). *Gesetze der Angst*. Frankfurt/M.: Suhrkamp.
- Surowiecki, J. (2007). *Die Weisheit der Vielen. Warum Gruppen klüger sind als der Einzelne*. München: Goldmann.
- Sztompka, P. (1998). Trust, Distrust and Two Paradoxes of Democracy. *European Journal of Social Theory* 1 (1), 19-32.
- Tauss, J. (2008). Vertrauen in der Informationsgesellschaft. In D. Klumpp, H. Kubicek, A. Roßnagel & W. Schulz (Hrsg.). *Informationelles Vertrauen für die Informationsgesellschaft* (S. 63-70). Berlin: Springer.





- The 9/11 Commission Report (2004). *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Company. Verfügbar unter <http://www.9-11commission.gov/report/911Report.pdf> [11. September 2013].
- Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty. Heuristics and biases. *Science*, 185, 1124–1131.
- Tyler, T.R. (1990). *Why People Obey the Law*. New Haven: Yale Univ. Press.
- von Arnim, G., Deile, V. & Hutter, F.-J. (Hrsg.) (2002). *Jahrbuch Menschenrechte 2003. Schwerpunkt: Terrorismusbekämpfung und Menschenrechte*, Frankfurt/M.: Suhrkamp.
- von Trotha, T. (2002). Über die Zukunft der Gewalt. In: *Monatsschrift für Kriminologie und Strafrechtsreform*, 85 (5), 349-368.
- von Trotha, T. (2010). Die präventive Sicherheitsordnung. Weitere Skizzen über die Konturen einer „Ordnungsform der Gewalt“. *Kriminologisches Journal*, 42 (1), 24-40.
- Vowe, G. (2012). Massenmedien. In U. Andersen & W. Woyke (Hrsg.). *Handwörterbuch des politischen Systems der Bundesrepublik Deutschland*. 7. Aufl. (S. 440–448). Wiesbaden: Springer VS.
- Walker, J. & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*, 42 (2), 143-160.
- Weber, M. (2008). *Akzeptanz biometrischer Authentifizierungssysteme*. Dissertation Univ. Mannheim, Mannheim.
- Welch, M. (2006). *Scapegoats of September 11th*. New Brunswick, NJ: Rutgers University Press.
- Weltecke, D. (2003). Gab es „Vertrauen“ im Mittelalter? Methodische Überlegungen. In U. Frevert (Hrsg.). *Vertrauen. Historische Annäherungen* (S. 7-66). Göttingen: Vandenhoeck & Ruprecht.
- Werber, N. (2010). Zur Genealogie des Nicht-Kriegs. Ein Epochenwandel in der gesellschaftlichen Selbstbeschreibung. In H. Münkler, M. Bohlender & S. Meurer (Hrsg.). *Handeln unter Risiko. Gestaltungsansätze zwischen Wagnis und Vorsorgen* (S. 83-104). Bielefeld: transcript.
- Will, R. (2006). Karlsruhe versagt Grundrechts-Schutz beim IMSI-Catcher. *Mitteilungen der Humanistischen Union*, 195 (4), 12-14.



Will, R. (2011). Die Evaluation als Bürgerrechtsfrage. 10 Jahre nach 9/11 fehlt noch immer eine nüchterne Bilanz der Terrorismusgesetzgebung. *Mitteilungen der Humanistischen Union*, 214 (3), 1-3.

Wolf, B. (2011). Literarischer Möglichkeitssinn in der Moderne. In R. Innerhofer, K. Rothe & K. Harrasser (Hrsg.). *Das Mögliche regieren. Gouvernamentalitätsanalyse in der Literaturwissenschaft* (S. 19-30). Bielefeld: transcript.

Würtenberger, T. , Gusy, C. & Lange, H.-J. (Hrsg.) (2012). *Innere Sicherheit im europäischen Vergleich. Sicherheitsdenken, Sicherheitskonzepte und Sicherheitsarchitektur im Wandel*. Berlin: Lit.

Zebrowski, C. (2009). Governing the Network Society: A Biopolitical Critique of Resilience. *Political Perspectives*, 3 (1), 1-43.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, 11 (2), 261-281.

Zedner, L. (2009). *Security*. London, New York: Routledge.

Zoche, P., Kaufmann, S. & Haverkamp, R. (Hrsg.) (2011). *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript.





## Quellen

Alfred-Herrhausen-Gesellschaft (2007). *Forsa-Umfrage: Öffentliche Sicherheit: Staatsmonopol oder marktfähiges Gut?* Verfügbar unter [http://www.alfred-herrhausen-gesellschaft.de/downloads/Umfrage\\_forsa\\_Sicherheit.pdf](http://www.alfred-herrhausen-gesellschaft.de/downloads/Umfrage_forsa_Sicherheit.pdf) [26. August 2013]

BR-Drs. 722/04 vom 24. September 2004. *Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung).*

Bundesamt für Justiz (2009-2012). *Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100g StPO) für 2008-2011.* Verfügbar unter <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html> [30. August 2013]

Bundesanstalt für Finanzdienstleistungsaufsicht (2005-2013): *Jahresbericht der Bundesanstalt für Finanzdienstleistungsaufsicht 2004-2012.* Verfügbar unter [http://www.bafin.de/DE/DatenDokumente/Dokumentlisten/ListeJahresberichte/liste\\_jahresberichte\\_node.html](http://www.bafin.de/DE/DatenDokumente/Dokumentlisten/ListeJahresberichte/liste_jahresberichte_node.html) [26. August 2013]

Bundesministerium des Innern (Hrsg.) (2011a). *Das Gemeinsame Internetzentrum. Zur Bekämpfung des islamistischen Terrorismus im Internet.* Verfügbar unter [http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Terrorismus/giz.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Terrorismus/giz.pdf?__blob=publicationFile) [26. August 2013]

Bundesministerium des Innern (Hrsg.) (2011b). *Das Gemeinsame Terrorismusabwehrzentrum. Zusammenarbeit der Sicherheitsbehörden zur Bekämpfung des islamistischen Terrorismus.* Verfügbar unter [http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Terrorismus/gtaz.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Terrorismus/gtaz.pdf?__blob=publicationFile) [26. August 2013]

Bundesregierung (2005). *Bericht der Bundesregierung zu den Auswirkungen der nach Artikel 22 Abs. 2 des Terrorismusbekämpfungsgesetzes befristeten Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Artikel 10-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des § 7 Abs. 2 des BKA-Gesetzes. Innenausschuss A-Drs. 15(4)218.* Verfügbar unter [http://www.cilip.de/terror/eval\\_tbg\\_11052005.pdf](http://www.cilip.de/terror/eval_tbg_11052005.pdf) [30. August 2013]

BT-Drs. 14/7386 (neu) vom 08. November 2001. *Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN. Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz).*

BT-Drs. 15/3699 vom 09. September 2004. *Unterrichtung durch die Bundesregierung. Bericht der Bundesregierung gemäß Artikel 13 Abs. 6 Satz 1 Grundgesetz für das Jahr 2003.*



BT-Drs. 16/4138 vom 29. Januar 2007. *Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften.*

BT-Drs. 16/4456 vom 28. Februar 2007. *Unterrichtung durch die Bundesregierung. Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften – Drucksache 16/4138 – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung.*

BT-Drs. 17/6223 vom 16. Juni 2011. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Jens Petermann, Frank Tempel und der Fraktion DIE LINKE. – Drucksache 17/6017 (neu) – Einrichtung einer Visa-Warndatei.*

BT-Drs. 17/7104 vom 25. Oktober 2011. *Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, Petra Pau, Jens Petermann, Frank Tempel, Halina Wawzyniak und der Fraktion DIE LINKE. Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage („Staatstrojaner“).*

BT-Drs. 17/7760 vom 17. November 2011. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/7104 – Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage („Staatstrojaner“).*

BT-Drs. 17/10601 vom 05. September 2012. *Unterrichtung durch die Bundesregierung. Bericht der Bundesregierung gemäß Artikel 13 Abs. 6 Satz 1 Grundgesetz für das Jahr 2011.*

BT-Drs. 17/12774 vom 14. März 2013. *Unterrichtung durch das Parlamentarische Kontrollgremium Bericht gemäß § 8a Absatz 6 Satz 2, § 9 Absatz 4 Satz 7 des Bundesverfassungsschutzgesetzes (BVerfSchG), § 2a Satz 4, § 3 Satz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) sowie den §§ 4a, 5 des Gesetzes über den Militärischen Abschirmdienst (MADG) und § 8a Absatz 8 BVerfSchG über besondere Auskunftsverlangen im Sinne von § 8a Absatz 2 BVerfSchG und den Einsatz technischer Mittel im Sinne von § 9 Absatz 4 BVerfSchG im Jahre 2010 (Bericht zu den Maßnahmen nach dem Terrorismusbekämpfungsgesetz).*

BT-Drs. 17/14515 vom 2. August 2013. *Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, Jan van Aken, Herbert Behrens, Christine Buchholz, Inge Höger, Ulla Jelpke, Niema Movassat, Thomas Nord, Frank Tempel, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.*

BT-Drs. 17/14714 vom 06. September 2013. *Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE – Drucksache 17/14515 – Neuere Formen der Überwachung der Telekommunikation durch Polizei und Geheimdienste.*



BT-Protokoll 14/192 vom 11. Oktober 2001. *Stenographischer Bericht*, 14. Wahlperiode, 192. Sitzung, 18680-18698.

BT-Protokoll 14/195 vom 18. Oktober 2001. *Stenographischer Bericht*, 14. Wahlperiode, 195. Sitzung, 19019-19020.

Europäische Kommission (2007b). *Soziale Wirklichkeit in Europa. Eurobarometer Spezial 273. Country Sheet*. Verfügbar unter [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_273\\_fiche\\_de.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_273_fiche_de.pdf) [26. August 2013]

Europäische Kommission (2010). *Mitteilung der Kommission an das Europäische Parlament und den Rat. Politik der EU zur Terrorismusbekämpfung: wichtigste Errungenschaften und künftige Herausforderungen*. Verfügbar unter <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0386:FIN:DE:PDF> [26. August 2013]

Hummelsheim, D. (2013). *(Un-)Sicherheitswahrnehmung und Lebenszufriedenheit in Deutschland. Empirische Ergebnisse einer repräsentativen Bevölkerungsbefragung*, Vortrag auf der Konferenz „Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung“ des Bundesministeriums für Bildung und Forschung, Berlin, 13.6.2013. V [www.bmbf.de/pubRD/Vortrag\\_Hummelsheim.pdf](http://www.bmbf.de/pubRD/Vortrag_Hummelsheim.pdf) [26. August 2013]

Infocenter der R+V Versicherung (2009). *Die Ängste der Deutschen 2009*. Verfügbar unter <http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2009/20090903-aengste-der-deutschen-2009-grafik.pdf> [26. August 2013]

Infocenter der R+V Versicherung (2011). *Die Ängste der Deutschen 2011*. Verfügbar unter <http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2011/20110908-aengste-der-deutschen-grafiken-bundesweit.pdf> [26. August 2013]

Infocenter der R+V Versicherung (2012a). *Die Ängste der Deutschen 2012. Untersuchungsmethode der Studie*. Verfügbar unter [http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2012/20120903\\_fragen\\_methode.pdf](http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2012/20120903_fragen_methode.pdf) [26. August 2013]

Infocenter der R+V Versicherung (2012b). *Die Ängste der Deutschen 2012*. Verfügbar unter [http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2012/dieaengstederdeutschen\\_bundesweit.pdf](http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2012/dieaengstederdeutschen_bundesweit.pdf) [26. August 2013]

Infocenter der R+V Versicherung (2013). *Die Ängste der Deutschen 2013*. Verfügbar unter [http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2013/dieaengstederdeutschen\\_bundesweit.pdf](http://www.ruv.de/de/presse/download/pdf/aengste-der-deutschen-2013/dieaengstederdeutschen_bundesweit.pdf) [11. September 2013]