KOMMENTAR

Zehn Jahre nach 9/11: Zum politischen Umgang mit dem ‚Terrorrisiko'

Ulrich Schneckener

Ten Years after 9/11: On the political response to the 'risk of terror'
Abstract: This commentary deals with the question of what typical patterns are characteristic of the political and administrative response to the 'risk of terror'. The key assumption is that the 'new' transnational terrorism is not only in itself a risk that is difficult to calculate but is furthermore perceived as enforcing those catastrophic risks which generally exist in modern high-tech societies. This combination of risk and 'risk enforcement' explains why in such societies terrorism could have such a big impact which shapes the ways of reaction described here. As a conclusion, the article advocates to add a political conflict perspective to the dominant, primarily technocratic risk perspective.

Keywords: Transnational Terrorism, Fighting Terrorism, Threat, Risk

Schlüsselwörter: Transnationaler Terrorismus, Terrorismusbekämpfung, Bedrohung, Risiko

1. Einleitung

Aus einer ‚abstrakten Gefährdungslage' wurde im November 2010 eine ‚konkrete': Der damalige Innenminister Thomas de Maizière sprach eine umfassende ‚Terrorwarnung' aus, wohl eine der umfassendsten in Deutschland seit den Tagen nach dem 11. September 2001. Es gebe „Grund zur Sorge", da sich verschiedene „Hinweise" verdichtet hätten, wonach islamistische Terroristen Anschlagsplanungen vorantrieben und bereits „Ende November ein mutmaßliches Anschlagsvorhaben" durchgeführt werden könnte.[1] In den USA oder in Großbritannien hätte man in einem solchen Fall wohl die höchste Alarmstufe ausgelöst – *red* bzw. *critical*. Offen wurde in den Medien über ein ‚Mumbai-Szenario' spekuliert, wonach ein Terrorkommando – wie im November 2008 im indischen Mumbai – schwer bewaffnet das Berliner Regierungsviertel stürme und versuche, so viele Menschen wie möglich zu töten. De Maizière bezog sich bei seiner Warnung auf Erkenntnisse in- und ausländischer Dienste, aber auch auf öffentliche Ankündigungen von Al-Qaida-nahestehenden Gruppen und Personen. Das Resultat war unter anderem eine erhöhte Polizeipräsenz auf Flughäfen, Bahnhöfen und öffentlichen Plät-

1 Siehe die Stellungnahme von Innenminister Thomas de Maizière zur aktuellen Gefährdungslage vom 17.11.2010 (http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/11/statement2.html; zugegriffen: 23.6.2011).

zen sowie nicht zuletzt die wochenlange Schließung des Reichstagsgebäudes für Besucher. Der Anschlag hat – zum Glück – nicht stattgefunden.

Vielleicht war er nie geplant; vielleicht aber haben sich die Täter von der erhöhten Aufmerksamkeit abschrecken lassen und ihre Planungen (vorerst) auf Eis gelegt. Vielleicht saßen die Geheimdienste Fehlinformationen auf, die bewusst von Extremisten gestreut wurden, um in Ermangelung anderer Alternativen ein diffuses Gefühl von Unsicherheit zu verbreiten. Vielleicht haben die Sicherheitsbehörden auch ihre Quellen ‚falsch' gelesen und waren, kommunikationstheoretisch gesprochen, schlicht nicht in der Lage ‚*noise*' von ‚*signals*' zu unterscheiden. In einer solchen Situation ist kein Innenminister zu beneiden. Wenn er nicht warnt und es passiert etwas, kann er vermutlich seinen Rücktritt einreichen. Wenn er warnt und es passiert nichts, setzt er sich dem Vorwurf des ‚Alarmismus' oder der ‚Panikmache' aus und muss befürchten, dass seine Warnungen beim nächsten Mal weniger ernst genommen werden. Zwar wird bei solchen Gelegenheiten betont, es bestehe „kein Grund zur Hysterie" (De Maizière), derartige Floskeln hinterlassen aber beim Publikum zumeist einen zwiespältigen Eindruck. Warnt er und es passiert etwas, kann er sich zwar bestätigt sehen, muss aber möglicherweise trotzdem zurücktreten, weil die ergriffenen Maßnahmen nicht erfolgreich waren, um einen – bereits antizipierten – Anschlag zu verhindern. Nüchtern betrachtet wäre für alle die beste Variante: Er warnt nicht und es passiert nichts. Das Risiko, auf das Nicht-Eintreten eines Ereignis zu spekulieren, dürfte jedoch ein/e Minister/in, der oder die politisch für die öffentliche Sicherheit verantwortlich ist, in einer demokratischen Gesellschaft kaum eingehen. Insofern wird das Ergebnis stets eine ‚Warnung' sein, verbunden mit den entsprechenden Sicherheitsvorkehrungen. Die Episode zeigt: Terrorismus ist hierzulande ein „handlungsaktivierendes Noch-Nicht-Ereignis" (Beck 1986, S. 43) *par excellence*, auch darauf können sich im Übrigen die Terroristen verlassen.

Die Gründe für das Agieren des Ministers hängen eng damit zusammen, wie nach 9/11 Gesellschaft und Politik auf die Herausforderung durch den ‚neuen', transnationalen Terrorismus reagiert haben.[2] Dieser Kommentar nimmt keine umfassende Bilanz und Bewertung der Terrorismusbekämpfung vor, wie sie sich national und international in den vergangenen zehn Jahren entwickelt hat, sondern stellt vielmehr einige grundsätzliche Beobachtungen zu typischen Mustern im Umgang mit Terrorismus zur Diskussion. Die zentrale These lautet dabei, dass der ‚neue' Terrorismus nicht nur für sich genommen als schwer kalkulierbares Risiko gilt, das angesichts des Schadens- und Zerstörungspotenzial an andere Groß-Risiken erinnert, sondern zudem auch als ‚Verstärker' für jene Katastrophen-Risiken wahrgenommen wird, die grundsätzlich in einer modernen, durch Hochtechnologie geprägten Gesellschaft bestehen. Diese Kombination aus Risiko und ‚Risikoverstärkung' erklärt, warum Terrorismus – und zwar bereits als bloße, latente Drohung – in solchen Gesellschaften eine besondere Wirkung entfaltet, der eine demokratisch verfasste Politik Rechnung tragen muss. Der empirische Hin-

2 Das Adjektiv „neu" bezieht sich ausschließlich auf einige *neuartige* Aspekte des transnationalen Terrorismus, der allerdings in mehrfacher Hinsicht eine Weiterentwicklung bisheriger Formen des Terrorismus darstellt, siehe dazu ausführlicher Schneckener (2006).

tergrund für die folgenden Überlegungen sind primär die innenpolitischen Debatten in Deutschland, die mir gleichwohl symptomatisch für westliche Industrieländer zu sein scheinen. Bevor auf die Probleme und Mechanismen des Umgangs eingegangen werden soll, gilt es allerdings, kurz wesentliche Aspekte der ‚neuen' terroristischen Herausforderung für die Politik der inneren Sicherheit zu skizzieren.

2. Die Transnationalisierung des Terrorismus als Herausforderung

Was Terrorismus ist, ist und bleibt bekanntermaßen hochgradig umstritten (und politisch umkämpft). Noch umstrittener ist, wer eigentlich als Terrorist gelten kann. Will man den Begriff analytisch verstanden wissen, handelt es sich dabei um eine spezifische Form politisch motivierter Gewalt, die wiederum von anderen Varianten gewaltsamen Handelns unterscheidbar ist.[3] Diejenigen, deren Gewaltanwendung im Wesentlichen durch diese Form gekennzeichnet ist, kann man soziologisch als „Terroristen" oder als „terroristische Organisationen" bezeichnen. Insofern ist Terrorismus mehr als eine bloße Gewaltstrategie, die unterschiedlichen Akteuren (bis hin zum Staat) offen steht, sondern es geht um eine Praxis, die wiederum bestimmte organisatorische Anforderungen an den Akteur stellt. Kurz: Wer Terrorismus praktizieren will, muss sich in einer spezifischen Weise organisieren. Terrorismus – auch in seiner transnationalen, netzwerkförmigen Variante – ist nach wie vor ein Mittel von klandestinen „Kleingruppen" (Neidhardt 1988, S. 196-197), die mangels eigener militärischer Stärke aus dem Untergrund agieren und versuchen, durch Attentate eine Gesellschaft oder wesentliche Teile davon in Panik und Schrecken zu versetzen, um nach eigener Aussage politische Ziele durchzusetzen.

Auch wenn sich das grundlegende terroristische Kalkül im Kern nicht von ‚älteren' Formen des Terrorismus unterscheidet (vgl. dazu Münkler 1992, Waldmann 1998, Hoffman 2001), so ist es dem ‚neuen' transnationalen Terrorismus, paradigmatisch verkörpert durch das Netzwerk Al Qaida, seine regionalen Ableger und ihm nahestehende islamistische Gruppierungen, gelungen, lokale und internationale Aspekte ideologisch, strategisch und operativ miteinander zu verknüpfen. Von zentraler Bedeutung ist dabei das von Osama Bin Laden und anderen seit Mitte der 1990er-Jahre verbreitete ‚Narrativ', wonach es gelte eine Reihe von lokalen Konflikt- und Problemlagen von Nordafrika über die Golfregion bis hin nach Zentral-, Süd- und Südostasien in den Kontext einer globalen Auseinandersetzung zwischen dem ‚Westen' (‚Ungläubigen'), allen voran den USA und ihren Verbündeten, einerseits und der vermeintlich ‚erniedrigten' oder ‚fremdbestimmten' muslimischen Welt andererseits einzubetten. Im Unterschied zum Terrorismus alten Typs geht es den transnationalen Gruppierungen eben nicht (allein) um die Änderung einer nationalen Ordnung, sondern sie streben eine neue internationale – oder zumindest regionale – Ordnung an. Mit dieser Zielsetzung sind ideelle und organisatorische Aspekte verbunden wie eine multi-nationale

3 Zur Abgrenzung des Begriffs zu anderen Gewaltphänomen und insbesondere zum Problem des „Staatsterrors", vgl. Schneckener (2006, S. 21-39; 2008, S. 26-29; 2010).

Mitglieder- und Gefolgschaft, transnationale Ideologie und Kommunikationsräume sowie grenzüberschreitende Netzwerkstrukturen.

In dieser Transnationalisierung von militanten Gruppierungen drückt sich die neue Qualität aus, die dazu führt, dass die Terrorismusbekämpfung – zumindest in westlichen Industrieländern – stärker als zu früheren Zeiten aus einer *Risikoperspektive* erfolgt – und nicht aus einer ‚traditionellen' *Bedrohungsperspektive*. Zwar kann man argumentieren, dass es sich bei Terrorismus in Gestalt von benennbaren Akteuren, die intentional Gewalt gegen andere anwenden (wollen), um eine konkrete *Bedrohung* handelt. Gleichzeitig verweist aber seine Untergrundaktivität (Intransparenz), seine Latenz, sein schwer kalkulierbares Potenzial und – wie noch zu zeigen sein wird – die mit dem ‚neuen' Terrorismus verbundene Proliferation von denkbaren Szenarien eher auf ein *Risiko*, das strukturell gewisse Parallelen zu Risiken im Technologie-, Umwelt- oder Gesundheitsbereich aufweist.[4] Die Bedrohungsperspektive stellt dagegen auf die Minimierung von Szenarien ab und konzentriert sich auf wenige, einigermaßen bekannte Variablen (*known knowns*) – man kennt den Gegner, dessen Kapazitäten und *grosso modo* dessen strategische Optionen (was Fehlkalkulationen und -wahrnehmungen aber keinesfalls ausschließt). All dies ist jedoch beim transnationalen – oder sich transnationalisierenden – Terrorismus noch viel weniger der Fall als bei seinen ähnlich ambivalent wirkenden Vorläufern. Es sind vor allem fünf Aspekte, die in ihrer Kumulation den Wandel von der Bedrohungs- zur Risikoperspektive markieren und jene Ansätze in Frage stellen, die in der Bekämpfung des ‚internen' Terrorismus der 1970er- und 1980er-Jahre relevant waren.

(a) *Netzwerkförmige Strukturen statt hierarchisch gegliederter Organisationen*: Die Prozesse der Transnationalisierung spiegeln sich in netzwerkförmigen Strukturen wider, durchaus unter Beibehaltung gewisser hierarchischer Elemente, da auch der transnationale Terrorismus nicht ‚führungslos' agiert. Stattdessen werden bei Al-Qaida und nahestehenden Gruppierungen je nach Funktion – und abhängig von Opportunitäten – unterschiedliche Organisationsprinzipien genutzt und kombiniert. Folgende Merkmale dürften für die Netzwerke charakteristisch sein: flexible, dezentrale Strukturen; geringer Grad an Hierarchisierung und Formalisierung; ideologische und strategische ‚Richtlinienkompetenz' der Führung; hohes Maß an sozialer Mobilität innerhalb des Netzwerks sowie latente, aktivierbare Kontakte zu anderen Akteuren, insbesondere zu potenziell globalen Logistik-, Unterstützer- und Sympathisantennetzwerken. Die einzelnen Zellen, Kommandos oder auch assoziierten Gruppierungen, die teilweise unter anderen Namen firmieren, genießen einen relativ hohen Grad an Autonomie und Autarkie. Mit anderen Worten: Al-Qaida – im eigenen Selbstverständnis eine Art ‚Dachverband' – ist nicht nur selbst ein transnationales Netzwerk, sondern wiederum von anderen, kleineren und größeren Netzwerken, zumeist verbunden über personalisierte Kontakte, umgeben. Diese Struktur bedingt – fast schon systemisch – einen relativ hohen Grad an Robustheit und Resistenz gegenüber dem generellen Verfolgungsdruck bzw. gegenüber gezielten Angriffen von außen. In der Tendenz sind

4 Zur analytischen Unterscheidung von Bedrohung und Risiko, vgl. Daase (2002, 2011).

Netzwerke anpassungsfähiger und innovativer als strikt hierarchisch gegliederte Organisationen. Netzwerke können zumindest in Teilen fortbestehen, solange wichtige Knotenpunkte innerhalb des Netzes bzw. Schnittstellen zu anderen Akteuren funktionsfähig bleiben und in der Lage sind, auftretende personelle Lücken oder materielle Engpässe rasch zu schließen. Auch wenn zentrale Führungspersonen – wie etwa bei der Tötung Osama Bin Ladens durch US-Spezialkräfte am 2. Mai 2011 – ausgeschaltet werden, bleiben wesentliche Teile des Netzwerkes aktiv und lebensfähig. Es genügt daher nicht, eine zentrale Kommandoebene auszuschalten oder gar – wie im Falle der Gruppe Carlos – einen einzelnen ‚Topterroristen' zu jagen.

(b) *Gewachsene Bedeutung nicht-staatlicher Unterstützung*: Die Transnationalisierung des Terrorismus ist auch durch die stark gewachsene Bedeutung nichtstaatlicher, grenzüberschreitender Unterstützung bedingt. Diese allgemeine Entwicklung vom *state sponsored* zum *non-state sponsored terrorism* gilt zwar auch für lokale militante Gruppierungen (z. B. Finanzierung über Diaspora-Gemeinschaften wie etwa im Falle der LTTE in Sri Lanka), aber in einem hohen Maße gerade für transnationale Netzwerke. Im Unterschied zum staatlich geförderten Terrorismus genügt es hierbei nicht, bestimmte Regierungen mit politischen, wirtschaftlichen und, gegebenenfalls, militärischen Sanktionen unter Druck zu setzen, um sie dazu zu bewegen, ihre (mutmaßliche) Kooperation mit Terrorgruppen zu beenden. Die vielfältigen, nicht-staatlichen Sponsoren entziehen sich oftmals der Kontrolle von Regierungen oder sie bewegen sich schlicht in einem legalen Rahmen. Nicht-staatliche Unterstützer sind zudem sehr unterschiedlich motiviert: Es gibt die Sympathisantenkreise im engeren Sinne, die weitgehend die Ideologie und die politischen Ziele der jeweiligen Gruppierung teilen. Daneben gibt es eher profitorientierte Sponsoren, die, weniger aus ideologischer denn aus kommerzieller Absicht, Terrorgruppen unterstützen; dazu gehören in erster Linie Geschäftsleute, Steuer- und Finanzexperten, Schmuggler, Waffen- und Drogenhändler, Passfälscher, Kleinkriminelle, kriminelle Banden oder Warlords. Eng verbunden mit dieser Ausweitung potenzieller Unterstützer und Helfer ist eine starke Diversifizierung von Möglichkeiten zur Finanzierung. Terroristische Netzwerke verfügen in der Regel über zahlreiche Finanzquellen und Transferwege. Der Verlust einzelner Quellen kann durch andere relativ rasch kompensiert werden, zumal Terrorismus grundsätzlich mit vergleichsweise wenigen Mitteln auskommt. Die Kontrolle und Eindämmung von Finanzströmen wird damit erheblich erschwert. Die größten Probleme bereiten legale Quellen (z. B. Fundraising, Erträge aus Wirtschaftsaktivitäten), der Bargeld-Schmuggel und die informellen Geldtransfersysteme, die sich staatlichen Kontrollen bzw. verschärften Bankvorschriften weitgehend entziehen.

(c) *Erhöhtes Zerstörungspotenzial und verstärkte mediale Effekte*: Bereits vor dem 11. September ließ sich der Trend zu größeren Operationen mit entsprechenden Opferzahlen (*mass casualty attacks*) statistisch belegen. Spätestens die Anschläge auf die Zwillingstürme sowie nachfolgende Attentate auf Verkehrsinfrastruktur, internationale Einrichtungen oder große Hotelkomplexe in Bali (2002), Casablanca (2003), Istanbul (2003), Madrid (2004), London (2005), Amman (2005), Algier (2006), Islamabad (2008), Mumbai (2008) oder Kampala (2010), bei denen es stets mehrere Dutzend Tote und eine hohe Zahl an Verletzten gab,

verweisen ebenso wie diverse aufgedeckte oder gescheiterte Anschlagspläne auf eine wachsende Bereitschaft und Fähigkeit zur Zerstörung. Diese Entwicklung hängt sowohl mit verbesserten technologischen Möglichkeiten als auch mit veränderten taktischen Mitteln zusammen, wie etwa dem vermehrten Einsatz von Selbstmordattentätern oder der Planung von simultanen Mehrfach-Anschlägen (wie z. B. auf die Londoner U-Bahn oder auf das UN-Gebäude in Algier). Damit geht auch die Verstärkung von medialen Effekten einher, auf die Terrorismus elementar angewiesen ist, um seine psychologische Wirkung zu entfalten.[5] Insbesondere Al-Qaida, aber mehr und mehr auch andere gleichgesinnte Gruppierungen, haben die massenmediale Inszenierung ihrer Aktivitäten professionalisiert und perfektioniert, sie senden ihre Bild-, Ton- und Textbotschaften unmittelbar an eine globale Öffentlichkeit. Aufgrund der modernen Kommunikationstechnologie kontrollieren sie heute sowohl die Inhalte als auch die Formen und Kanäle ihrer Verbreitung; es gibt keinen ‚Filter' mehr zwischen Sender und Empfänger. Diese Entwicklung erleichtert militanten Gruppierungen die psychologische ‚Kriegführung', da sie ihnen eine mediale Bühne verschafft, die sie gegenüber Gegnern wie Sympathisanten ‚größer' und ‚mächtiger' erscheinen lässt, als dies unter Umständen einzelne Anschläge vermögen.

(d) *Unklares Täterprofil*: Im Unterschied beispielsweise zum europäischen Linksterrorismus der 1970er-Jahre ist das Täterprofil beim transnationalen Terrorismus weitaus diffuser, was allein schon der Tatsache geschuldet ist, dass es hierbei um multi-nationale Gruppierungen geht, deren Angehörige nicht auf eine bestimmte nationale/ethnische/sprachliche Gruppe beschränkt sind. Dies spiegelt sich in der Zusammensetzung und Struktur der Zellen und der Unterstützernetzwerke wider. Zudem werden unterschiedliche Methoden und Pfade der Rekrutierung genutzt, die dem jeweiligen Kontext und den lokalen Milieus angepasst werden. Damit kommt grundsätzlich ein sehr großer, letztlich nicht überschaubarer Personenkreis für eine potenzielle Täterschaft in Frage. Es bleibt unklar, nach welchen typischen gemeinsamen Merkmalen man eigentlich suchen soll, abgesehen vielleicht von einer gewaltbereiten, islamistischen Einstellung und entsprechenden Aufenthalten in afghanischen, pakistanischen oder anderen Trainings- und Schulungscamps. Die bisherigen Anschläge oder Anschlagsversuche in Europa und Nordamerika passen in dieses Bild: Ob bei den Anschlägen in Madrid, London oder Istanbul, ob bei Festnahmen in Deutschland, Italien, den Niederlanden, Kanada oder den USA – stets waren unterschiedliche Personenkreise involviert, die sich einem gemeinsamen Muster entziehen. Dies gilt für die nationale und soziale Herkunft ebenso wie für den beruflichen Hintergrund (zu finden sind u. a. Studenten, Sozialarbeiter, Ärzte, Lehrer, Ingenieure, Geschäftsleute, Kleinkriminelle). Unter den Attentätern und Terrorverdächtigen sind erst vor wenigen Jahren eingereiste Ausländer, im jeweiligen Land geborene bzw. aufgewachsene Angehörige der zweiten oder dritten Migrantengeneration, eingebürgerte Personen oder auch zum Islam konvertierte Staatsbürger.

5 Die frühere britische Premierministerin Margaret Thatcher sprach zugespitzt davon, dass die Medien den „Sauerstoff der Publizität" lieferten, von dem die Terroristen letztlich abhängen, vgl. Hoffman (2001, S. 189).

(e) *Unklares Tatprofil*: Ebenso wie das Täter- ist auch das Tatprofil deutlich unschärfer geworden. Spätestens seit dem 11. September wird bei den Sicherheitsbehörden im Prinzip jeder Plot, jede Art von Anschlag, für vorstellbar gehalten. Beschränkte sich früher das ‚klassische' Spektrum internationaler Anschläge typischerweise auf Flugzeugentführungen, Auto- und LKW-Bomben, Botschaftsbesetzungen oder Geiselnahmen, scheint heute keine Fantasie mehr so absurd, als dass sie nicht von Terrorgruppen, die über die notwendige Bereitschaft und Fähigkeit verfügen, in die Tat umgesetzt werden könnte. Die Bandbreite möglicher Anschlagsziele ist erheblich größer geworden. Dies wird durch die diversen Terrorwarnungen oder Szenarien belegt, die seit 9/11 von Sicherheitsexperten diskutiert werden oder über die munter in den Medien spekuliert wird: Sprengung von Brücken und Hochhäusern; Umbau von Schiffscontainern zu Bomben; Konstruktion ‚schmutziger Bomben'; Anschläge auf Energiesysteme, Ölraffinerien, Chemiefabriken oder Atomkraftwerke; Terrorattacken gegen öffentliche Transportsysteme, Handelsschiffe, Fähren und Öltanker; Verseuchung des Trinkwassers bzw. von Lebensmitteln; Anschläge mit Pockenviren; Cyberterrorismus etc. Beflügelt werden diese Überlegungen durch angeblich vereitelte oder gescheiterte Plots, wie etwa die Sprengung eines Tunnels unter dem Hudson River in New York (2006), die Explosion von mehreren Flugzeugen über dem Atlantik mit Flüssigsprengstoff (2006), die nicht gezündeten ‚Kofferbomben' in Regionalzügen in Deutschland (2006), der mutmaßliche Angriff auf den Frankfurter Flughafen bzw. auf amerikanische Einrichtungen im Rhein-Main-Gebiet (‚Sauerlandgruppe', 2007) oder der fehlgeschlagene Autobomben-Anschlag auf dem Times Square in New York (2010). Kurz: Seit 2001 vergeht kaum ein Monat, in dem nicht über neue potenzielle Anschlagsziele und -formen berichtet wird; es gibt vermutlich kaum ein weltbekanntes Bauwerk und kaum ein Groß-Ereignis, das nicht bereits einmal als mögliches Ziel ausgedeutet wurde. Das Dilemma besteht nun darin, dass kein Staat der Welt auf diese enorme Proliferation von Szenarien und die damit verbundenen, potenziellen Risiken gleichermaßen angemessen reagieren, geschweige denn entsprechende Vorsorge- und Schutzmaßnahmen treffen kann. Allein schon aus Kapazitätsgründen müssen daher in jeder Gesellschaft grundlegende Entscheidungen und Präferenzen bei der Aufklärung, der Gefahrenabwehr und dem Schutz kritischer Infrastruktur getroffen werden.

3. Terrorismus als Risiko und ‚Risikoverstärker'

Die zentrale Frage lautet daher: Welche Risiken, die der ‚neue' Terrorismus mit sich bringt bzw. bringen *könnte*, ist eine Gesellschaft bereit, zu welchen materiellen und ideellen Kosten (etwa im Kontext von Freiheitseinschränkungen) abzudecken? Und welche Risiken nimmt man letztlich in Kauf? Gefragt sind eine robuste Risikobewertung (*risk assessment)*, ein entsprechendes Risikomanagement und eine darauf abgestimmte Risikokommunikation (insbesondere zwischen Staat und Bürger). Doch was in der Theorie relativ einfach klingt, erweist sich in der Praxis allein angesichts der Vielzahl von denkbaren Variablen mit Blick auf Strukturen, Unterstützung, Zerstörungspotenzial, Täter und Taten als überaus schwierig. Anders formuliert: Terrorismus ist schlicht durch zu viele *known unknowns*

charakterisiert. Daran ändert – wie man aus der Forschung zu anderen Risiken weiß – auch die Zunahme von Wissen relativ wenig, da diese immer auch mit der Zunahme von Nicht-Wissen (*blind spots*) verbunden ist. Dies soll nun keinesfalls implizieren, dass es müßig wäre, sich um einen Erkenntnisgewinn zu bemühen, sondern es soll nur darauf hingewiesen werden, dass der unmittelbare Nutzen für die Risikokalkulation zumeist begrenzt ist. Die Lage wird dadurch noch komplizierter, dass der ‚neue' Terrorismus nicht nur für sich genommen unbekannte Risiken birgt, sondern zudem als potenzieller ‚Verstärker' von bekannten Groß-Risiken gilt und damit wiederum deren Risikobewertung verändert. Auf diese Weise befördert der Terrorismus den Bereich der *unknown unknowns* – jener Katastrophen-Risiken oder Desaster, die sich nur schwerlich antizipieren lassen und die demzufolge als ‚unkalkulierbar' gelten.[6] Die Debatten um einen möglichen terroristischen Anschlag auf Kernkraftwerke, auf große Rechenzentren oder auf die Trinkwasserversorgung mögen diesen Punkt illustrieren. Ulrich Beck bezeichnet daher das „Terrorrisiko" als einen „Unfall-Katastrophen-Zwitter": „Das entgrenzte Terrorrisiko kann begrenzte Schadensfälle wie entgrenzte Katastrophen auslösen" (2007, S. 243).

Diese ‚Doppelrolle' trifft nun auf spezifische Weise den ‚Nerv' von industrialisierten und demokratisch verfassten Gesellschaften. Dies hängt nicht allein mit der reinen physischen Präsenz von hochtechnologischer Infrastruktur zusammen, die stets als die zentrale Achillesferse von Risikogesellschaften ausgemacht wird, sondern vor allem mit tieferliegenden sozialen und kognitiven Entwicklungen, die die Risikoperzeption und die ‚Kultur' im Umgang mit Risiken prägen. In Anlehnung an die Arbeiten von *Ortwin Renn* sollen dabei drei Aspekte besonders hervorgehoben werden, die für unser Thema relevant sind (vgl. Renn et. al. 2007; Renn u. Keil 2008). *Erstens* werden aufgrund von Verdichtungs- und Vernetzungsprozessen Groß-Risiken zunehmend von einer ‚systemischen' Warte aus wahrgenommen und analysiert. Darunter werden jene Risiken gruppiert, bei denen zeitgleich oder kaskadenartig verschiedene ‚Systeme' geschädigt werden können – wie etwa Ökosysteme, ‚Märkte', Logistik und Transport, Telekommunikation, öffentliche Gesundheit oder auch, mittelbar, das politische System. „Systemische Risiken" sind charakterisiert durch dynamische Ausstrahlungseffekte, eine kaum durchschaubare Komplexität von Ursache-Wirkungs-Ketten sowie ein hohes Maß an Ambiguität, sprich an Mehrdeutigkeit im Hinblick auf die zu erwartenden Konsequenzen (Renn u. Keil 2008, S. 350). Diese vernetzte Sicht auf Risiken, die auch sekundäre und tertiäre Folgen in den Blick nimmt, erhöht die Anforderungen an Risikobewertung und Risikomanagement erheblich. Dessen ungeachtet besteht *zweitens* nach wie vor im Alltagsverhalten grundsätzlich eine hohe Bereitschaft Katastrophen-Risiken einzugehen, die mit modernen Verkehrssystemen und groß-technologischen Anlagen verbunden sind, sofern deren Eintrittswahrscheinlichkeit als überaus niedrig gilt und damit die individuelle Schadenswahrscheinlichkeit als gering einzustufen ist (z. B. das Risiko, bei einem Bahnunglück oder einem Flugzeugabsturz ums Leben zu kommen). Zugleich hat

6 Die Verwendung des Known/Unknown-Vokabulars erfolgt in Anlehnung an Daase und Kessler (2007, S. 414-415).

aber *drittens* in unseren Breitengraden der Grenznutzen materieller Güter gegenüber immateriellen Gütern abgenommen, was zu einer höheren Sensibilität mit Blick auf ganz bestimmte Risiken führt. Fragen allgemeiner Gesundheit, einer sauberen Umwelt und des persönlichen Wohlbefindens spielen eine weitaus größere Rolle als dies noch auf dem Höhepunkt des Industriezeitalters der Fall war (Renn et. al. 2007, S. 159-160). Das zeigen hierzulande nicht zuletzt die öffentlichen Debatten im Kontext von ‚Lebensmittelskandalen'. Alle drei Aspekte sind mit Vorsorgeansprüchen an die staatliche Politik verbunden. Von denjenigen, die politisch und administrativ auf Risiken reagieren müssen, wird erstens erwartet, dass sie die ‚systemischen Effekte' in das Risikomanagement einkalkulieren und durch entsprechende Vorkehrungen abfedern (z. B. vernetzte Sicherheitssysteme, Vorhaltung von Nahrungs- und Energiereserven); zweitens, dass sie die Eintrittswahrscheinlichkeit von Katastrophen-Risiken durch hohe Sicherheitsstandards niedrig halten; und drittens, dass sie angesichts eines „gestiegenen Gesundheits-, Umwelt- und Sicherheitsbewusstseins" für „intakte Lebensumstände" (Renn et. al. 2007, S. 165) sorgen. Kurz: Der Staat ist unter dieser Perspektive mehr denn je der „ultimative Rückversicherer" (Beck 2007, S. 246). Dies verschafft ihm zwar eine zusätzliche Legitimation (vgl. Czada 2000), setzt seine gewählten Vertreter aber auch unter einen hohen Erwartungs- und Handlungsdruck.

Auf diese Disposition trifft der ‚neue' Terrorismus mit seinen Unwägbarkeiten. Aufgrund seines risikoverstärkenden Charakters erhöht er die Komplexität ‚systemischer Risiken' und ihrer Wirkungsketten. Er erhöht, wenn man bestimmten Szenarien Glauben schenkt, die Wahrscheinlichkeit von in Kauf genommenen Katastrophen-Risiken und er tangiert in hohen Maße immaterielle Güter, da Terrorismus – medial verstärkt – stets auf die psychische und mentale Verfasstheit einer Gesellschaft abzielt. Was euphemistisch als ‚Rest-Risiko' bezeichnet wird, verändert sich durch das Hinzutreten eines Terrorismus mit amorphen Strukturen, bei dem sich weder der Täterkreis noch die Art und Weise der Anschläge sinnvoll einschränken lassen. Das Unbekannte führt zu neuen Unbekannten. Die zentrale Verunsicherung besteht darin, dass Terrorismus grundlegend die technokratische Vorstellung von der Bewert- und Steuerbarkeit von Risiken sowie von der fortwährenden Optimierbarkeit des Risikomanagement in Frage stellt, wie sie mit dem Risikokonzept verbunden ist (im Unterschied zum Begriff der Gefahr).[7] Es geht eben nicht mehr darum bloßes ‚menschliches Versagen' zu minimieren, Vorsorge mit Blick auf natürliche Gefahren (z. B. Erdbeben, Flutwellen) zu treffen oder mögliche Kettenreaktionen zu antizipieren, sondern nunmehr kommt der intentionale Faktor ins Spiel, möglichst große Katastrophen auslösen zu *wollen*. Wir wissen nicht, ob und unter welchen Bedingungen so etwas passiert – und wir wissen auch nicht, welche sozialen, ökonomischen und ökologischen Folgen ein solches Ereignis hätte. Wir wissen demzufolge weder etwas über die Eintritts-

7 Zur Unterscheidung von Risiko und Gefahr, siehe vor allem Luhmann (1991). Allerdings verwendet Luhmann einen anderen Risikobegriff als Beck (1986, 2007) oder Renn et. al. (2007), die beide nicht auf die Zurechenbarkeit auf einen ‚Entscheider' abstellen, der ein Risiko eingeht. Bei Luhmann gibt es genau genommen keine komplexen oder systemischen Risiken, da diese immer kausal zurechenbar sein müssen (Luhmann 1991, S. 128).

wahrscheinlichkeit solcher ‚Terrorrisiken' noch etwas über das zu erwartende Schadensausmaß (was die Frage nach der räumlichen und zeitlichen Ausdehnung sowie nach der Reversibilität der Schäden einschließt). Die beiden wesentlichen Variablen einer Risikokalkulation bleiben Leerstellen. Was warum zu tun ist, bleibt letztlich eine zutiefst politische Entscheidung. Die Politik steht hier vor der Alternative, entweder das ‚Risiko der Unterschätzung' (und damit Verharmlosung) oder das ‚Risiko der Überschätzung' (und damit Dramatisierung) des ‚Terrorrisikos' einzugehen. Die Sache wird dadurch noch komplizierter, dass die Politik oftmals gar nicht weiß, wann sie eigentlich das eine oder das andere tut. War die Warnung von Minister de Maizière ‚übertrieben', weil man Spekulationen und Gerüchten aufgesessen war oder war sie ‚untertrieben', weil in Wahrheit die Gefahr viel größer war als vermutet? Wer will das mit letzter Gewissheit beantworten?

4. Typische Reaktionsmuster im Umgang mit dem ‚Terrorrisiko'

Was also tun? Unter diesen Vorzeichen besteht die Tendenz, sich im Diskurs und bei Sachentscheidungen primär an der Kategorie des ‚Möglichen' und nicht an der Kategorie des ‚Wahrscheinlichen' zu orientieren. Beck (2007, S. 195-196) spricht daher auch von einer Gesellschaft, die sich in den „Zustand des Konjunktivs" versetze, von einer „Könnte-sein-Gesellschaft". Da jedoch – wie oben ausgeführt – mit Blick auf den ‚neuen' Terrorismus alles Mögliche für ‚möglich' gehalten werden *kann*, wächst dieser Faktor der Risikogleichung potenziell ins Unendliche und kann kaum als Maßstab dafür herhalten, welche Maßnahmen zur Terrorismusbekämpfung eigentlich erforderlich, angemessen oder gar ausreichend sind (vgl. Daase u. Kessler 2007, S. 424-426). Polemisch zugespitzt formuliert: Die staatlichen Sicherheitsdienste und mit ihnen die demokratische Politik werden auf diese Weise zu ‚Gefangenen' ihrer eigenen Fantasien, die zu immer neuen imaginierten ‚Sicherheitslücken' und damit zu immer neuen Deckungsproblemen führen. Es kann unter diesen Vorzeichen nie ‚genug' Sicherheit geben. Die Politik muss jedoch letztlich der Öffentlichkeit plausibel machen, warum man sich gegen bestimmte Aspekte des ‚neuen' Terrorismus und gegen bestimmte Szenarien wappnen soll, gegen andere aber nicht, um nicht beim Publikum den Eindruck eines defizitären Umgangs mit der Herausforderung zu hinterlassen.

Die Lage wird jedoch zusätzlich dadurch erschwert, dass die Politik und die Sicherheitsbehörden ihre Schlüsse und Lehren – trotz aller denkbarer und diskutierter Szenarien – letztlich aus einer relativ kleinen Fallzahl (*Small-n*-Problematik) ziehen. Denn größere terroristische Anschläge – wie Katastrophen generell – sind in Europa vergleichsweise seltene Ereignisse (im Unterschied zu anderen Weltregionen, in denen Gewaltkonflikte an der Tagesordnung sind). Das ist zwar überaus erfreulich, bedeutet aber, dass es methodisch schwierig ist, genauer festzustellen, ob und welche Maßnahmen zur Bekämpfung und zur Prävention wirksam sind und welche nicht. Ist die geringe Anzahl nun das Ergebnis der eigenen, offenbar erfolgreichen Bemühungen oder aber anderen, wenig beeinflussbaren Faktoren geschuldet (z. B. der Vorgehensweise, den Absichten oder der strukturellen Schwäche des terroristischen Akteurs)?

Dieser eklatante Mangel an Gewissheit verschärft das Problem von „Risiken zweiter Ordnung", die sich aus der gesellschaftlichen Sinnzuschreibung von Risiken sowie aus dem politischen und administrativen Umgang damit ergeben (vgl. Renn et. al. 2007, S. 165-166). Gemeint sind damit soziale Risiken wie Kompetenz- und Interessenskonflikte zwischen Institutionen, der Verlust von Vertrauen in die politisch Verantwortlichen, Legitimations- und Akzeptanzprobleme, Versuche der Stigmatisierung (z. B. Bildung von islamfeindlichen Parteien), politische Machtverschiebungen oder die systematische Stärkung der Exekutive zulasten von Legislative und Judikative (u. a. eingeschränkte parlamentarische und richterliche Kontrollmöglichkeiten). Die öffentliche Debatte um die Frage „wie viel Sicherheit und wie viel Freiheit" dreht sich beispielsweise im Kern um solche ‚Risiken zweiter Ordnung' (vgl. Huster u. Rudolph 2008).

In diesem Korridor bewegt sich nun die politische Reaktion auf das ‚Terrorrisiko': Die Entscheidungsträger müssen einerseits möglichst sachgerechte Antworten auf ein überaus komplexes und potenziell entgrenztes Problem finden, sie müssen andererseits dabei die Wirkungen auf ‚Risiken zweiter Ordnung' berücksichtigen. Letztere sind für sie oftmals von größerer Bedeutung als jene ‚erster Ordnung'. Dies gilt insbesondere dann, wenn man bei diesen weitgehend im Nebel herumstochern muss und auch die Experten in- und außerhalb des Sicherheitsapparates widersprüchliche Empfehlungen abgeben.[8] Was in einer solchen Situation passiert, lässt sich an folgenden Reaktionsmustern ablesen, die aus meiner Sicht den politisch-administrativen Umgang mit dem Terrorismus seit 9/11 charakterisieren.

(a) *Worst-Case-Denken*: Es besteht die starke Neigung, sich auf *Worst-Case*-Szenarien zu konzentrieren. Da niemand genau weiß, was passieren kann, rechnet man mit dem schlimmstmöglichen Fall, selbst wenn dieser in Relation zu anderen Szenarien als eher unwahrscheinlich gilt. Das beste Beispiel dafür ist das Szenario eines Terrorismus mit Massenvernichtungswaffen – in der amerikanischen Literatur schon vor 9/11 als *catastrophic terrorism* oder *ultimate terrorism* bezeichnet (vgl. Carter et al. 1998; Stern 1998). Die Debatte, unter welchen Bedingungen Terroristen nukleare, biologische, chemische oder radiologische Waffen einsetzen würden, gewann nach 9/11 enorm an Bedeutung, obwohl die Anschläge mit Flugzeugen und Teppichmessern durchgeführt worden waren. Der frühere Innenminister Wolfgang Schäuble bereicherte diese Diskussion einmal mit der lakonischen Bemerkung, wonach es gar nicht mehr die Frage sei, ob ein Terroranschlag mit nuklearem Material passiere, sondern nur noch wann und wo.[9] Geht man wie Schäuble hypothetisch von einem solchen Anschlag aus, stellt sich angesichts des möglichen Schadensausmaßes die Frage nach der Wahrscheinlichkeit nicht mehr. Solche *non-standard scenarios* (Daase u. Kessler 2007, S. 427) dominieren dann

8 Auf dieses „Expertendilemma" hat Czada (2000) mit Blick auf den Umgang mit der Kernenergie hingewiesen und dabei herausgearbeitet, dass die uneinheitliche Position von ‚Experten' mit Gutachten und Gegengutachten letztlich den Handlungsspielraum politischer Entscheidungsträger vergrößert.

9 Interview mit Innenminister Wolfgang Schäuble (Frankfurter Allgemeine Sonntagszeitung vom 16.9.2007). Zur ‚Beruhigung' fügte Schäuble hinzu: „Es hat keinen Zweck, dass wir uns die verbleibende Zeit auch noch verderben, weil wir uns vorher schon in eine Weltuntergangsstimmung versetzen."

nicht nur die Risikoperzeption, sondern auch die Suche nach geeigneten Abwehrmaßnahmen und Schutzvorkehrungen, was notwendigerweise materielle und personelle Ressourcen bindet.[10] Gleichzeitig stellt diese ‚Politik des Äußersten' elementare Grund- und Menschenrechte in Frage – bis hin zum Folterverbot, wie sich am Umgang mit Terrorverdächtigen und Guantánamo-Häftlingen zeigte. Auch die deutschen Regierungen seit 2001, ob nun Rot-Grün, Rot-Schwarz oder Schwarz-Gelb gefärbt, hatten letztlich wenig Hemmungen, die Informationen, die auf solch fragwürdige Weise generiert wurden, für die eigenen Sicherheitsanalysen und entsprechende Maßnahmen zu nutzen.

(b) *Sammeln und Speichern von Daten*: Wer – nicht zuletzt angesichts unklarer Täter- und Tatprofile – nicht genau weiß, wonach er eigentlich suchen soll, muss letztlich jedes Detail für potenziell relevant halten. Wer die Stecknadel nicht kennt, hält zwangsläufig den ganzen Heuhaufen für potenzielle Stecknadeln. Diese Logik führte zu einer sukzessiven Ausweitung bei der Sammlung und Speicherung von personenbezogenen Daten in den Großrechnern der Sicherheitsbehörden. Jeder Anschlag nach 9/11 beförderte diese Aktivitäten, da als eine Ursache stets der Mangel an ‚Informationen' galt; jeder verhinderte Anschlag wiederum wurde als Beleg für den Nutzen solcher Maßnahmen herangezogen. Unabhängig davon, was gerade geschah: Für das Sammeln und Speichern von Daten ließen sich stets Argumente finden. Darunter fallen unter anderem Personenangaben, Telefon-, E-Mail- und Internetverbindungen, Bankverbindungen, Bewegungs-, Reise- oder Flugpassagierdaten, wie sie etwa im transatlantischen Flugverkehr erfasst werden. Um an einige dieser Daten heranzukommen, wurden Eingriffe in das Post- und Briefgeheimnis notwendig; die Befugnisse zur Überwachung von Telekommunikation wurden ausgeweitet, neue Befugnisse (Stichwort „Online-Durchsuchung") eingeführt (vgl. Schaar 2008). Zudem gilt es, wie die Debatte um die ‚Vorratsdatenspeicherung' zeigt, auf diese Daten möglichst lange Zugriff zu behalten, da man eben nicht wissen kann, welches Material wann gebraucht werden *könnte*. Wer Daten nicht erhebt oder ‚zu früh' löscht, der geht das Risiko ein, entscheidende Hinweise nicht zu erhalten. Wer allerdings umfangreiche Daten erhebt und vorhält, der setzt sich selbst unter den Zugzwang, solche Hinweise auch zu finden, d. h., er muss die Daten ‚lesen' und auswerten zu können, er muss ‚Datenschrott' von verwertbaren ‚Informationen' trennen, er muss den Daten einen Sinn verleihen. Dazu bedarf es aber wiederum bestimmter Hypothesen über Attentäter und Anschlagsformen, die – wie oben gezeigt – nicht einfach zu generieren sind.

(c) *Rückgriff auf bekannte Methoden*: Unter diesem Punkt kann eine Reihe von Mechanismen subsumiert werden, die typisch sind, wenn bürokratische Organisationen mit ‚Neuem' konfrontiert werden. Sie reagieren durch Routinehandeln im Rahmen bekannter Methoden und Maßnahmen, die notfalls adaptiert oder optimiert werden, um der ‚neuen' Herausforderung zu begegnen. Es handelt sich im

10 Den Extremfall dieses Denkens erlebte die Welt beim Irakkrieg, als die Regierung von US-Präsident Bush argumentierte, dass das Regime von Saddam Hussein über solche Waffen verfügen *könnte* und diese an Al-Qaida-Terroristen weitergeben *könnte*, weshalb ein Präventivkrieg nicht nur geboten, sondern geradezu notwendig sei (vgl. kritisch dazu Schneckener 2003).

Wesentlichen um die Fortschreibung des Bekannten, oftmals erklärbar durch administrative Pfadabhängigkeiten und Zuständigkeiten. Ein Beispiel war die Einführung von biometrischen Reisedokumenten (seit 1.11.2005), die letztlich auf der seit Jahrzehnten verfolgten Linie liegt, solche Papiere so fälschungssicher wie möglich zu halten. Von Dörner (2011, S. 83-86) wird diese Reaktionsweise auch „Methodismus" genannt, wobei er betont: „Methodismus ist nicht einfach die Wiederholung von Verhaltensweisen, die in der Vergangenheit erfolgreich waren, sondern die Wiederholung solcher Verhaltensweisen, *ohne dass* kontrolliert wird, ob die Bedingungen noch gegeben sind" (2011, S. 85, Herv. i. O.). Eine Illustration wie aus dem Lehrbuch ist die nach 9/11 durchgeführte, aber wirkungslose Rasterfahndung; ähnliches ließe sich angesichts des ‚unklaren Täterprofils' über die europaweite Verschärfung von Einreise- und Visabestimmungen sagen. Daneben findet sich auch die Übertragung oder ‚Umetikettierung' von bekannten Methoden aus anderen, thematisch verwandten Feldern – etwa aus dem Bereich der transnational organisierten Kriminalität (z. B. Maßnahmen zur Geldwäschebekämpfung). Damit verbunden sind in der Regel Analogieschlüsse und das „Denken in Ähnlichkeiten" (Dörner), die es den Apparaten erleichtern, bekannte Methoden weiter zu praktizieren. Ein Beleg dafür sind die diversen Versuche zur Entwicklung von ‚Täterprofilen', wie sie auch bei der Bekämpfung des RAF-Terrorismus angewandt wurden. Dies reichte seit 9/11 von der These ‚eingeschleuster Schläfer-Zellen' (Analogie aus dem Geheimdienstmilieu) über die Vorstellung von Al-Qaida als einem ‚Franchising-Unternehmen' bzw. einem ‚Label', das sich unterschiedliche Gruppierungen zunutze machen (Analogie aus dem Wirtschaftsleben) bis hin zu den jüngst diskutierten Typen des *Self-made*-Terroristen, der sich (angeblich) allein über das Internet radikalisiert (Analogie zum kriminellen Einzeltäter), und des *homegrown terrorism*, der sich auf jene Extremisten bezieht, die in Deutschland aufgewachsen sind (Analogie zur Bandenkriminalität bzw. zu gewaltbereiten Jugendgangs). Auf diese Weise werden vorgefundene Schablonen und Stereotypen weiterentwickelt, die sich selektiv auf einzelne Aspekte konzentrieren, ohne aber das Gesamtproblem erfassen zu können. Die ‚neue' Herausforderung wird letztlich so definiert und perzipiert, wie sie den existierenden Maßnahmen und Instrumenten am ehesten gerecht wird.

(d) *‚Einfache Lösungen'*: Es besteht ferner die Tendenz, dass sich die Politik auf relativ ‚einfache Lösungen' kapriziert, die entweder ohnehin zur Verfügung stehen und insofern schon als ‚erprobt' gelten oder aber relativ einfach umgesetzt werden können. Ein Beispiel für Ersteres ist der Ausbau von Videoüberwachung an öffentlichen Plätzen oder die Ausweitung von Personenkontrollen in öffentlichen Gebäuden; ein Beispiel für Letzteres ist die Anschaffung und Einlagerung von Impfdosen, um sich gegen einen möglichen terroristischen Anschlag mit Pockenviren zu wappnen. Man schützt sich auf diese Weise gegen jene Szenarien, gegen die man sich leicht schützen kann, unabhängig davon, wie wahrscheinlich oder bedrohlich diese sind. Dies erklärt eben auch, warum auf Flughäfen das Gepäck kontrolliert wird, aber nicht auf Bahnhöfen oder in Zügen – es lässt sich leichter

bewerkstelligen. Es wird getan, was man tun kann, ohne dass dies aber zwingend das ist, was man gegebenenfalls tun sollte.[11]

(e) *Präferenz für technologische Antworten*: Eine weitere Reaktionsweise besteht darin, auf die terroristische Herausforderung mit der Entwicklung von neuen Sicherheitstechnologien zu antworten – gemäß dem Motto „Sicherheit durch Technik". Diese Überlegung folgt ein wenig der Logik, wonach man sich mit Alarmanlagen vor Einbrechern schützen kann.[12] Befördert wird dieser Ansatz durch die oben beschriebene ‚Doppelrolle' des Terrorrisikos. Die Folgen sind erhöhte Sicherheitsstandards bei technischen Neuerungen (z. B. im Bereich der IT-Sicherheit) oder die Einführung neuer Techniken – wie etwa der ‚Körperscanner' auf Flughäfen oder die biometrische Gesichtserkennung bei Überwachungskameras. Ein Beleg für diese Ausrichtung ist das 2007 von der Bundesregierung aufgelegte Programm zur zivilen Sicherheitsforschung (im Umfang von 123 Millionen Euro), das sich primär als High-Tech-Strategie versteht, um die Entwicklung innovativer Produkte im Sicherheitsbereich zu fördern. Die zuständige Ministerin, Annette Schavan, machte am Beispiel der ‚Körperscanner' deutlich, wie sehr die Politik auf High-Tech-Lösungen setzt, um die Bevölkerung vor *Low-Tech*-Mitteln, wie sie typischerweise Terroristen anwenden, zu schützen: „Ausgangspunkt ist, dass bestimmte Waffen wie Keramikmesser oder Sprengstoffe mit den bisherigen Metalldetektoren nicht gefunden und schon gar nicht sichtbar gemacht werden können. Es wäre in keiner Weise verantwortbar, uns nicht mit Technologien zu befassen, die solche Waffen erkennen können" (Schavan 2011, S. 22).

(f) *‚Aktionismus'*: Eine andere Reaktionsweise ist die Flucht in den „Aktionismus", womit man sich selbst und dem Publikum politische Handlungsfähigkeit suggeriert (vgl. Dörner 2011, S. 86). Es handelt sich dabei nicht nur um reine PR-Aktionen oder weitgehend wirkungslose symbolische Maßnahmen, sondern nicht selten dient der ‚Aktionismus' dazu, die Bevölkerung oder auch den eigenen Beamtenapparat aufzurütteln und die öffentliche Aufmerksamkeit auf bestimmte Probleme zu lenken, ohne dass man allerdings substanzielle Lösungen für diese parat hätte. In diese Kategorie gehören beispielsweise der stets wiederkehrende Ruf nach neuen gesetzlichen Regelungen (und vor allem nach härteren Strafen), turnusmäßig wiederholte Terrorwarnungen, das publikumswirksame Einsetzen von Gremien, Krisenstäben und Sonderbeauftragten, das demonstrative Verkünden von neuen Aktionsplänen und – zumeist plakativen – Slogans (z. B. „Netzwerke bekämpft man durch Netzwerke" [Otto Schily]) oder auch die Reorganisation von ganzen Apparaten.

(g) *Suche nach Ursache-Wirkungs-Ketten:* Der Umgang mit dem ‚Terrorrisiko' ist zudem durch die Suche nach Meta-Variablen gekennzeichnet, die die ‚Ursachen' des Terrorismus schlüssig erklären können, um darauf aufbauend gezielte Gegenstrategien zu entwickeln. Häufig genannte ‚Kandidaten' für solche unab-

11 Dieser Reaktionsmodus erinnert an den von Dörner als „horizontale Flucht" bezeichneten Umgang mit Komplexität: „Man zieht sich in einen Bereich zurück, in dem man handeln kann, der aber für die Lösung der tatsächlich anstehenden Probleme kaum eine Rolle spielt" (Dörner 2011, S. 86).

12 Zu den ambivalenten Folgen von Technisierungsstrategien, vgl. Strohschneider (2011).

hängigen Variablen sind die Rolle des Islam, Armut oder soziale Benachteiligung, Mangel an Bildung, mangelnde oder ‚gescheiterte' Integration von Ausländern, fehlende Modernisierung oder Demokratisierung in der arabisch-islamischen Welt, Staatszerfall oder, kritisch gewendet, die hegemoniale Politik des Westens. Solche relativ pauschalen Erklärungsversuche kursieren zumeist auch in den Medien und werden auf diese Weise handlungsleitend.[13] Neidhardt (1988, S. 179) sieht in postulierten Ursache-Wirkungs-Ketten eine typische Reaktionsweise, wenn der Handlungsdruck zunimmt: „Sie sichern hohe und schnelle Handlungsfähigkeit, indem sie von irritierender Komplexität entlasten, und sie verweisen auf Verantwortlichkeiten, an die man sich halten kann." Diese Kausalitätsfixierung ist für Neidhardt (1988, S. 182) eine Folge der relativ geringen „Kontingenztoleranz", die bürokratische Apparate kennzeichnet, deren rationale Planungs- und Verwaltungsabläufe gerade darauf abzielen, die Anfälligkeit für Zufälliges oder Überraschendes zu minimieren. Scheinbar erratische Gewaltphänomene – zumal Terrorismus – bedürfen daher einer rationalistisch abgesicherten Einordnung. In diesem Punkt richtet die Politik nicht zuletzt entsprechende Erwartungen an *die* Wissenschaft, die – einem positivistischen Denkschema folgend – Kausalmechanismen identifizieren und somit zur Entlastung von „irritierender Komplexität" beitragen soll. Allzu häufig wird sie jedoch hier enttäuscht, da Wissenschaft – wenn überhaupt – zumeist genau das Gegenteil tut und mit komplexen Erklärungsmodellen aufwartet, die sich nicht ohne weiteres operativ umsetzen lassen.

5. Fazit und Schlussfolgerungen

Für sich genommen besitzt jede Reaktionsweise eine nachvollziehbare Rationalität. Allesamt dienen sie der Reduktion von Komplexität und der Selektion von Risiken bzw. Szenarien, vor denen die Bevölkerung geschützt werden soll. Sie reflektieren zudem politische und administrative Sachlogiken, sie dienen der Durchsetzung von spezifischen Interessen und Präferenzen, sie zielen nicht zuletzt auf die Minimierung von ‚Risiken zweiter Ordnung'. Zumeist wird dies mit der Standardfloskel verbunden, die Politik werde ‚alles Menschenmögliche' unternehmen, um die Bevölkerung vor diesem oder jenem zu schützen. Dieser Satz führt jedoch in die Irre, da – wie es die Reaktionsmuster zeigen – eben nicht alles ‚Menschenmögliche' getan wird (und auch gar nicht getan werden sollte!), sondern es letztlich um das ‚Zweckmäßige' geht, bei dem ‚Kosten' und ‚Nutzen' der Risikovermeidung gegeneinander abgewogen werden müssen. Faktisch geschieht dies auf der Grundlage der genannten Reaktionsweisen auch – denn diese machen im Umkehrschluss deutlich, welche ‚Terrorrisiken' die Politik offenbar in Kauf nimmt oder schlicht ignoriert. Nur wenig kritische Reflexion erfahren dabei – und das sollte in der Darstellung deutlich werden – die impliziten, selten hinterfragten

13 Ein Beispiel dafür ist die Figur des *homegrown terrorism*, die einen kausalen Zusammenhang von Extremismus und gelungener bzw. missglückter Integrationspolitik unterstellt, was bei jedoch bei näherer Betrachtung weder eindeutig noch sonderlich überzeugend ist, vgl. Schneckener (2008, S. 36-37).

Grundannahmen, die unbeabsichtigten Nebenfolgen und die ‚neuen' Risiken, die mit den jeweiligen Reaktionsmustern verbunden sind.

Das größte Defizit besteht aus meiner Sicht aber darin, dass sich keine der beschriebenen typischen Reaktionsweisen mit dem terroristischen Kalkül im engeren Sinne auseinandersetzt, sondern primär mit den Risiken und Folge-Risiken, die potenziell aus diesem erwachsen *können*. Die hierzulande dominierende, eher technokratische *Risikoperspektive* sollte daher um eine politische *Konfliktperspektive* ergänzt werden. Denn Terrorismus, ob ‚alter' oder ‚neuer' Prägung, ist grundsätzlich ein Ausdruck gesellschaftlicher und internationaler Konflikt- und Problemlagen. Diese Form der Gewalt ist in den allermeisten Fällen ein Resultat von politischen und sozialen Prozessen und Dynamiken im Kontext von eskalierten bzw. eskalierenden Konflikten. Eine solche Perspektive, die hier nur angedeutet werden kann, setzt das Verständnis voraus, dass offenbar – zumindest in der Wahrnehmung der Terroristen – Deutschland, Europa oder der ‚Westen' Teil dieser Eskalation sind und dass es sich hierbei um eine *Aktions-Reaktions-Spirale* handelt, an der ‚wir', ob gewollt oder nicht, mit ‚schrauben'. Während sich die ‚Terrorbekämpfer' als legitime Verteidiger der öffentlichen Ordnung verstehen, sind sie aus einer konflikttheoretischen Perspektive zunächst einmal nichts anderes als eine *Konfliktpartei*, auch wenn ihnen diese Rolle von den Terroristen aufgenötigt wurde. Im eigenen Handeln wird diese Positionierung jedoch nicht reflektiert, sondern zumeist negiert, da damit das politische Eingeständnis verbunden wäre, dass man selbst Teil einer dynamischen *Konfliktkonstellation* ist und nicht nur ein passives ‚Zielgebiet' potenzieller Anschläge. Wer jedoch das Denken in Konfliktkategorien meidet, dem bleiben die eigendynamischen und mikropolitischen Prozesse verborgen, die Gewaltkonflikten typischerweise innewohnen und die das Kalkül und das Verhalten von Gewaltakteuren maßgeblich bestimmen.[14] Deren Einsatz von Gewalt erfolgt zwar intentional, ist aber in hohem Maße von kontingenten Faktoren abhängig, die auch von den Gewaltakteuren selbst nicht bis ins Letzte zu kontrollieren sind. Das ist im Übrigen ein Grund dafür, dass Terroristen – ungeachtet aller *Worst-Case*-Szenarien – sich in aller Regel eher konservativ verhalten und zu solchen Mitteln greifen, die sie leidlich beherrschen, weshalb vermutlich die Gepäck- oder Fahrzeugbombe mit oder ohne Selbstmordattentäter der ‚Normalfall' bleiben wird – und 9/11 der extreme Ausnahmefall.[15] Insofern entbehrt es, rückblickend, nicht einer gewissen Ironie, dass dieser – zugegeben dramatische – Sonderfall aufgrund der besonderen Disposition westlicher Gesellschaften eine stark normierende Wirkung auf die Perzeption des ‚Terrorrisikos' und den Umgang mit demselben hatte. Dabei ist der Gedanke nicht neu (vgl. z. B. Fromkin 1977), wonach nicht der Terrorismus definiert, wie man auf ihn reagieren soll, sondern dass wir grundsätzlich die Wahl haben, ob wir überhaupt und in welcher Form wir reagieren. Ob wir von dieser Wahl Gebrauch machen oder nicht, entscheiden wir im Übrigen auch. Ob diese schlichte

14 Siehe zu diesem Punkt u.a. den nach wie vor überaus lesenswerten Beitrag von Neidhardt (1988: 178-191).

15 Diese These wird nicht zuletzt durch diverse Beispiele an fehlgeschlagenen Anschlägen bestätigt, in denen sich Terroristen an Innovationen oder gar an einer Nachahmung von 9/11 versuchten.

Erkenntnis in dem Jahrzehnt seit 9/11 stets beherzigt wurde, darf man allerdings getrost bezweifeln.

Literatur

Beck, Ulrich. 1986. *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a. M.: Suhrkamp.

Beck, Ulrich. 2007. *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*. Frankfurt a. M.: Suhrkamp.

Carter, Ashton, B., John M. Deutch, und Philip D. Zelikow. 1998. Catastrophic Terrorism: Tackling the New Danger. *Foreign Affairs* 77:80-94.

Czada, Roland. 2000. Legitimation durch Risiko – Gefahrenvorsorge und Katastrophenschutz als Staatsaufgaben. In *Politik und Technik*, Politische Vierteljahrsschrift Sonderheft 31, Hrsg. Georg Simonis, Renate Martinsen und Thomas Saretzki, 319-345. Wiesbaden: VS Verlag für Sozialwissenschaften.

Daase, Christopher. 2002. Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. In *Internationale Risikopolitik*, Hrsg. Christopher Daase, Susanne Feske, und Ingo Peters, 9-35. Baden-Baden: Nomos.

Daase, Christopher. 2011. Der Wandel der Sicherheitskultur – Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*, Hrsg. Peter Zoche, Stefan Kaufmann und Rita Haverkamp, 139-158. Bielefeld: Transcript.

Daase, Christopher, und Oliver Kessler. 2007. Knowns and Unknowns in the ‚War on Terror': Uncertainty and the Political Construction of Danger. *Security Dialogue* 38:411-434.

Dörner, Dietrich. 2011. Über die Schwierigkeiten des Umgangs mit Komplexität. In *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*, Hrsg. Peter Zoche, Stefan Kaufmann und Rita Haverkamp, 71-90. Bielefeld: Transcript.

Fromkin, David. 1977. Die Strategie des Terrorismus. In *Terrorismus. Untersuchungen zur Strategie und Struktur revolutionärer Gewaltpolitik*, Hrsg. Manfred Funke, 83-99. Bonn: Bundeszentrale für politische Bildung.

Hoffman, Bruce. 2001. *Terrorismus. Der unerklärte Krieg*. Frankfurt a. M.: Fischer.

Huster, Stefan, und Karsten Rudolph. 2008. Vom Rechtsstaat zum Präventionsstaat? In *Vom Rechtsstaat zum Präventionsstaat*, Hrsg. Stefan Huster und Karsten Rudolph, 9-24. Frankfurt a. M.: Suhrkamp.

Luhmann, Niklas. 1991. *Die Soziologie des Risikos*. Berlin: de Gruyter.

Münkler, Herfried. 1992. *Gewalt und Ordnung*. Frankfurt a. M.: Fischer.

Neidhardt, Friedhelm. 1988. *Gewalt und Terrorismus. Studien zur Soziologie militanter Konflikte*. Berlin: Wissenschaftszentrum Berlin für Sozialforschung.

Renn, Ortwin, Marion Dreyer, Andreas Klinke, und Pia-Johanna Schweizer. 2007. Systemische Risiken: Charakterisierung, Management und Integration in eine aktive Nachhaltigkeitspolitik. In *Jahrbuch Ökologische Ökonomik 5, Soziale Nachhaltigkeit*, 157-188. Marburg: Metropolis.

Renn, Ortwin, und Florian Keil. 2008. Systemische Risiken: Versuch einer Charakterisierung. *GAIA* 17:349-354, http://www.oekom.de/gaia.

Schaar, Peter. 2008. Der Rüstungswettlauf in der Informationstechnologie. In *Vom Rechtsstaat zum Präventionsstaat*, Hrsg. Stefan Huster und Karsten Rudolph, 45-63. Frankfurt a. M.: Suhrkamp.

Schavan, Annette. 2011. Eröffnungsansprache. In *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*, Hrsg. Peter Zoche, Stefan Kaufmann und Rita Haverkamp, 21-28. Bielefeld: Transcript.

Schneckener, Ulrich. 2003. *Irak und Terrorismus. Was verbindet „Schurkenstaaten" mit Terroristen?*, SWP-Aktuell 5, Februar 2003. Berlin: Stiftung Wissenschaft und Politik.

Schneckener, Ulrich. 2006. *Transnationaler Terrorismus*. Frankfurt a. M.: Suhrkamp.

Schneckener, Ulrich. 2008. Warum lässt sich Terrorismus nicht „besiegen"? Herausforderungen und Leitlinien für die Terrorismusbekämpfung. In *Vom Rechtsstaat zum Präventionsstaat*, Hrsg. Stefan Huster und Karsten Rudolph, 25-44. Frankfurt a. M.: Suhrkamp.

Schneckener, Ulrich. 2010. Dealing with Armed Non-State Actors in State- and Peacebuilding. Types and Strategies. In *Transnational Terrorism, Organized Crime and Peacebuilding*, Hrsg. Wolfgang Benedek, Christopher Daase und Petrus Van Duyne, 229-248. London: Palgrave Macmillan.

Stern, Jessica. 1998. *The Ultimate Terrorists*. Cambridge: Harvard University Press.

Strohschneider, Stefan. 2011. Technisierungsstrategien und der Human Factor. In *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*, Hrsg. Peter Zoche, Stefan Kaufmann und Rita Haverkamp, 161-178. Bielefeld: Transcript.

Waldmann, Peter. 1998. *Terrorismus. Provokation der Macht*. München: Gerling Akademie Verlag.

Autorenangaben:

Prof. Dr. Ulrich Schneckener,
Universität Osnabrück, Fachbereich Sozialwissenschaften, Seminarstraße 33,
49069 Osnabrück,
ulrich.schneckener@uni-osnabrueck.de