Von strategischer Vulnerabilität zu strategischer Resilienz

Die Herausforderung zukünftiger Sicherheitsforschung und Sicherheitspolitik

von Herfried Münkler und Felix Wassermann,
Humboldt-Universität zu Berlin, 2012

Erscheint in: Lars Gerhold/Jochen Schiller (Hg.), Perspektiven der Sicherheitsforschung. Beiträge aus dem Forschungsforum Öffentliche Sicherheit, Frankfurt/M. 2012: Peter Lang, S.77–95.

Mit dem Ende des Ost-West-Konflikts ist die unmittelbare Bedrohung Deutschlands, präziser: der beiden deutschen Staaten, verschwunden. Aber das Verschwinden der unmittelbaren Bedrohung ist nicht gleichbedeutend mit dem Ende der Unsicherheit. Die Gefährdungsszenarien sind vielmehr diffus geworden, und sie verändern sich in einem Tempo, das die je getroffenen sicherheitspolitischen Maßnahmen mit derselben Geschwindigkeit veralten lässt. Unter diesen Umständen ist es nicht mehr sinnvoll, Sicherheitsforschung und Sicherheitspolitik an einzelnen, aktuell identifizierten, freilich eher potenziellen als konkreten Bedrohungen auszurichten. Stattdessen haben sie sich an Indikatoren der eigenen Verwundbarkeit zu orientieren. Vulnerabilität ist die Schlüsselkategorie in gegenwärtigen Sicherheitsüberlegungen und Zukunftsprognosen.

Statt auf eigene Stärken und Schwächen im Verhältnis zu einem Gegner zu fokussieren oder Bedrohungen auf ihre Eintrittswahrscheinlichkeit und ihr Schadenspotenzial hin zu kalkulieren, erlaubt es die Kategorie der Vulnerabilität, im Bewusstsein der Unvorhersehbarkeit und Unvorhersagbarkeit konkreter Gefährdungslagen die zentralen Verwundbarkeiten eines politischen Systems bzw. einer gesellschaftlichen Ordnung zu identifizieren. Vulnerabilitätsanalysen nehmen dabei von einer Außenperspektive aus die möglichen Eintrittspforten, Schadens- und Folgewirkungen antizipierter, oder besser: imaginierter Gefährdungen des als verwundbar vorgestellten politischen und gesellschaftlichen Körpers in den Blick, und zwar unabhängig davon, ob diese Gefährdungen ursächlich primär auf Umweltereignisse, wie z. B. Naturkatastrophen, auf Systemereignisse, wie z. B. das Versagen bzw. den Ausfall komplexer technischer Anlagen, oder auf durch strategische Gegner absichtlich herbeigeführte Schädigungsereignisse, wie z. B. Terroranschläge zurückgeführt werden (Perrow, 2011). Mit der Kategorie der Vulnerabilität werden dementsprechend unterschiedliche Verletzungsursachen zusammengefasst und, so etwa im „Grünbuch Öffentliche Sicherheit“ (Reichenbach et al., 2008) oder im „Vierten Gefahrenbericht“

der Schutzkommission beim Bundesministerium des Innern (2011), der Aufmerksamkeit der Bundesregierung empfohlen. Diese erkennt ihrerseits in ihrer „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ die „gesellschaftliche Verletzlichkeit aufgrund des zunehmenden Durchdringungs- und Abhängigkeitsgrades nahezu sämtlicher Lebensbereiche mit und von Kritischen Infrastrukturen“ (BMI 2009, S. 5) an und hebt mit der „terroristischen Bedrohung“ sowie den „wachsenden Naturgefahren“ (BMI 2009, S. 10) zwei Hauptursachen möglicher Verletzungen hervor. Die Kategorie der Vulnerabilität, die in ihrer unspezifischen Offenheit die Vielfalt solcher Ursachen umfasst, entspricht damit der diffusen (Un-)Sicherheitslage zu Beginn des 21. Jahrhunderts, deren Bewältigung gleichfalls nach unspezifischen und flexiblen Maßnahmen zur Steigerung gesellschaftlicher Widerstandsfähigkeit bzw. Resilienz verlangt.

Wenn hier *strategische* Vulnerabilität und *strategische* Resilienz ins Zentrum der Betrachtung gerückt werden, so liegt dem die Annahme zugrunde, dass es trotz der vergleichbaren Verletzungsfähigkeit natürlicher, systemischer und menschlicher Verletzungsursachen für die Analyse von – und den Umgang mit – Verwundbarkeiten von Bedeutung ist, ob eine Gefährdung prinzipiell, wenn auch nicht in jedem Fall konkret, einem Gefährder in Gestalt eines rationalen, intentionalen und lernfähigen, sprich: eines *strategischen* Gegenakteurs zugerechnet werden kann (und wird) oder nicht. So ist etwa ein mehrtägiger, flächendeckender Stromausfall, wie ihn das Schneechaos im Dezember 2005 im Münsterland verursachte, grundsätzlich von einem nur auf den ersten Blick identischen Szenario zu unterscheiden, in dem der Zusammenbruch der Stromversorgung auf einen Terroranschlag zurückzuführen ist: Selbst wenn in beiden Szenarien dieselben Verwundbarkeiten derselben „Kritischen Infrastruktur“ betroffen sind und es zudem zu denselben Schäden und Folgewirkungen kommen mag, worauf das inhaltlich offene Vulnerabilitätskonzept abstellt, so ist es für die Analyse, Vorbeugung sowie Nachsorge dieser Gefahrenlagen doch bedeutsam, ob in ihnen Schwachstellen lediglich *offengelegt* oder aber strategisch *ausgenutzt* werden.[1] Zum besseren Verständnis dieses Unterschieds soll hier die jüngere Vulnerabilitäts- und Resilienzdiskussion um eine strategische Perspektive erweitert werden, die das Handeln und Gegenhandeln entweder wechselseitig oder einseitig vulnerabler, also symmetrischer oder asymmetrischer Akteure in den Mittelpunkt stellt. Ausgehend von der analytischen Umorientierung von Bedrohung zu Vulnerabilität (Kapitel 1) werden die Herausforderungen betrachtet, die *strategische* Vulnerabilität mit sich bringt (Kapitel 2), um vor deren Hintergrund

1 In begrifflichen Studien zum Konzept der Vulnerabilität wird diese Unterscheidung zumeist nur implizit getroffen, so etwa bei Lenz (2009, S. 32), die den gefahrenspezifischen Charakter von Vulnerabilität betreffend betont, dass „ein Risikoelement eine unterschiedlich hohe Verletzbarkeit gegenüber unterschiedlichen Gefahren besitzen“ kann, ohne jedoch *strategische* Schlüsse hieraus zu ziehen. Für eine *strategische* Analyse und Simulation der Vulnerabilität kritischer Infrastrukturen am Beispiel des Internet siehe hingegen Fischer (2007).

strategische Resilienz als angemessene Reaktion auf strategische Vulnerabilität zu beschreiben (Kapitel 3) und deren Paradoxien ins Auge zu fassen, vor denen Sicherheitsforschung und Sicherheitspolitik in Zukunft stehen werden (Kapitel 4).

1. Von der Bedrohung zur Vulnerabilität

Die analytische Umorientierung von Bedrohung zu Vulnerabilität entspricht einer veränderten Wahrnehmung von „Sicherheit und Risiko“ (Münkler et al., 2010) in der „Weltrisikogesellschaft“ (Beck, 2007) des 21. Jahrhunderts. Vor allem zwei Problemkomplexe, die miteinander zusammenhängen, rücken dabei ins Zentrum der Aufmerksamkeit: Zum einen die zunehmend diffuse, durch Asymmetrien gekennzeichnete sicherheitspolitische Bedrohungslage nach dem Ende des Ost-West-Konflikts (Münkler, 2006), zum anderen die erhöhte Störungs- und Verletzungsanfälligkeit hochkomplexer moderner Industriegesellschaften im Bereich insbesondere ihrer „Kritischen Infrastrukturen“ (Kloepfer, 2010; Birkmann et al., 2010; Petermann et al., 2011). Bezieht die erste dieser Diagnosen sich zunächst vor allem auf veränderte Ursachen bzw. Verursacher äußerer Verletzungen des politischen Körpers, so betrifft die zweite Veränderungen im Inneren dieses Körpers, und zwar insbesondere solche, die für die Wirkungsweise und die Konsequenzen von Verletzungen bedeutsam sind. Die Kategorie der Vulnerabilität, die beide Perspektiven, also die auf Verletzungsursachen und die auf Verletzungsfolgen, miteinander verbindet, unterläuft dabei die Unterscheidung zwischen „äußerer“ und „innerer Sicherheit“, nach der der Schutz vor äußeren Verletzungen bislang der äußeren Sicherheitspolitik, die Sorge um die innere Verfassung des politischen Körpers hingegen der inneren Sicherheitspolitik überantwortet werden konnte und musste. Die Umstellung von Bedrohung auf Vulnerabilität verschafft der Sicherheitsforschung und Sicherheitspolitik damit jene Flexibilität, die nach dem Ende der symmetrischen Konfrontation des Ost-West-Konflikts und angesichts der gestiegenen inneren Störungs- und Verletzungsanfälligkeit moderner Gesellschaften nötig geworden ist, um auf plötzlich auftauchende asymmetrische Herausforderungen reagieren zu können.

Unter der Bedingung einer symmetrischen Konfrontation stand die Analyse und Evaluation konkreter Bedrohungen im Zentrum einer Sicherheitspolitik, die im Wesentlichen als Verteidigungspolitik konzipiert war. Sicherheit wurde im Falle einer identifizierbaren Bedrohung durch die Herstellung von Verteidigungsfähigkeit nach außen generiert, und die Sicherstellung von Verteidigungsfähigkeit war die Aufgabe des Militärs. Mit dem Wegfall bzw. der Relativierung einer symmetrischen Bedrohung hat der Verteidigungsgedanke an Bedeutung verloren und ist in dem sehr viel allgemeineren Begriffskonzept von Sicherheit aufgegangen. Zwar ist gelegentlich auch von asymmetrischen Bedrohungen die Rede, was aber nur dann einen Sinn ergibt, wenn sich

die Herausforderung durch asymmetrische Konstellationen zu einer konkreten, identifizierbaren Bedrohung verdichtet hat. Das aber ist für asymmetrische Herausforderungen untypisch, insofern diese auf eine „Entspiegelbildlichung“ der potenziellen Konfrontation hinauslaufen. Ein grundsätzlich verschiedener Zugriff auf Raum und Zeit spielt dabei die Hauptrolle, daneben der Verzicht auf eine wie auch immer geartete militärische Professionalisierung der Gewaltanwendung, so dass es kaum möglich ist zu antizipieren, aus welcher Richtung und in welcher Form ein Angriff erfolgen könnte. Es ist unter den Bedingungen asymmetrischer Herausforderung darum angezeigt, von der Analyse möglicher *Bedrohungen* zu einer Analyse der eigenen *Vulnerabilität* überzugehen. An die Stelle der Herausforderung von außen tritt die systematische Suche nach eigenen Schwächen und Defiziten, die minimiert werden müssen, um die Verletzlichkeit für asymmetrische Angriffe zu begrenzen. Aus der Analyse der eigenen Verwundbarkeit und einer entsprechenden Vorsorge erwächst so eine erhöhte Abwehrfähigkeit gegenüber asymmetrischen Herausforderungen, gleich welcher Art diese sein mögen. Im Kern läuft diese Umstellung der Analyse von Bedrohung auf Vulnerabilität auf einen relativen Bedeutungsverlust des Militärs im sicherheitspolitischen Portfolio der Staaten hinaus.

Durch die Wendung des Blicks von außen nach innen, die mit dem Vulnerabilitätskonzept vollzogen wird, geraten die störungsanfälligen Schwachstellen hochkomplexer Industriegesellschaften ins Zentrum der Sicherheitsanalyse. War die klassische Verletzlichkeit von Territorialstaaten eine des Raumes, der gegen Angriffe von außen verteidigt werden musste, so hat inzwischen die Verwundbarkeit politischer Akteure infolge des hohen Sicherheitsbedürfnisses der Zivilbevölkerung, durch die leicht zu attackierenden Transport- und Versorgungssysteme moderner Gesellschaften und vor allem durch die Angreifbarkeit ihrer elektronischen Steuerungssysteme an Bedeutung gewonnen. An die Stelle der herkömmlichen Raumverteidigung ist die Abwehr von Terroranschlägen und Cyberattacken getreten, bei denen zunächst unklar bleibt, wer der Angreifer ist und welche Absichten und Ziele ihn leiten. Die jüngere Sicherheitspolitik hat es in wachsendem Maße mit dem Problem der Anonymität bzw. Maskierung der Angreifer zu tun. Es ist daher unmöglich, auf solche Angriffe mit einer Gegenoffensive zu reagieren, zumal die Angreifer, wenn man sie denn zu identifizieren vermag, nicht in einem territorial geschlossenen Gebiet versammelt sind, sondern aus der Tiefe der sozialen Räume heraus agieren. Militärische Fähigkeiten haben dementsprechend bei der Abwehr solcher Angriffe relativ an Bedeutung verloren. Angriffen in Form von Angsterzeugung und Störungen der Steuerungssysteme lässt sich mit Strategien der Raumnahme kaum effektiv begegnen. Überhaupt ist eine prompte offensive Reaktion unmöglich, weswegen vor allem die Abwehrfähigkeiten gestärkt und Strukturen verminderter Verwundbarkeit hergestellt werden müssen. Unter dem Begriffskonzept der Resilienz

versammeln sich entsprechende Erwartungen, die auf allgemeine gesellschaftliche Widerstandsfähigkeit statt auf bedrohungsspezifische Verteidigungs- und Schutzfähigkeit abzielen. Vulnerabilität und Resilienz treten so an die Stelle älterer Begriffspaare, wie Bedrohung und Abschreckung, Angriff und Verteidigung, mit denen in symmetrischen Konstellationen Sicherheitspolitik beschrieben und betrieben worden ist.

Mit dem Bedeutungsverlust jener älteren Konzepte geht in der jüngeren Diskussion über Vulnerabilität ein Bedeutungsverlust des Konzepts eines strategischen Gegenakteurs einher. Da unter Bedingungen der Asymmetrie nicht abzusehen ist, welcher bzw. was für ein Akteur in Zukunft zur tatsächlichen Bedrohung bzw. zum Gegner werden könnte und da bis zu dem Zeitpunkt, an dem sich dies zeigt, zudem auch verborgen bleibt, welche Verwundbarkeiten dieser Gegner mit welchen Absichten und Strategien auszunutzen strebt, verliert das Konzept des strategischen Gegenakteurs klare Konturen und konkreten Inhalt – und damit (vermeintlich) seine Relevanz für die Sicherheitspolitik. Diese Ausblendung von Gegenakteuren scheint auch jenen Problemstellungen geschuldet, zu deren Bearbeitung das Vulnerabilitätskonzept, das der Sicherheitsdiskurs erst in jüngster Zeit für sich entdeckt, ursprünglich im ökologisch-geografischen Kontext entwickelt wurde: der Verwundbarkeit von Gesellschaften durch gefährdende Ereignisse bzw. Prozesse (*Hazards*) in ihrer natürlichen Umwelt, wie sie insbesondere dem Klimawandel zugeschrieben werden (Turner et al. 2003; Wisner et al., 2004; Birkmann, 2006; Bohle & Glade, 2008).[2] In dem Maße, in dem der erweiterte Sicherheitsdiskurs das Vulnerabilitätskonzept übernimmt und unter diesem nichtintendierte *sowie* intendierte Gefährdungen subsumiert, hat dieses Konzept – spiegelbildlich zum erweiterten Sicherheitsbegriff – ein immer größeres Maß an Heterogenität und Komplexität zu inkludieren, was es mit einem Verlust an Analyseschärfe zu begleichen hat. So tritt die Frage danach, welcher Art die Ereignisse sind, die potenzielle Verwundbarkeiten in tatsächliche Wunden verwandeln (könnten) – ob es sich hier um unintendierte Natur- bzw. Ökosystemereignisse oder aber um intendierte Schädigungsereignisse handelt –, zugunsten des Abtastens des politischen Körpers auf seine ereignis- und gefährdungsübergreifende Verwundbarkeit hin zurück. Das Erdbeben, der Atomunfall und die Cyberattacke erscheinen in dieser Vulnerabilitätsperspektive vor allem als funktionale (bzw. dysfunktionale) Äquivalente, deren Äquivalenz sich aus ihren verletzenden Folgen ergibt. Dass Maßnahmen zur Vorbeugung oder Bewältigung solcher Verletzungen, gleichgültig ob auf dem Gebiet der Gebäude-,

2 In der ökologisch-geografischen Diskussion konkurrieren vielfältige Konzepte der Vulnerabilität miteinander. Thywissen (2006) listet allein 29 unterschiedliche Definitionen auf, denen zumeist gemeinsam ist, dass sie ihrem Gegenstand entsprechend auf den Aspekt eines strategischen Gegenakteurs verzichten. Für eine Vermittlung zwischen dem (akteursfreien) geografischen und dem (akteursbezogenen) strategischen Vulnerabilitätsdiskurs plädiert unter dem Eindruck der Anschläge vom 11. September 2001 Cutter (2003).

Energie- oder der Internetsicherheit, in ihrer Wirkung davon abhängen könnten, ob mit dem Gegenhandeln eines rationalen, intentionalen, lernfähigen, sprich: eines *strategischen* Gegenakteurs zu rechnen ist und gerechnet wird, darauf macht die Kategorie der *strategischen* Vulnerabilität aufmerksam.

2. Strategische Vulnerabilität als Herausforderung

Der Begriff der *strategischen* Vulnerabilität hebt den Aspekt des Gegenhandelns eines strategischen Akteurs hervor, einen Aspekt also, der in ökologisch- und technisch-systemischen Vulnerabilitätsanalysen vernachlässigt werden kann, der das Nachdenken über Verwundbarkeit aber seit jeher begleitet. So verdankt das Vulnerabilitätskonzept seine Metaphorik und Plausibilität denn auch nicht allein der jüngeren Diskussion über die Folgen des Klimawandels, sondern kann daneben aus einer zweiten, älteren Quelle schöpfen. Diese ältere Quelle liegt im strategischen Denken selbst begründet, das als solches seit jeher eigene *und* gegnerische Verwundbarkeiten im Kontext wechselseitiger Verletzbarkeit *und* Verletzungsfähigkeit, also Vulnerabilität *und* Vulneranz zu identifizieren strebt. So zielt die *Strategie* als (Lehre vom) Handeln *und* Gegenhandeln in einem Feld der Paradoxie (Luttwak, 2003) einerseits darauf ab, *defensiv* die eigene Vulnerabilität zu erkennen, sie möglichst zu verringern und vor der Ausnutzung durch den Gegner, sprich: vor seiner Vulneranz zu schützen, andererseits zugleich aber auch darauf, *offensiv* die gegnerische Vulnerabilität zu enttarnen, sie möglichst zu vergrößern und strategisch unter Anwendung der eigenen Vulneranz auszunutzen. Dieses *strategische* Vulnerabilitätsverständnis entwickelten nicht erst die Analytiker der im anbrechenden Luftkriegszeitalter neu perspektivierten territorialen Vulnerabilität.[3] Vielmehr haben Rüstungsanstrengungen und Strategieplanungen seit jeher das Ziel, die eigene Vulnerabilität zu minimieren sowie die des Gegners zu maximieren und dabei zugleich die eigene Vulneranz zu maximieren und die des Gegners zu minimieren. Das Ideal entsprechender Anstrengungen besteht demnach in vollständiger Invulnerabilität, aus deren Deckung heraus die Vulneranz ungehindert ihre maximale Wirkung entfalten kann. Dieses Ideal leitet bis hin zur US-amerikanischen Vision einer technologie- und netzwerkgestützten *Zero Casualties*-Kriegführung die Sicherheits- und Rüstungspolitik strategischer Akteure an.

3 Zur Formierung des Diskurses „Kritische Infrastrukturen“ in italienischen und US-amerikanischen Luftkriegstheorien vor dem Zweiten Weltkrieg siehe Kaufmann (2010, S. 109): „Avancierten Städte und Infrastrukturen zum lohnenden Angriffsziel, so sah sich die Verteidigung gezwungen, das eigene Land aus der Perspektive des Angreifers zu betrachten. Mit der Umkehr des Blicks entdeckte man die eigene Verwundbarkeit, das eigene Territorium erscheint nun als eine Ansammlung lohnender Ziele.“ Ähnlich führt Dombrowsky (2008, S. 64) „die Anfänge der US-amerikanischen Katastrophenforschung“ auf die *Strategic Bombings Surveys* zurück, mit denen die USA in den Jahren 1944–1947 die verletzbaren Nervenstränge und Infrastruktur-Knotenpunkte auf dem gegnerischen sowie eigenen Territorium zu entdecken suchten, deren gezielte Bombardierung die größte Schadenswirkung versprach bzw. befürchten ließ. Für Vulnerabilitätsstudien aus diesem Kontext siehe exemplarisch Coale (1947) sowie Kaysen (1953).

In mythischen Bildern der Unverwundbarkeit fand dieses Ideal seine narrative bzw. ikonische Verdichtung: Achill als im Zweikampf unbesiegbarer Held erscheint ebenso unverwundbar wie Siegfried, der im Drachenblut badete. Beide Helden haben jedoch ihre Schwachstellen, ihre eigenen Vulnerabilitäten: Achilles' Ferse bzw. Siegfrieds Stelle zwischen den Schultern, an der beim Bade das Lindenblatt klebte. Die strategische Pointe bzw. Lehre dieser Bilder kann darin gesehen werden, dass die beiden Helden an ihren Schwachstellen nur zu treffen sind, wenn sie fliehen würden – doch genau das tun sie nicht. So sind sie auf direktem Weg mittels Frontalangriffen nicht zu verwunden, was ihr tragisches Ende aber dennoch nicht zu verhindern vermag: Im Fall des Achill war die Fernwaffe Pfeil und Bogen tödlich, im Falle Siegfrieds die vertrauensselige Geschwätzigkeit seines Weibes. Phoebus Apoll, der den Pfeil des Paris lenkt, und Hagen, der seinen Speer Siegfried in den Rücken rammte, als dieser vertrauensselig nach einem Wettlauf an einer Quelle kniete, um seinen Durst zu löschen, haben also die entscheidende Stelle der Verwundbarkeit gefunden. Mit der Einsicht in die Verwundbarkeit der vermeintlich Unverwundbaren speichern und tradieren diese mythischen Bilder somit einen strategischen Wissensbestand, den sich die USA nach dem Ende des Kalten Krieges in einem schmerzhaften Lernprozess (wieder) anzueignen hatten: dass vollständige Unverwundbarkeit in einem strategischen Kontext kaum jemals zu erwarten bzw. zu erreichen – und daher auch nicht anzustreben – sei.[4] Die Mahnung der Erzählungen von Achill und Siegfried, dass auch der vermeintlich Unverwundbare verwundbar sei, sofern sein Gegner die Verwundbarkeit nur entdeckt, verstanden strategische Akteure dabei zumeist als Appell, die eigenen und zudem auch die gegnerischen Verwundbarkeiten sowie Verwundungsfähigkeiten zu entdecken, um entsprechende Entdeckungen sodann in offensive und defensive, aktive und reaktive strategische Entscheidungen und Programme zu überführen. Die Strategie- und Kriegsgeschichte kann in diesem Sinne als eine Abfolge der Entdeckungen auf der Suche nach der jeweils optimalen Kombination aus Invulnerabilität und Vulneranz gelesen werden. Dabei erwies sich weniger das Abklopfen der gegnerischen Front auf mögliche Schwachstellen hin als vielversprechend, sondern eher die Suche nach Einbruchstellen, an denen der Gegner keine Front hat bzw. keine Front aufbauen konnte. So zielte das von Churchill favorisierte amphibische Angriffsunternehmen von Gallipoli auf den „weichen Unterleib" der Mittelmächte (Wolf, 2008), und auf ähnliche Weise entdeckte Mao Zedong mit seinem Konzept des Partisanenkrieges Raum und Zeit als strategische Ressourcen der Schwachen, gegenüber denen die Starken verwundbar sind: „Irreguläre gewinnen, wenn sie nicht verlieren, Reguläre verlieren, wenn sie nicht gewinnen", so fasste

4 Stellvertretend für die nach dem Ende des Ost-West-Konflikts zeitgleich mit dem Aufstieg der USA zur imperialen Macht einsetzende Reflexion über die Verwundbarkeit des Imperiums siehe Kupchan (1994).

Henry Kissinger unter dem Eindruck des Vietnamkriegs die strategische Vulneranz der Partisanen und die Vulnerabilität der regulären Streitkräfte zusammen. Unter dem Gesichtspunkt der Entdeckung und Nutzung gegnerischer Vulnerabilität zeichnen diese Strategien sich dadurch aus, dass mit ihnen nicht etwa nach einer Schwachstelle gesucht wird, sondern vielmehr die Stärke des Gegners in Schwäche verwandelt bzw. die unter der Stärke verborgenen Schwachstellen herausgefunden und ausgenutzt werden. Strategische Wirkung entfalten solche Strategien der Ausnutzung von Vulnerabilität insbesondere dann, wenn sich der Gegner für unverwundbar hält und dementsprechend keine Abwehrvorbereitungen trifft. In Gestalt des von Odysseus listig ersonnen Trojanischen Pferdes fand auch dieser strategische Wissensbestand Eingang in die mythische Bilderwelt: Odysseus, der die strategische Vulnerabilität Trojas in der Frömmigkeit seiner Bewohner erkennt, präsentiert ihnen das Trojanische Pferd als eine göttliche Opfergabe, um sie damit in ein strategisches Dilemma aus zwei miteinander konkurrierenden Verwundbarkeiten zu verstricken: das Dilemma zwischen der Verwundbarkeit gegenüber der Göttin Athene, deren Zorn die Trojaner zu fürchten haben, wenn sie das ihr geweihte Opfergeschenk ablehnen, und der Verwundbarkeit gegenüber der Kriegslist der Griechen, vor der die Seherin Kassandra vergeblich warnt. Die Trojaner, die sich für die Minimierung der Verwundbarkeit gegenüber der Göttin entscheiden, öffnen dadurch ihrer Verwundung durch die griechische Kriegslist das (Stadt-)Tor: Durch dieses ziehen sie die Griechen, die im Bauch des hölzernen Pferdes versteckt sind, in die Stadt hinein (Münkler, 1990, S. 78ff.). Das Schicksal der Trojaner ist damit besiegelt.

Bemühungen um Minimierung von Verwundbarkeit sind freilich nicht immer, wie im Fall Trojas, zum Scheitern verurteilt. Vielmehr brachte die Kriegsgeschichte vielfältige erfolgreiche Methoden und Innovationen der Vulnerabilitätsminimierung hervor, darunter insbesondere solche der *Panzerung*, die allerdings nicht beliebig gesteigert werden kann: Ein Übermaß von Panzerung macht den Kämpfer zugleich schwer und unbeweglich und verringert so seine offensive Kampfkraft. Eben dies war die Erfahrung der Ritterschaft, die feststellen musste, dass die Panzerung, die beim Stoßangriff gegen ebenfalls gepanzerte Ritter von Vorteil war, in der Konfrontation mit leichter Reiterei zum Nachteil wurde bzw., wie in der Schlacht von Azincourt gegen die britischen Langbogner, wenig half.[5] Zudem hat die Vulnerabilitätsverminderung qua Panzerung auch weitreichende Folgen für das Ressourcenregime: sie ist kostspielig und zeitaufwendig und kann schon aus diesem Grund nicht beliebig gesteigert werden. Als Alternative

5 Ein Beispiel für die Niederlage schwergepanzerter Ritter gegen hochbewegliche leichte Reiterei, zumal unter klimatischen Bedingungen, die letztere begünstigten, ist die Schlacht von Hattin am 4. Juli 1187 (Hoch 2002). Zur Niederlage des französischen Ritterheeres gegen die Engländer vgl. die berühmte Darstellung bei Keegan (1978, S. 89–134), zu den anschließenden Lernprozessen vgl. Kortüm (2004).

zur Panzerung bietet sich daher *erhöhte Beweglichkeit* an, die aber prinzipiell nur dort gegeben ist, wo man auf eine feste logistische Basis verzichtet, weil diese zur Verteidigung eines Ortes zwingt und damit immobilisiert. Napoleon war ein Meister dieser schnellen und beweglichen Kriegführung, mit der er bei seinem Feldzug in Russland (1812) jedoch an eine Grenze stieß, als die Russen durch eine Strategie der verbrannten Erde die Vorzüge der Beweglichkeit begrenzten und ebenso beweglich agierten wie Napoleon. Aufgrund der jeweiligen Nachteile, die aus der Maximierung von Panzerung oder Beweglichkeit resultieren, erscheint es naheliegend, beide Methoden der Verringerung von Vulnerabilität miteinander zu kombinieren, um diese Schwächen zu vermeiden. Entsprechende Bemühungen führen unter Bedingungen der Symmetrie zu Wettläufen um die optimale Kombination, ein Beispiel hierfür ist etwa der Schlachtschiffbau vor dem Ersten Weltkrieg. Allerdings verändern sich solche symmetrischen Konstellationen, sobald eine Seite ihre Verwundbarkeit durch Unsichtbarkeit minimiert: Invisibilität schafft Invulnerabilität, und die mythische „Figur“, die diese strategische Beobachtung zum Bild verdichtet, ist die der Tarnkappe, als deren moderne Variante der Tarnkappenbomber und in mancher Hinsicht auch die Drohne angesehen werden kann. Das Streben nach Invisibilität zeigt sich kriegshistorisch etwa in der Geschichte des U-Boot-Einsatzes: Die für Invasoren ursprünglich unangreifbare (unverwundbare) Insel England wurde dadurch verwundbar, dass die Hochseeflotte der Briten aufgrund des U-Boot-Einsatzes der Deutschen zeitweilig die Versorgung und den Ressourcenzufluss nicht mehr gewährleisten konnte. Erst die Entwicklung von Techniken zur Minimierung der Verwundbarkeit von Handelsschiffen durch deren Zusammenfassung zu Geleitzügen oder aber zur Sichtbar- bzw. Hörbarmachung der zunächst unsichtbaren und lautlosen Bedrohung (Sonar) führte zur Minimierung der neu entstandenen Verwundbarkeit.

Sind solche Spiralen der Auf- und Nachrüstung zum Zweck der Minimierung eigener und Maximierung gegnerischer Vulnerabilität für symmetrische Konstellationen kennzeichnend, in denen die rüstungspolitischen und strategischen Anstrengungen der sich wechselseitig beobachtenden und nachahmenden Gegner in die gleiche Richtung zielen, so ist dies unter den Bedingungen der Asymmetrie gerade nicht der Fall. Stattdessen hat die Ungleichartigkeit und wechselseitige Unberechenbarkeit der Parteien hier zur Folge, dass Unverwundbarkeit in unterschiedlichen Richtungen gesucht wird. So generieren etwa Terrornetzwerke innovative Formen der Panzerung, der Mobilität und der Invisibilität gerade nicht aus technologischer Nachahmung, sondern aus organisatorischer und strategischer Kreativität. Der technologiegestützte Drohnenangriff findet somit im Selbstmordattentat, das sich unvorhersehbar und plötzlich an unbekanntem Ort aus der Anonymität des sozialen Untergrunds heraus ereignet, seinen asymmetrischen Widerpart, der auf *andere* Weise als dieser Invulnerabilität mit Vulneranz

kombiniert. Die Suche nach der optimalen Kombination setzt unter Bedingungen der Asymmetrie also jenen Eskalationsprozess in Gang, den Carl von Clausewitz (2002) in seinem Buch „Vom Kriege“ mit drei Tendenzen „zum Äußersten“ beschrieben hat. Sah Clausewitz diese eskalierenden Tendenzen noch durch solche der Mäßigung abgeschwächt, die darauf beruhen, dass die Gegner im wirklichen Krieg einander nie völlig fremd – und daher auch nicht absolut feindlich – sind, so scheint unter Bedingungen der Asymmetrie aufgrund der Unsichtbarkeit der Akteure letzteres wahrscheinlicher zu werden: Mit der Ungleichartigkeit steigt die Unsicherheit bezüglich der Absichten und Fähigkeiten des Gegners, und es gewinnen die eskalierenden gegenüber den moderierenden Tendenzen die Oberhand. Die klassischen symmetriebezogenen Theorien zur Logik der Abschreckung einerseits und der Rüstungsbegrenzung andererseits verlieren dadurch offensichtlich an Plausibilität und Relevanz, beruht bei ihnen doch die Genese reziproker Sicherheit auf der Herstellung reziproker Vulnerabilität und dem beiderseitigen Verzicht auf deren Schließung etwa durch Raketenabwehrsysteme ballistischer Art. Diese Logik scheint in asymmetrischen Konstellationen nicht zu greifen, da allein unter Bedingungen der Symmetrie die Verwundbarkeit des Gegners angesichts der eigenen Verwundbarkeit zu einem Generator von Vertrauen und Garanten von Vernünftigkeit und Verlässlichkeit werden kann.

Bei der Entstehung der europäischen Territorialstaaten war eine derartige Entwicklung zu beobachten: Die Bildung eines *Body Politic* im Sinne von Territorium und Bevölkerung bedeutete hier, dass der souveräne Wille bzw. der Wille des Souveräns sich ebenso äußerte wie gleichzeitig angreifbar, also: verwundbar wurde, was unter Bedingungen der Asymmetrie gerade nicht der Fall ist. Dort treten entterritorialisierte politische Akteure ohne eindeutig identifizierbaren Körper (wieder) auf, die gänzlich anderen Vulnerabilitätsregimen als Staaten unterliegen. Nicht ohne Grund ging der neuzeitliche Staat konsequent gegen die Netzwerke vor, die sich in Gestalt von Ritterorden und Kaufmannshansen noch gegen Philipp den Schönen zu behaupten versuchten. Mit Blick auf die Rückkehr nichtstaatlicher Netzwerke und „unsichtbarer“ strategischer Akteure auf die Bühne der (Un-)Sicherheit im 21. Jahrhundert stellt sich also die Frage, inwiefern nicht nur die klassischen Theorien der Abschreckung bzw. Vertrauensgenerierung, sondern mit diesen das strategische Wissen über strategische Vulnerabilität *insgesamt* seine Anschlussfähigkeit verliert oder bereits verloren hat. Will die Sicherheitsforschung auf die Einsichten jenes strategischen Wissens nicht ganz verzichten, so hat sie dieses den veränderten, asymmetrischen Bedingungen anzupassen. Das Leitbild „strategische Resilienz“ kann als Versuch bzw. Ergebnis solcher Anpassungen betrachtet werden, da sich in ihm das strategische Wissen über die Dialektik und Dynamik von Handeln und Gegenhandeln verwundbarer Akteure mit den vom jüngeren

Vulnerabilitäts- und Resilienzdiskurs herausgestellten Überlegungen zur Widerstandsfähigkeit moderner Gesellschaften verbindet.[6]

3. Von strategischer Vulnerabilität zu strategischer Resilienz

Im jüngeren Sicherheitskontext bezeichnet die Kategorie der Resilienz „die Widerstandsfähigkeit von Organismen und Systemen", also deren Fähigkeit, „sich geeignet, d. h. durch die Kombination von Wissen, Fertigkeiten und mobilisierbaren Ressourcen, vor extremen Belastungen, Widrigkeiten oder Schadwirkungen schützen und dadurch ihre Vitalfunktionen länger aufrechterhalten zu können" (Reichenbach et al., 2008, S. 52). Zielt diese Definition primär auf den *Schutz* vor Belastungen, Widrigkeiten oder Schadwirkungen – sprich: den Schutz vor Verletzungen – ab, so heben Begrifflichkeiten, die sich enger an die Theorie ökologischer Systeme (Holling, 1973) anlehnen, aus der der Sicherheitsdiskurs das Konzept der Resilienz ursprünglich übernahm, die *Bewältigung* möglicher Verletzungen stärker hervor. Ein ökologisches System gilt in dieser Theorie als resilient, wenn es in einem Umfeld der Veränderungen seinen Fortbestand dadurch sichern kann, dass es diese Veränderungen zu absorbieren vermag. Resilienz erscheint in dieser Perspektive gerade nicht als Synonym, sondern vielmehr als Gegenbegriff zu Stabilität, da der Fortbestand eines Systems unter Bedingungen des Wandels gerade nicht durch die Stabilisierung des Systemzustands, sondern vielmehr durch dessen Flexibilisierung und beständige Anpassung sichergestellt werden kann.[7] Für soziale Systeme und insbesondere komplexe, verwundbare Industriegesellschaften kann das heißen, dass sie, wenn sie sich in einem Umfeld der Ungewissheit und des Wandels der Bedrohungslage zu behaupten suchen, auf plötzliche, unerwartete, überraschende Veränderungen bzw. Gefährdungen vorbereitet zu sein haben, was durch flexible Bewältigungsmaßnahmen besser als durch stabile Schutz- und Panzerungsbemühungen gelingt. An die Stelle des Ideals der Invulnerabilität tritt hier also die Einsicht in die Unvermeidlichkeit von Vulnerabilität, an die Stelle der Methode des Schutzes jene der Bewältigung und an die Stelle des Sicherheitsparadigmas ein „Leben mit Risiko" als „neues Paradigma für die Risikowelten von morgen" (Bohle, 2008, S. 435). Resilienz erscheint somit eher als Komplementär- denn als Gegenbegriff zu Vulnerabilität, insofern als gerade verwundbare Systeme wie etwa komplexe Industriegesellschaften darauf angewiesen

6 Im Fall der „strategischen Resilienz" erfolgt die konzeptionelle Anpassung strategischen Wissens an die veränderten asymmetrischen Bedingungen also primär auf Seiten der Defensive, während andere adaptierte Konzepte, wie das der „erweiterten Abschreckung" bzw. *Expanded Deterrence* (Gallucci 2006), das die indirekte Abschreckung terroristischer Netzwerke durch (angedrohte) Angriffe auf deren staatliche Unterstützer thematisiert, eher offensiv (bzw. präventiv) orientiert sind.

7 Die für die weitere Resilienz-Diskussion prägende Definition von Holling (1973, S. 17) lautet: „Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist. In this definition resilience is the property of the system and persistence or probability of extinction is the result."

sind, durch resiliente Strukturen ihre Überlebenschancen in einem Umfeld großer Unsicherheit zu sichern. Der Versuch, diese Unsicherheiten durch eine Maximierung von Sicherheit mit dem Ziel der Unverwundbarkeit zu beantworten, würde entweder zu Lernblockaden oder zu Ressourcenüberforderung führen. Wie im Modell der Panzerung des Ritters angedeutet, gibt es auch hier einen Weg zur Selbstparalyse durch bedingungslose Sicherheitsmaximierung. In diesem Sinn ist Resilienz eine Alternative zum Ziel der Unverwundbarkeit.

Wenn Resilienz die Antwort auf Vulnerabilität bildet, so erscheint es naheliegend, *strategische* Resilienz als Antwort auf *strategische* Vulnerabilität ins Auge zu fassen. Doch was ist mit *strategischer* Resilienz gemeint? Als Untertyp allgemeiner Resilienz, so legt es die hier angestrebte Verbindung der Einsichten des jüngeren Resilienzdiskurses mit denen des überlieferten strategischen Wissen nahe, meint *strategische* Resilienz die Widerstandsfähigkeit eines verwundbaren politischen Systems bzw. einer verwundbaren Gesellschaft nicht gegenüber beliebigen möglichen Verletzungen, sondern gegenüber jenen möglichen Verletzungen, die *durch einen strategischen Gegenakteur* verursacht werden können. Strategische Widerstandsfähigkeit setzt also voraus, dass die resiliente Gesellschaft um ihre prinzipielle Verwundbarkeit gegenüber den verschiedensten Gefährdungen weiß und sie in ihrer jeweils konkreten, sich stets verändernden Ausprägung durch beständiges Abtasten des eigenen Körpers präventiv zu entdecken strebt, um dann mit geeigneten Schutzmaßnahmen darauf reagieren und die Vulnerabilität nach Möglichkeit zu verringern. Zugleich aber ist damit auch gemeint, dass diese Gesellschaft sich der Vergeblichkeit – und Tragik – jedes Strebens nach vollkommener Unverwundbarkeit bewusst ist und daher nicht allein ihren Schutzmaßnahmen vertraut, sondern diese durch Vorkehrungen zur besseren Bewältigung eintretender Verletzungen flankiert. Im Wortsinne *strategisch* resilient ist die betreffende Gesellschaft jedoch erst dann, wenn sie auch die *strategische* Bedeutung ihrer unvermeidbaren Vulnerabilität reflektiert, und das heißt: wenn sie ihre Vulnerabilität im Lichte potenzieller Auseinandersetzungen mit einem (unbekannten) strategischen Gegenakteur evaluiert. Dies setzt ein Verständnis der Dialektik und Dynamik des Handelns und Gegenhandelns strategischer Gegenakteure voraus, deren Fremd- und Selbstbeobachtungen sich bei ihrer *beiderseits* betriebenen Suche nach der optimalen Kombination aus minimierter Vulnerabilität und maximierter Vulneranz überlagern und kreuzen.

Zu diesen allgemeinen Anforderungen an eine „strategisch resiliente“ Gesellschaft treten in dem diffusen und komplexen, von Asymmetrien geprägten (Un-)Sicherheitskontext des 21. Jahrhunderts noch besondere Herausforderungen hinzu. Dazu gehört vor allem die Herausforderung, den sozialen bzw. politischen Körper *aus der Perspektive eines Unbekannten* auf seine Schwachstellen hin abzutasten. Anders als in symmetrischen Konstellationen nämlich

bleiben das Kalkül und die Absichten des (imaginierten) Gegners für die Vulnerabilitätsanalyse hier grundsätzlich vage, sodass sie gewissermaßen blind und im Dunkeln erfolgt. Inwiefern unter diesen Umständen die dem Leitbild „strategische Resilienz“ entsprechende Selbstbeobachtung durch die Brille des strategischen Gegenakteurs gelingen kann und sie zu verwertbaren und substanziellen Resultaten führt, hängt nicht nur von der Fähigkeit zu strategischer Empathie ab, sondern insbesondere auch von der Art der Rationalität, die dem Gegner zu unterstellen ist: Handelt dieser auf der Basis instrumenteller Vernunft, mit der er bei der Planung und Verfolgung seiner Verletzungsabsichten unter Abwägung von Kosten und Nutzen die Zwecke, Ziele und Mittel seiner Verletzungen kalkuliert, so stehen die Chancen, die Tastbewegung der gegnerischen Suche nach den eigenen Schwachstellen rekonstruieren und vorhersagen zu können, besser, als wenn dem Gegenakteur eine nicht primär instrumentelle Rationalität oder gar vollkommene Irrationalität unterstellt werden muss. Allein in letzterem Fall wäre die Gefährdung durch einen völlig unberechenbaren Gegner derjenigen gleichzusetzen, die von einem völlig unabsehbaren Naturereignis ausgeht, da beiden eine *bewusste* Schädigungsabsicht und Schädigungsrationalität nicht unterstellt werden kann, sodass das Konzept des strategischen Gegenakteurs hier – jedoch nur hier – verzichtbar erscheint. Eine derart vollständige Unsicherheit bezüglich der gegnerischen Rationalität ist aber selbst in asymmetrischen Konfrontationen kaum zu erwarten, da auch in deren Verlauf die Clausewitz’schen „Tendenzen der Mäßigung“ wirken, da der zunächst „unbekannte Unbekannte“ (*unknown unknown*) immer mehr zum „bekannten Unbekannten“ (*known unknown*) mutiert: So lässt etwa seine Kampfstrategie in der Auswahl der Orte und Zeitpunkte der Angriffe Muster erkennen, die einer politisch-strategischen Hermeneutik ebenso zugänglich sind wie Bekennerschreiben und Unterstützungsaufrufe, deren Interpretation Rückschlüsse über Ziele und Zwecke, Ressourcen und Adressaten – und letztlich: über die strategische Rationalität des Gegenakteurs – erlaubt. Dies freilich setzt die *strategische* Analyse *strategischer* Vulnerabilität voraus.

Eine zweite spezifisch asymmetriebedingte Herausforderung, die sich mit dem Leitbild „strategische Resilienz“ verbindet, ergibt sich daraus, dass unter Bedingungen der Asymmetrie von dem (imaginierten) strategischen Gegenakteur erwartet werden muss, dass er jede Bemühung um Schließung bzw. Bewältigung strategischer Verwundbarkeit beobachtet oder gar antizipiert, um sie in seine Gesamtstrategie einzukalkulieren und durch diese zu konterkarieren. Anders also als natürliche oder systemisch-technische Gefährdungsursachen, bei denen eine derart reaktionssensitive oder gar antizipative strategische Anpassung an die Reaktionen des Gegners nicht erfolgt, und anders zudem auch als symmetrische Gegenakteure, die sich bei der Formulierung und Anwendung ihrer Strategien reziprozitätsbedingten Restriktionen zu

unterwerfen haben, sind der strategischen Rationalität und Kreativität asymmetrischer Akteure bei ihrem (präventiven) Gegenhandeln keine Grenzen gesetzt. Welche Folgen dies haben kann, zeigt sich etwa in der (jüngst vor allem im Irak zu beobachtenden) Strategie der Anschlags*serie*, mit der – anders als mit synchron koordinierten Angriffen – neben den primären Zielen auch die Bewältigungsbemühungen der angegriffenen Gesellschaft attackiert werden: Wenn nach dem ersten Anschlag die Hilfskräfte und mit ihnen die medialen Berichterstatter eintreffen und die aktiven sowie kommunikativen Bewältigungsmaßnahmen der „resilienten" Gesellschaft anlaufen, führen weitere Einschläge an demselben Ort medienwirksam das Scheitern der Bewältigungsbemühungen und Bewältigungskapazitäten vor Augen – mit dem strategischen Ziel, die kollektive Widerstandskraft bzw. Resilienz der Gesellschaft zu erschüttern. Szenarien, in denen eine solche Eskalation nicht ausgeschlossen werden kann, in denen also rationale, intentionale und lernfähige, sprich: *strategische* Gegenakteure relativ frei von den Restriktionen der Symmetrie reaktionssensibel aus der Unsichtbarkeit heraus zu agieren vermögen, unterscheiden sich grundsätzlich von durch Naturereignisse oder Technikversagen verursachten Katastrophenszenarien einerseits und von symmetrischen Konfrontationen, wie denen des Kalten Krieges, andererseits. Anders als diese Szenarien unterwerfen jene die Sicherheitspolitik dem Zwang zur Reflexivität, dem Zwang also, ihre eigenen Schritte zu „strategischer Resilienz" wiederum aus dem Blickwinkel des (unbekannten) Gegenakteurs und unter dem Gesichtspunkt der Verwundbarkeit zu evaluieren, um mögliche Verletzungen auch in diesem Bereich zu antizipieren. Eine solche stetige Selbstbeobachtung birgt für eine Gesellschaft selbstverständlich die Gefahr, sich im unendlichen Regress präventiver Spekulation zu verlieren. Diesen Regress an geeigneter Stelle zu unterbrechen, um Handlungsfähigkeit herzustellen, ist Aufgabe von Sicherheitspolitik. Sie wird diese Aufgabe freilich nur dann verantwortungsvoll meistern können, wenn sie den von der Strategietheorie aufgezeigten Paradoxien strategischer Vulnerabilität nicht ausweicht, sondern sich ihnen stellt.

4. Paradoxien strategischer Vulnerabilität – und ihrer resilienten Bewältigung

Insbesondere drei Paradoxien hat eine Gesellschaft zu bewältigen, wenn sie auf strategische Vulnerabilität mit strategischer Resilienz zu reagieren versucht: das sicherheitspolitische, das sicherheitspsychologische und das sicherheitskommunikative Vulnerabilitätsparadox. Dem sicherheitspolitischen Vulnerabilitätsparadox zufolge gilt: *Je entschlossener und effektiver eine Gesellschaft mit den Mitteln der Sicherheitspolitik ihre Vulnerabilität zu verringern strebt, desto größer kann diese werden.* Wenn eine Gesellschaft sicherheitspolitische Maßnahmen trifft, um ihre identifizierten Schwachstellen zu schließen oder die Folgen einer gegnerischen Ausnutzung dieser

Schwachstellen zu bewältigen, so können die Kosten solcher Maßnahmen deren Nutzen überwiegen und letztlich gar zu größerer statt verringerter Vulnerabilität führen. Das ist das klassische Dilemma der Terrorismusbekämpfung: dass die terroristische Gefährdung zu Schutz- und Gegenmitteln provoziert, die zu vitalen (Selbst-)Verletzungen führen können. Eine konsequente Schließung etwa jener vulnerablen Stelle im Luftfrachtbereich, die durch das Auftauchen von Sprengstoffpaketen im Bundeskanzleramt und anderenorts im Jahr 2010 offengelegt wurde, zöge erhebliche finanzielle Belastungen und Zeitverluste infolge strengerer Sicherheitsvorkehrungen nach sich, die die Prosperitätssteigerungen der letzten Jahre in ihr Gegenteil verkehren könnten. Diese Prosperitätssteigerungen erwuchsen nämlich im Wesentlichen aus Beschleunigungen, wie sie die Just-in-time-Produktion verlangt, die in den vergangenen Jahren zum Abbau von Reserven und Redundanzen führte. Deren Wiederaufbau mag zwar die Verwundbarkeit des Transportwesens und der Ökonomie verringern, hat aufgrund der damit einhergehenden Entschleunigung aber auch erhebliche Wohlstandsverluste zur Folge. Die Regierungen befinden sich in dieser Frage – wie so oft bei der Terrorismusabwehr – in einer klassischen Zwickmühle: Es geht dabei um zwei hintereinander gelagerte Verwundbarkeiten: Sicherheit und Wohlstand. Eines dieser Güter muss zurücktreten, und da ein strategisch kalkulierender Gegenakteur dieses Dilemma mit vergleichbar begrenzten Mitteln aufdecken kann, handelt es sich hier um eine folgenreiche strategische Vulnerabilität. Sie zu bewältigen, hieße im Sinne der Steigerung strategischer Resilienz, im Bewusstsein der (zuweilen untolerierbar hohen) Kosten der Vulnerabilitätsminimierung eine Güterabwägung zwischen Wohlstand, Sicherheit und weiteren zentralen Werten, darunter insbesondere Freiheit, durchzuführen, um so die Prioritäten einer Gesellschaft im Umgang mit strategischer Vulnerabilität zu bestimmen. Ob und wie hier ein gesellschaftlicher Konsens gefunden und umgesetzt werden kann, der insbesondere auch den Angriffen eines strategischen Gegenakteurs standzuhalten vermag, bleibt die große Herausforderung für eine strategisch resiliente Reaktion auf strategische Vulnerabilität. Durch das sicherheitspsychologische Vulnerabilitätsparadox wird diese Herausforderung noch vergrößert.

Das sicherheitspsychologische Vulnerabilitätsparadox besagt: *Je weniger verwundbar eine Gesellschaft ist bzw. sich verwundbar fühlt, desto schwerwiegender fallen Verwundungen aus, die dennoch eintreten.*[8] Selbst wenn eine Gesellschaft auf der Grundlage eines Konsenses über ihre „prioritären“ bzw. „kritischen“ Vulnerabilitäten Anstrengungen zu deren gezielter Minimierung unternimmt und diese Anstrengungen dann sowohl objektiv als auch subjektiv die Sicherheit

8 Vgl. hierzu auch das inhaltlich identische „Verletzungsparadoxon“, welches das Bundesministerium des Innern (BMI, 2009, S. 11) wie folgt formuliert: „In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus.“

erhöhen, so kann die Vulnerabilität dieser Gesellschaft insgesamt steigen, insofern als eine Verbesserung der Sicherheitslage bzw. des Sicherheitsempfindens die Wirkung dennoch eintretender Schadensfälle und insbesondere intendierter Gefährdungen in möglicherweise strategische Dimensionen erhöht. So wird ein Gegenakteur, der diese Dialektik erkennt und sie ebenso wie das hohe Sicherheitsbedürfnis postheroischer Gesellschaften[9] in seine Planungen einkalkuliert, gerade in jenen Bereichen anzugreifen versuchen, in denen vermeintlich Sicherheit herrscht. Die Medien dienen ihm dabei zur dramatischen Verstärkung des zu erzielenden Unsicherheitsempfindens. Der Terrorismus nutzt sie als nichtkinetische Waffen, um moderne Gesellschaften zu attackieren, wobei er zur Ausführung dieser Attacken nur eines Minimums an kinetischen Waffen bedarf. Mit der so freigesetzten Angst und deren kataklysmischer Verstärkung durch die Berichterstattung haben die Terroristen die strategische Verletzlichkeit moderner postheroischer Gesellschaften entdeckt, und um diese Wunde offenzuhalten, haben sie in ihr ein Symbol platziert: den Selbstmordattentäter. Die Anstrengungen zur Schließung dieser Wunde im bisherigen Stile, also insbesondere durch die Verschärfung von Schutzmaßnahmen und Sicherheitsvorkehrungen in „kritischen“ Bereichen, werden nicht nur zu weiteren Verlusten – an Freiheit, an Wohlstand, aber auch an Sicherheit – führen, sondern können aufgrund des sicherheitspsychologischen Vulnerabilitätsparadoxes auch zur Folge haben, dass die Vulnerabilität eher steigt als sinkt. Eine notorische Überforderung der Sicherheitssysteme sowie der verwundbaren gesellschaftlichen Psyche können hier nur durch eine Änderung der Rahmenbedingungen verhindert werden. Der Schlüssel besteht im Nachdenken über Unsicherheitsakzeptanz. Wenn eine Gesellschaft derzeit infolge ihrer Güterabwägung dazu bereit ist, etwa auf den Gebieten des Extremsports oder der Ernährung Unsicherheiten in Kauf zu nehmen, dann müsste sie auch bereit sein, im Gesamtentwurf des Lebens Elemente der Unsicherheit zu akzeptieren, um auf diese Weise unter dem Strich ökonomisch und normativ unangenehme Randerscheinungen wie etwa Wohlfahrtseinbußen, Überwachungssysteme oder Datenbanken zu vermeiden. Die strategisch resiliente Antwort auf das sicherheitspsychologische Vulnerabilitätsparadox bestünde daher in *heroischer Gelassenheit* als bewusster Paradoxie: Es kommt darauf an, strategische Widerstandsfähigkeit nicht durch die Herstellung von Schutz, sondern durch Unsicherheitsakzeptanz zu generieren. Für den politischen Akteur bedeutet dies, nicht nur gesellschaftlich formulierte Anforderungen an mehr Sicherheit zu erfüllen, sondern auch Gegenkonzepte der Unsicherheitsakzeptanz zu kommunizieren, was auf das dritte, das sicherheitskommunikative Vulnerabilitätsparadox verweist.

9 Zum Begriff der postheroischen Gesellschaft und dessen Implikationen vgl. Münkler (2006, S. 310ff.).

Das sicherheitskommunikative Vulnerabilitätsparadox besagt: *Je offener eine Gesellschaft über ihre Vulnerabilität kommuniziert, desto verwundbarer kann sie werden.* Wenn eine Gesellschaft, wie das Leitbild der „Risikokommunikation" (Renn et al., 2007, S. 111) es vorsieht, offen thematisiert, welche Risiken und Unsicherheiten sie einzugehen bereit ist, welche Werte, Strukturen und Institutionen sie für „kritisch" hält und welche Schwachstellen sie mit guten Gründen nicht vollends zu schließen beabsichtigt, um ihnen auf andere Weise, etwa mit heroischer Gelassenheit, zu begegnen, so kann dies durchaus zu dem gesuchten gesellschaftlichen Konsens und damit zu strategischer Resilienz führen. Freilich setzt dies voraus, dass an dem Prozess der Risikokommunikation neben den „Sicherheitsexperten" auch die „Sicherheitslaien" gleichberechtigt beteiligt werden, dass also das „objektive" strategische Wissen der Sicherheitsforschung und Sicherheitspolitik mit dem „subjektiven" Sicherheitswissen und Sicherheitsempfinden der Bürger in einen Austausch tritt. Ob in einem solchen Austausch ein Konzept wie das der „heroischen Gelassenheit" seine gewünschte Wirkung entfalten kann, hängt vor allem davon ab, wie überzeugend, sensibel und auch gelassen die politischen und wissenschaftlichen Sicherheitsexperten über Unsicherheit kommunizieren. Unabhängig davon ergibt sich das sicherheitskommunikative Vulnerabilitätsparadox jedoch aus dem Umstand, dass an der offenen Risikokommunikation neben den Sicherheitsexperten und Sicherheitslaien ein zuweilen übersehener Dritter beteiligt ist: der strategische Gegenakteur. Als stiller Beobachter verfolgt er aus der Deckung seiner Anonymität und Unsichtbarkeit heraus die offene Risikokommunikation, um aus deren Verlauf und Ausgang seine eigenen, strategischen Schlüsse zu ziehen. Wenn die Risikokommunikation in ihrer Offenheit diesen strategischen Gegenakteur nicht im Blick behält, so droht sie selbst zur Zielscheibe oder zum Einfallstor für Verletzungen zu werden und gesellschaftliche Vulnerabilität zu vergrößern statt zu verringern.[10] Soll dies verhindert werden, ohne dass es zu kritischen Selbstverletzungen etwa durch Eingriffe der Zensur oder Maßnahmen der Geheimhaltung kommt, die die normativen Grundlagen der offenen Gesellschaft und damit letztlich auch ihre strategische Resilienz zerstören können, so ist an die Kommunikationsteilnehmer die Erwartung zu richten, dass sie selbst ihre Vulnerabilitätskommunikation verantwortungsvoll auf deren mögliche Folgen hin reflektieren: im Hinblick auf die Folgen für das gesellschaftliche Sicherheitsbedürfnis und Sicherheitsempfinden einerseits sowie die Informationslage strategischer Gegenakteure andererseits. Ein derart reflexiver

10 Anders als zumeist die Risikoforschung ist die deutsche Sicherheitspolitik sich dieser Gefahr bewusst: Die „Nationale Strategie zum Schutz Kritischer Infrastrukturen" betont, dass die anzustrebende „Risikokultur" unter anderem auf „einer offenen Risikokommunikation zwischen Staat, Unternehmen, Bürgern und Öffentlichkeit *unter Berücksichtigung der Sensibilität bestimmter Informationen*" (BMI, 2009, S. 11; Hervorhebung durch die Autoren) beruht.

Umgang mit dem eigenen Wissen und Reden über Vulnerabilität, der die wissenschaftliche und politische Vulnerabilitätskommunikation fortlaufend einer strategischen Folgenabschätzung unterzieht, ist die Voraussetzung dafür, dass die (verletzungs-)offene Gesellschaft im Angesicht verletzungsfähiger strategischer Gegenakteure Widerstandskraft generiert. Wenn sie stattdessen freilich diese Gegenakteure aus ihrem Vulnerabilitätsdiskurs ausblendet und auf die *strategische* Analyse ihrer Verwundbarkeit verzichtet, so wäre dies kein Zeichen der Resilienz, sondern vielmehr eines *strategischer* Vulnerabilität.

Literatur

Bohle, H.-G. (2008). Leben mit Risiko: Resilience als neues Paradigma für die Risikowelten von morgen. In C. Felgentreff & T. Glade (Hrsg.). *Naturrisiken und Sozialkatastrophen* (S. 435–441). Berlin: Spektrum Akademischer Verlag.

Bohle, H.-G. & Glade, T. (2008). Vulnerabilitätskonzepte in Sozial- und Naturwissenschaften. In C. Felgentreff & T. Glade (Hrsg.). *Naturrisiken und Sozialkatastrophen* (S. 99–119). Berlin: Spektrum Akademischer Verlag.

Beck, U. (2007). *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit.* Frankfurt/M.: Suhrkamp.

Birkmann, J. (Ed.) (2006). *Measuring vulnerability to natural hazards: towards disaster resilient societies.* Tokyo: United Nations University Press.

Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T. & Schmude, M. (2010). *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall.* Berlin: Forschungsforum Öffentliche Sicherheit.

Bundesministerium des Innern (BMI) (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* Berlin.

Clausewitz, C. von (2002). *Vom Kriege.* München: Ullstein.

Coale, A. (1947). The Problem of Reducing Vulnerability to Atomic Bombs. *The American Economic Review, 37* (2), 87–97.

Cutter, S. L. (2003). The Vulnerability of Science and the Science of Vulnerability. *Annals of the Association of American Geographers 93* (1), 1–12.

Dombrowsky, W. R. (2008). Zur Entstehung der soziologischen Katastrophenforschung – eine wissenshistorische und -soziologische Reflexion. In C. Felgentreff & T. Glade (Hrsg.). *Naturrisiken und Sozialkatastrophen* (S. 63–76). Berlin: Spektrum Akademischer Verlag.

Fischer, W. (2007). *www.InfrastrukturInternetCyberterror.Netzwerk. Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet.* Jülich: Forschungszentrum Jülich.

Gallucci, R. L. (2006). Contemplating Extreme Responses to U.S. Vulnerability. *Annals of the American Academy of Political and Social Science, 607* (Confronting the Specter of Nuclear Terrorism) (pp. 51–58).

Hoch, M. (2001). Falken, Tauben und der Elefant Gottes. Hattin, 4. Juli 1187. In S. Förster, M. Pöhlmann & D. Walter (Hrsg.). *Schlachten der Weltgeschichte* (S. 79–92). München: C. H. Beck.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics, 4*, 1–23.

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

Kaysen, K. (1953). The Vulnerability of the United States to Enemy Attack. *World Politics, 6* (2), 190–208.

Keegan, I. (1978). *Die Schlacht. Azincourt 1415 – Waterloo 1815 – Somme 1916*. München: dtv.

Kloepfer, M. (2010). *Schutz kritischer Infrastrukturen.* Baden-Baden: Nomos.

Kortüm, H.-H. (2004). Azincourt 1415: Militärische Delegitimierung als Mittel sozialer Disziplinierung. In H. Carl, H.-H. Kortüm, D. Langewiesche & F. Lenger (Hrsg.). *Kriegsniederlagen. Erfahrungen und Erinnerungen* (S. 89–106). Berlin: Akademie Verlag.

Kupchan, C. (1994). *The Vulnerability of Empire.* Ithaca: Cornell University Press.

Lenz, S. (2009). *Vulnerabilität kritischer Infrastrukturen.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Luttwak, E. (2003). *Strategie. Die Logik von Krieg und Frieden.* Lüneburg: zu Klampen.

Münkler, H. (1990). *Odysseus und Kassandra. Politik im Mythos*. Frankfurt/M.: Fischer Taschenbuch Verlag.

Münkler, H. (2006). *Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie.* Weilerswist: Velbrück Wissenschaft.

Münkler, H., Bohlender, M. & Meurer, S. (Hrsg.) (2010). *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert.* Bielefeld: Transcript Verlag.

Perrow, C. (2011). *The Next Catastrophe. Reducing our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (3. Aufl.). Princeton: Princeton University Press.

Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M. & Riehm, U. (2011). *Was bei einem Blackout geschieht. Folgen eines langandauernden und großräumigen Stromausfalls.* Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 33. Berlin: Edition Sigma.

Reichenbach, G., Göbel, R., Wolff, H. & Stokar von Neuforn, S. (2008). *Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen*. Grünbuch des Zukunftsforums Öffentliche Sicherheit. Berlin: ProPress Verlagsgesellschaft.

Renn, O., Schweizer, P.-J., Dreyer, M. & Klinke, A. (2007). *Risiko. Über den gesellschaftlichen Umgang mit Unsicherheit*. München: Oekom.

Schutzkommission (2011). *Vierter Gefahrenbericht der Schutzkommission beim Bundesministerium des Innern.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Thywissen, K. (2006). Core terminology of disaster reduction: A comparative glossary. In J. Birkmann (Ed.). *Measuring vulnerability to natural hazards: towards disaster resilient societies* (pp. 448–496). Tokyo: United Nations University Press.

Turner, B. L. II, Kasperson, R. E., Matson, P. A., McCarthy, J. J., Corell, R. W., Christensen, L. et al. (2003). A Framework for Vulnerability Analysis in Sustainability Science. *Proceedings from the National Academy of Science, 100* (14), 8074–8079.

Wisner, B., Blaikie, P., Cannon, T. & Davis, I. (2004). *At Risk. Natural Hazards, People's Vulnerability and Disasters* (2. Aufl.). London: Routledge.

Wolf, K. (2008): *Gallipoli 1915. Das deutsch-türkische Militärbündnis im Ersten Weltkrieg*, Sulzbach/Ts.: Report Verlag.